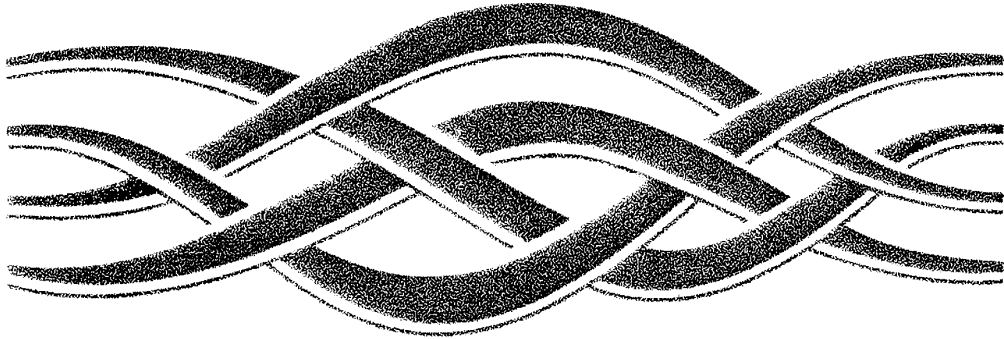


For Distribution Only With a New PC  
TCP/IP



Microsoft **WINDOWS NT**  
**SERVER**

# TCP/IP

## **Microsoft Windows NT™ Server**

**Version 3.5**

**Microsoft Corporation**

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

© 1985–1994 Microsoft Corporation. All rights reserved.

Microsoft, MS, MS-DOS, MSX, and Win32 are registered trademarks and Windows and Windows are trademarks of Microsoft Corporation in the U.S.A. and other countries.

Apple, AppleTalk, and Macintosh are registered trademarks of Apple Computer, Inc.

CompuServe is a registered trademark of CompuServe, Inc.

Open VMS is a registered trademark and DEC and DECnet are trademarks of Digital Equipment Corporation.

HP is a registered trademark of Hewlett-Packard Company.

IBM is a registered trademark of International Business Machines Corporation.

Lotus and Lotus Notes are registered trademarks of Lotus Development Corporation.

Novell and NetWare are registered trademarks of Novell, Inc.

NT is a trademark of Northern Telecom Limited in the U.S.A. and other countries.

PostScript is a registered trademark of Adobe Systems, Inc.

Sun is a registered trademark of Sun Microsystems, Incorporated.

UNIX is a registered trademark of UNIX Systems Laboratories.

008.A6430.EN112

# Contents

<b>Welcome</b> .....	<b>xi</b>
What's New in This Release? .....	xii
How to Use This Manual .....	xiii
Documentation Conventions .....	xv
Finding More Information .....	xv
<b>Chapter 1 Overview of Microsoft TCP/IP for Windows NT</b> .....	<b>1</b>
What Is TCP/IP for Windows NT? .....	2
What Does Microsoft TCP/IP Include? .....	3
Windows NT Solutions in TCP/IP Internetworks .....	7
Using TCP/IP for Scalability in Windows Networks .....	7
Using TCP/IP for Connectivity to the Internet .....	8
TCP/IP for Heterogeneous Networking .....	10
Using TCP/IP with Third-Party Software .....	11
<b>Chapter 2 Installing and Configuring Microsoft TCP/IP and SNMP</b> .....	<b>15</b>
Before Installing Microsoft TCP/IP .....	16
Installing TCP/IP .....	17
Configuring TCP/IP .....	20
Using DHCP .....	20
Configuring TCP/IP Manually .....	21
Configuring TCP/IP to Use DNS .....	25
Configuring Advanced TCP/IP Options .....	27
Configuring SNMP .....	30
Configuring SNMP Security .....	32
Configuring SNMP Agent Information .....	34
Removing TCP/IP Components .....	35
Configuring RAS for Use with TCP/IP .....	36
<b>Chapter 3 Networking Concepts for TCP/IP</b> .....	<b>37</b>
TCP/IP and Windows NT Networking .....	38
Internet Protocol Suite .....	39
Transmission Control Protocol and Internet Protocol .....	39
User Datagram Protocol .....	40
Address Resolution Protocol and Internet Control Message Protocol .....	40



---

IP Addressing .....	41
IP Addresses .....	41
Network ID and Host ID .....	42
Subnet Masks .....	43
Routing and IP Gateways .....	44
Dynamic Host Configuration Protocol .....	46
Name Resolution for Windows Networking .....	48
NetBIOS over TCP/IP and Name Resolution .....	50
B-Node .....	51
P-Node .....	51
M-Node .....	52
H-Node .....	52
B-Node with LMHOSTS and Combinations .....	52
Windows Internet Name Service and Broadcast Name Resolution .....	53
WINS in a Routed Environment .....	53
WINS Name Registration .....	58
WINS Name Release .....	58
WINS Name Renewal .....	59
IP Addressing for RAS .....	60
Name Resolution with Host Files .....	61
Domain Name System Addressing .....	62
SNMP .....	65
<b>Chapter 4 Installing and Configuring DHCP Servers .....</b>	<b>67</b>
Overview of DHCP Clients and Servers .....	68
Installing DHCP Servers .....	69
Using DHCP Manager .....	70
Defining DHCP Scopes .....	72
Creating Scopes .....	73
Changing Scope Properties .....	75
Removing a Scope .....	75
Configuring DHCP Options .....	75
Assigning DHCP Configuration Options .....	76
Creating New DHCP Options .....	78
Changing DHCP Option Values .....	80
Defining Options for Reservations .....	81
Predefined DHCP Client Configuration Options .....	82
Administering DHCP Clients .....	87
Managing Client Leases .....	88
Managing Client Reservations .....	89

---

Managing the DHCP Database Files .....	91
Troubleshooting DHCP .....	92
Restoring the DHCP Database .....	93
Backing up the DHCP Database onto Another Computer .....	93
Advanced Configuration Parameters for DHCP .....	94
Registry Parameters DHCP Servers .....	95
Registry Parameters for DHCP Clients .....	97
Guidelines for Setting Local Policies .....	97
Guidelines for Managing DHCP Addressing Policy .....	97
Dynamic Allocation of IP Addresses .....	97
Manual Allocation of IP Addresses .....	99
Guidelines for Lease Options .....	99
Guidelines for Partitioning the Address Pool .....	100
Guidelines for Avoiding DNS Naming Conflicts .....	100
Using DHCP with Diskless Workstations .....	101
Planning a Strategy for DHCP .....	101
Planning a Small-Scale Strategy for DHCP Servers .....	102
Planning a Large-Scale Strategy for DHCP Servers .....	103
<b>Chapter 5 Installing and Configuring WINS Servers .....</b>	<b>105</b>
WINS Benefits .....	106
Installing WINS Servers .....	106
Administering WINS Servers .....	107
Configuring WINS Servers and Replication Partners .....	112
Configuring WINS Servers .....	113
Configuring Replication Partners .....	116
Configuring Replication Partner Properties .....	118
Triggering Replication Between Partners .....	120
Managing Static Mappings .....	120
Adding Static Mappings .....	122
Editing Static Mappings .....	124
Filtering the Range of Mappings .....	125
Managing Special Names .....	126
Normal Group Names .....	126
Multihomed Names .....	126
Internet Group Names .....	126
How WINS Handles Special Names .....	127
Setting Preferences for WINS Manager .....	129

Managing the WINS Database .....	132
Scavenging the Database .....	132
Viewing the WINS Database .....	134
Backing Up the Database .....	136
Troubleshooting WINS .....	137
Basic WINS Troubleshooting .....	137
Restoring or Moving the WINS Database .....	139
Restoring a WINS Database .....	139
Restarting and Rebuilding a Down WINS Server .....	139
Moving the WINS Database .....	140
Advanced Configuration Parameters for WINS .....	141
Registry Parameters for WINS Servers .....	142
Registry Parameters for Replication Partners .....	143
Parameters for Push Partners .....	143
Parameters for Pull Partners .....	144
Planning a Strategy for WINS Servers .....	145
Planning for Server Performance .....	145
Planning Replication Partners and Proxies .....	145
Planning Replication Frequency Between Hubs .....	146
<b>Chapter 6 Setting Up LMHOSTS .....</b>	<b>147</b>
Editing the LMHOSTS File .....	148
Rules for LMHOSTS .....	148
Guidelines for LMHOSTS .....	150
Using LMHOSTS with Dynamic Name Resolution .....	151
Specifying Remote Servers in LMHOSTS .....	151
Designating Domain Controllers Using #DOM .....	153
Using Centralized LMHOSTS Files .....	155
<b>Chapter 7 Using the Microsoft FTP Server Service .....</b>	<b>157</b>
Installing the FTP Server Service .....	158
Configuring the FTP Server Service .....	159
Administering the FTP Server Service .....	163
Using FTP Commands at the Command Prompt .....	164
Managing Users .....	164
Controlling the FTP Server and User Access .....	165
Annotating Directories .....	165

Changing Directory Listing Format .....	166
Customizing Greeting and Exit Messages .....	166
Logging FTP Connections .....	166
Advanced Configuration Parameters for FTP Server Service .....	167
<b>Chapter 8 Using Performance Monitor with TCP/IP Services .....</b>	<b>171</b>
Using Performance Monitor with TCP/IP .....	172
Monitoring TCP/IP Performance .....	173
ICMP Performance Counters .....	173
IP Performance Counters .....	175
Network Interface Performance Counters for TCP/IP .....	177
TCP Performance Counters .....	179
UDP Performance Counters .....	180
Monitoring FTP Server Traffic .....	180
Monitoring WINS Server Performance .....	182
<b>Chapter 9 Internetwork Printing with TCP/IP .....</b>	<b>183</b>
Overview of TCP/IP Printing .....	184
Setting Up Windows NT for TCP/IP Printing .....	185
Creating a Printer for TCP/IP Printing .....	185
Printing to Windows NT from UNIX Clients .....	189
<b>Chapter 10 Troubleshooting TCP/IP .....</b>	<b>191</b>
Troubleshooting IP Configuration .....	192
Troubleshooting Name Resolution Problems .....	193
Name Resolution Problems in HOSTS .....	193
Name Resolution Problems in LMHOSTS .....	193
Troubleshooting Other Connection Problems .....	193
Troubleshooting Other Problems .....	195
Troubleshooting the FTP Server Service .....	195
Troubleshooting Telnet .....	196
Troubleshooting Gateways .....	196
Troubleshooting TCP/IP Database Files .....	197

---

<b>Chapter 11 Utilities Reference</b> .....	<b>199</b>
arp .....	200
finger .....	201
ftp .....	201
hostname .....	204
ipconfig .....	205
lpq .....	206
lpr .....	206
nbstat .....	207
netstat .....	209
ping .....	210
rcp .....	212
rexec .....	215
route .....	216
rsh .....	217
telnet .....	218
tftp .....	219
tracert .....	220

## Appendixes

<b>Appendix A MIB Object Types for Windows NT</b> .....	<b>223</b>
LAN Manager MIB II for Windows NT Objects .....	224
Common Group .....	224
Server Group .....	225
Workstation Group .....	228
Domain Group .....	228
Microsoft DHCP Objects .....	229
DHCP MIB Parameters .....	229
DHCP Scope Group .....	229
Microsoft WINS Objects .....	230
WINS Parameters .....	230
WINS Datafiles Group .....	232
WINS Pull Group .....	232
WINS Push Group .....	233
WINS Cmd Group .....	234

**Appendix B Windows Sockets Applications** ..... 237

    Vendors ..... 237

    Internet Sources for Applications ..... 241

**Glossary** ..... 245

**Index** ..... 253



# Welcome

Welcome to Microsoft® TCP/IP for Windows NT™.

Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks. This manual, *Microsoft Windows NT Server TCP/IP*, describes how to install, configure, and troubleshoot Microsoft TCP/IP on a computer running the Microsoft Windows NT Workstation or Windows NT Server operating system. It also provides a reference for the TCP/IP utilities and information about how to install and use the other TCP/IP services such as the File Transfer Protocol (FTP) Server service, TCP/IP printing, and Simple Network Management Protocol (SNMP), plus the software to support new dynamic configuration and name resolution services.

This manual assumes that you are familiar with the Microsoft Windows NT operating system. If you are not familiar with this product, refer to your Microsoft Windows NT documentation set.

This introduction provides the following basic information:

- What's new in this release
- How to use this manual
- Document conventions
- Finding more information



## What's New in This Release?

In this new version of Windows NT, TCP/IP capabilities have been expanded to include automatic TCP/IP configuration and powerful name resolution capabilities through the addition of new protocols and supporting administrative tools. New TCP/IP utilities plus the addition of performance counters for TCP/IP and related services will also help make administrative tasks easier. New elements include the following:

- Enhanced speed and performance
- Dynamic Host Configuration Protocol (DHCP)  
Microsoft TCP/IP supports automatic TCP/IP configuration through the new DHCP service. When DHCP servers are installed on the network, users can take advantage of dynamic IP address allocation and management.
- Windows Internet Name Service (WINS)  
Microsoft TCP/IP provides a powerful, new name resolution service for easy, centralized management of computer name-to-IP address resolution in medium and large internetworks.
- New TCP/IP utilities and commands  
This version includes a new Windows-based Telnet accessory for connecting to remote systems. The utilities provided with Microsoft TCP/IP have been expanded to include **ipconfig** for displaying current TCP/IP network configuration values, **tracert** for determining the route taken to a destination, **lpq** for showing print queue status for TCP/IP printing, and **lpr** for printing a file in TCP/IP printing.
- Performance counters  
You can use Performance Monitor to track performance of the IP protocols, FTP Server service traffic, and WINS servers. You can also use SNMP to monitor and manage WINS and DHCP servers.
- Multiple default gateways  
You can configure multiple default gateways for Windows NT computers. This ensures maximum reliability in networks that offer redundant routes.
- TCP/IP printing  
With TCP/IP printing installed on a single Windows NT computer on the network, other Windows networking computers can print to a direct-connect TCP/IP printer or a UNIX®-connected printer, without any special client software.

---

## How to Use This Manual

This manual contains the following chapters and appendix:

**Chapter 1, "Overview of Microsoft TCP/IP for Windows NT"**

Describes the elements that make up Microsoft TCP/IP and provides an overview of how you can use Microsoft TCP/IP to support various networking solutions.

**Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP"**

Describes the process for installing and configuring Microsoft TCP/IP, SNMP, and Remote Access Service (RAS) with TCP/IP on a computer running Windows NT.

**Chapter 3, "Networking Concepts for TCP/IP"**

Presents key TCP/IP networking concepts for network administrators interested in a technical discussion of the elements that make up Microsoft TCP/IP.

**Chapter 4, "Installing and Configuring DHCP Servers"**

Presents the procedures and strategies for setting up servers to support the Dynamic Host Configuration Protocol for Windows networks.

**Chapter 5, "Installing and Configuring WINS Servers"**

Presents the procedures and strategies for setting up Windows Internet Name Service servers.

**Chapter 6, "Setting Up LMHOSTS"**

Provides guidelines and tips for using LMHOSTS files for name resolution on networks.

**Chapter 7, "Using the Microsoft FTP Server Service"**

Describes how to install, configure, and administer the Microsoft FTP Server service.

**Chapter 8, "Using Performance Monitor with TCP/IP Services"**

Describes how to use the performance counters for TCP/IP, FTP Server service, DHCP servers, and WINS servers.

**Chapter 9, "Internetwork Printing and TCP/IP"**

Describes how to install TCP/IP printing and create TCP/IP printers on Windows NT computers with Microsoft TCP/IP.

**Chapter 10, "Troubleshooting TCP/IP"**

Describes how to troubleshoot IP connections and use the diagnostic utilities to get information that will help solve networking problems.

**Chapter 11, "Utilities Reference"**

Describes the TCP/IP utilities and provides syntax and notes.

**Appendix A, "LAN Manager MIB II for Windows NT Objects"**

Describes the LAN Manager MIB II objects provided when you install SNMP with Windows NT.

**Appendix B, "Windows Sockets Application Vendors"**

Lists third-party vendors who have created software based on the Windows Sockets standard to provide utilities and applications that run in heterogeneous networks that use TCP/IP. This appendix also lists Internet sources for public-domain software based on Windows Sockets.

The Glossary provides definitions of TCP/IP and networking technical terms used in this manual.

You can get online Help by pressing F1 in all dialog boxes for installing and configuring TCP/IP and related components. You can also get online Help about the Microsoft TCP/IP networking solutions and for the TCP/IP utilities.

**► To get help on Microsoft TCP/IP networking solutions**

- In File Manager, double-click TCPIP.HLP in *\systemroot\SYSTEM32* (this could be *C:\WINNT35\SYSTEM32*, or wherever you installed the Windows NT system files).

**► To get help on TCP/IP utilities**

- At the command prompt, type a TCP/IP command name followed by the *-?* switch. For example, type *ping -?* and press ENTER to get help on the *ping* command.

–Or–

1. In the Program Manager Main group, double-click the Windows NT Help icon.
2. In the Windows NT Help window, click the Command Reference Help button.
3. In the Commands window, click a command name.

–Or–

In the Command Reference window, choose the Search button, and then type a command name in the box or select a command name from the list.

## Documentation Conventions

This manual uses several type styles and special characters, described in the following list:

Convention	Use
<b>bold</b>	Represents commands, command options, and file entries. Type bold words exactly as they appear (for example, <b>net use</b> ).
<i>italic</i>	Introduces new terms and represents variables. For example, the variable <i>computer name</i> indicates that you type the name of a workstation or a server.
ALL UPPERCASE	Represents filenames and paths. (You can, however, type such entries in uppercase or lowercase letters, or a combination of the two.)
SMALL CAPITALS	Represents keyboard names (for example, CTRL, ENTER, and F2).
[brackets]	Encloses optional items in syntax statements. For example, [ <i>password</i> ] indicates that you can choose to type a password with the command. Type only the information within the brackets, not the brackets themselves.
...(ellipsis)	Indicates a command element may be repeated.
►	Indicates a procedure.
Windows NT	Refers to operating system and networking functionality that is available in both Windows NT Server and Windows NT Workstation.
\\WINNT or \\systemroot	Refers to the Windows NT system tree. This can be \\WINNT, \\WINNT35, \\WINDOWS, or whatever other directory name you specified when installing Windows NT.

## Finding More Information

In addition to the standard ways for receiving technical support from Microsoft (as described in the *Windows NT Server Installation Guide*), you can get support for Windows NT via the Internet.

---

**Note** Your computer must be connected to the Internet to take advantage of this service.

---

► **To get Windows NT support via the Internet**

- Start **ftp** and connect to **ftp.microsoft.com**

This support service uses anonymous FTP under Windows NT to provide documentation, utilities, updated drivers, and other information for many Microsoft systems products.

For a more technical discussion of the topics mentioned in this manual, refer to the following texts and articles:

Allard, J. "DHCP—TCP/IP Network Configuration Made Easy," *ConneXions*, Volume 7, No. 8, August 1993.

Allard, J., K. Moore, and D. Treadwell. "Plug into Serious Network Programming with the Windows Sockets API," *Microsoft Systems Journal*, July: 35–40, 1993.

Comer, D. *Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture*. Second edition. Englewood Cliffs, NJ: Prentice Hall, 1991.

Comer, D. and D. Stevens. *Internetworking with TCP/IP Volume II: Design, Implementation, and Internals*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Comer, D. and D. Stevens. *Internetworking with TCP/IP Volume III: Client-Server Programming and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1991.

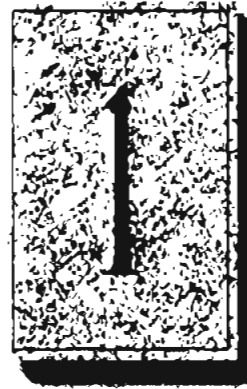
Hall, M., et al. *Windows Sockets: An Open Interface for Network Programming Under Microsoft Windows*, Version 1.1, Revision A, 1993.

Krol, E. *The Whole Internet User's Guide and Catalog*. Sebastopol, CA: O'Reilly and Associates, 1992.

Rose, M.T. *The Simple Book*. Englewood Cliffs, NJ: Prentice Hall, 1991.

## CHAPTER 1

# Overview of Microsoft TCP/IP for Windows NT



Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks made up of computers with diverse hardware architectures and various operating systems. TCP/IP can be used to communicate with Windows NT systems, with devices that use other Microsoft networking products, and with non-Microsoft systems, such as UNIX.

This chapter introduces Microsoft TCP/IP for Windows NT. The topics in this chapter include the following:

- What is TCP/IP for Windows NT?
- What does Microsoft TCP/IP include?
- Windows NT solutions in TCP/IP internetworks

For more detailed information on TCP/IP and its integration with Microsoft Windows NT and other networking products, see Chapter 3, "Networking Concepts for TCP/IP."

## What Is TCP/IP for Windows NT?

The TCP/IP protocol family is a standard set of networking protocols, or rules, that govern how data is passed between computers on a network. TCP/IP is used to connect the Internet, the worldwide internetwork connecting over two million universities, research labs, U.S. defense installations, and corporations. (By convention, "Internet" is capitalized when referring to the worldwide internetwork.) These same protocols can be used in private internetworks that connect several local area networks.

Microsoft TCP/IP for Windows NT enables enterprise networking and connectivity on Windows NT computers. Adding TCP/IP to a Windows NT configuration offers the following advantages:

- A standard, routable enterprise networking protocol that is the most complete and accepted protocol available. All modern operating systems offer TCP/IP support, and most large networks rely on TCP/IP for much of their network traffic.
- A technology for connecting dissimilar systems. Many standard connectivity utilities are available to access and transfer data between dissimilar systems, including File Transfer Protocol (FTP) and Terminal Emulation Protocol (Telnet). Several of these standard utilities are included with Windows NT.
- A robust, scalable, cross-platform client-server framework. Microsoft TCP/IP supports the Windows Sockets 1.1 interface, which is ideal for developing client-server applications that can run with Windows Sockets-compliant stacks from other vendors. Many public-domain Internet tools are also written to the Windows Sockets standard. Windows Sockets applications can also take advantage of other networking protocols such as Microsoft NWLink, the Microsoft implementation of the IPX/SPX protocols used in Novell® NetWare® networks.
- The enabling technology necessary to connect Windows NT to the global Internet. TCP/IP, Point to Point Protocol (PPP), and Windows Sockets 1.1 provide the foundation needed to connect and use Internet services.

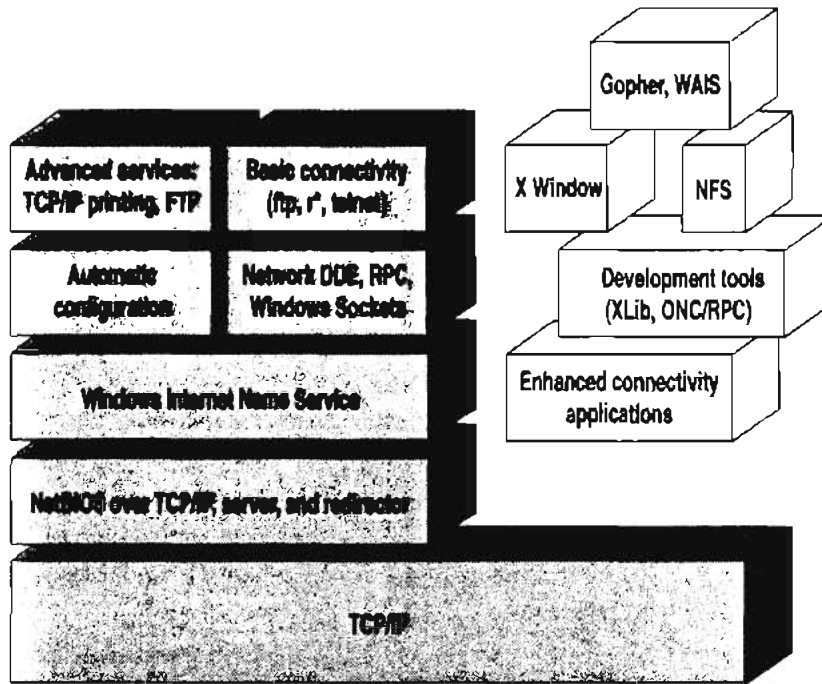
## What Does Microsoft TCP/IP Include?

Microsoft TCP/IP provides all the elements necessary to implement these protocols for networking. Microsoft TCP/IP includes the following:

- Core TCP/IP protocols, including the Transmission Control Protocol (TCP), Internet Protocol (IP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP). This suite of Internet protocols provides a set of standards for how computers communicate and how networks are interconnected. Support is also provided for PPP and Serial-Line IP (SLIP), which are protocols used for dial-up access to TCP/IP networks, including the Internet.
- Support for application interfaces, including Windows Sockets 1.1 for network programming, remote procedure call (RPC) for communicating between systems, NetBIOS for establishing logical names and sessions on the network, and network dynamic data exchange (Network DDE) for sharing information embedded in documents across the network.
- Basic TCP/IP connectivity utilities, including **finger**, **ftp**, **lpr**, **rcp**, **rexec**, **rsh**, **telnet**, and **tftp**. These utilities allow Windows NT users to interact with and use resources on non-Microsoft hosts, such as UNIX workstations.
- TCP/IP diagnostic tools, including **arp**, **hostname**, **ipconfig**, **lpq**, **nbtstat**, **netstat**, **ping**, **route**, and **tracert**. These utilities can be used to detect and resolve TCP/IP networking problems.
- Services and related administrative tools, including the FTP Server service for transferring files between remote computers, Windows Internet Name Service (WINS) for dynamically registering and querying computer names on an internetwork, Dynamic Host Configuration Protocol (DHCP) service for automatically configuring TCP/IP on Windows NT computers, and TCP/IP printing for accessing printers connected to a UNIX computer or connected directly to the network via TCP/IP.
- Simple Network Management Protocol (SNMP) agent. This component allows a Windows NT computer to be administered remotely using management tools such as Sun® Net Manager or HP® Open View. SNMP can also be used to monitor and manage DHCP servers and WINS servers.
- The client software for simple network protocols, including Character Generator, Daytime, Discard, Echo, and Quote of the Day. These protocols allow a Windows NT computer to respond to requests from other systems that support these protocols. When these protocols are installed, a sample QUOTES files is also installed in the `\systemroot\SYSTEM32\DRIVERS\ETC` directory.
- Path MTU Discovery, which provides the ability to determine the datagram size for all routers between Windows NT computers and any other systems on the WAN. Microsoft TCP/IP also supports the Internet Gateway Multicast Protocol (IGMP), which is used by new workgroup software products.



The following diagram shows the elements of Microsoft TCP/IP alongside the variety of additional applications and connectivity utilities provided by Microsoft and other developers.



- Integrated with Windows NT
- Developed by third parties or the research community

Microsoft TCP/IP: Core Technology and Third-Party Add-ons

TCP/IP standards are defined in *Requests for Comments* (RFCs), which are published by the Internet Engineering Task Force (IETF) and other working groups. The relevant RFCs supported in this version of Microsoft TCP/IP (and for Microsoft Remote Access Service) are described in the following table.

**Requests for Comments (RFCs) Supported by Microsoft TCP/IP**

<b>RFC</b>	<b>Title</b>
768	User Datagram Protocol (UDP)
783	Trivial File Transfer Protocol (TFTP)
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
826	Address Resolution Protocol (ARP)
854	Telnet Protocol (TELNET)
862	Echo Protocol (ECHO)
863	Discard Protocol (DISCARD)
864	Character Generator Protocol (CHARGEN)
865	Quote of the Day Protocol (QUOTE)
867	Daytime Protocol (DAYTIME)
894	IP over Ethernet
919, 922	IP Broadcast Datagrams (broadcasting with subnets)
959	File Transfer Protocol (FTP)
1001, 1002	NetBIOS Service Protocols
1034, 1035	Domain Name System (DOMAIN)
1042	IP over Token Ring
1055	Transmission of IP over Serial Lines (IP-SLIP)
1112	Internet Gateway Multicast Protocol (IGMP)
1122, 1123	Host Requirements (communications and applications)
1134	Point to Point Protocol (PPP)
1144	Compressing TCP/IP Headers for Low-Speed Serial Links
1157	Simple Network Management Protocol (SNMP)

**Key Requests for Comments (RFCs) Supported by Microsoft TCP/IP (Continued)**

RFC	Title
1179	Line Printer Daemon Protocol
1188	IP over FDDI
1191	Path MTU Discovery
1201	IP over ARCNET
1231	IEEE 802.5 Token Ring MIB (MIB-II)
1332	PPP Internet Protocol Control Protocol (IPCP)
1334	PPP Authentication Protocols
1533	DHCP Options and BOOTP Vendor Extensions
1534	Interoperation Between DHCP and BOOTP
1541	Dynamic Host Configuration Protocol (DHCP)
1542	Clarifications and Extensions for the Bootstrap Protocol
1547	Requirements for Point to Point Protocol (PPP)
1548	Point to Point Protocol (PPP)
1549	PPP in High-level Data Link Control (HDLC) Framing
1552	PPP Internetwork Packet Exchange Control Protocol (IPXCP)
1553	IPX Header Compression
1570	Link Control Protocol (LCP) Extensions
Draft RFCs	NetBIOS Frame Control Protocol (NBFCP); PPP over ISDN; PPP over X.25; Compression Control Protocol

All RFCs can be found on the Internet via [ds.internic.net](http://ds.internic.net).

In this version of Windows NT, Microsoft TCP/IP does not include a complete suite of TCP/IP connectivity utilities, Network File System (NFS) support, or some TCP/IP server services (daemons) such as **routed** and **telnetd**. Many such applications and utilities that are available in the public domain or from third-party vendors work with Microsoft TCP/IP.

---

**Tip** For Windows for Workgroups computers and MS-DOS-based computers on a Microsoft network, you can install the new version of Microsoft TCP/IP—32 for Windows for Workgroups and the Microsoft Network Client version 2.0 for MS-DOS from the Windows NT Server 3.5 compact disc. This software includes the DHCP and WINS clients and other elements of the new Microsoft TCP/IP software. For information about installing these clients, see Chapter 9, "Network Client Administrator," in the *Windows NT Server Installation Guide*.

---

## Windows NT Solutions in TCP/IP Internetworks

When TCP/IP is used as a transport protocol with Windows NT, Windows NT computers can communicate with other kinds of systems without additional networking software. Microsoft TCP/IP in combination with other parts of Windows NT provides a scalable solution for enterprise networks that include a mix of system types and software on many platforms.

This section summarizes how TCP/IP works with Windows NT to provide enterprise networking solutions. For information about how the elements discussed in this section fit within the networking architecture, see "TCP/IP and Windows NT Networking" in Chapter 3, "Networking Concepts for TCP/IP."

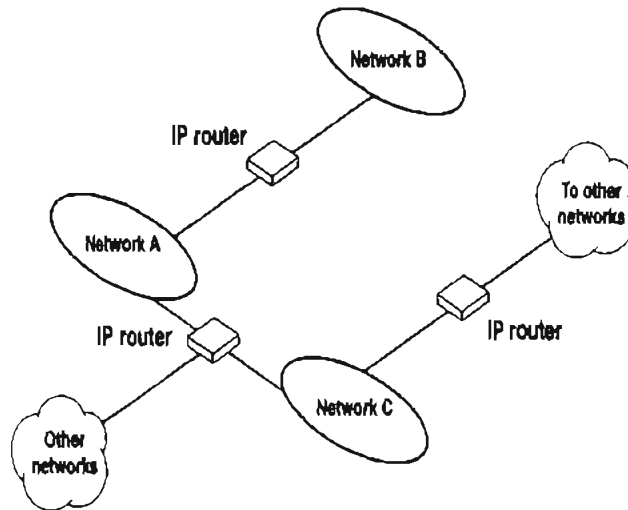
## Using TCP/IP for Scalability in Windows Networks

TCP/IP delivers a scalable internetworking technology widely supported by hardware and software vendors.

When TCP/IP is used as the enterprise networking protocol, the Windows networking solutions from Microsoft can be used on an existing internetwork to provide client and server support for TCP/IP and connectivity utilities. These solutions include:

- Microsoft Windows NT Workstation 3.5, with enhancements to support wide area networks (WAN), TCP/IP printing, extended LMHOSTS, Windows Sockets 1.1, FTP Server service software, and DHCP and WINS client software.
- Microsoft Windows NT Server 3.5, with the same enhancements as Windows NT, plus DHCP server and WINS server software to support the implementation of these new protocols.
- Microsoft TCP/IP-32 for Windows for Workgroups 3.11, with Windows Sockets support, can be used to provide access for Windows for Workgroups computers to Windows NT, LAN Manager, and other TCP/IP systems. Microsoft TCP/IP-32 includes DHCP and WINS client software.
- Microsoft LAN Manager, including both client and server support for Windows Sockets, and MS-DOS<sup>®</sup>-based connectivity utilities. The Microsoft Network Client 2.0 software on the Windows NT Server compact disc includes new Microsoft TCP/IP support with DHCP and WINS clients.

The current version of TCP/IP for Windows NT also supports IP routing in systems with multiple network adapters attached to separate physical networks (multihomed systems).

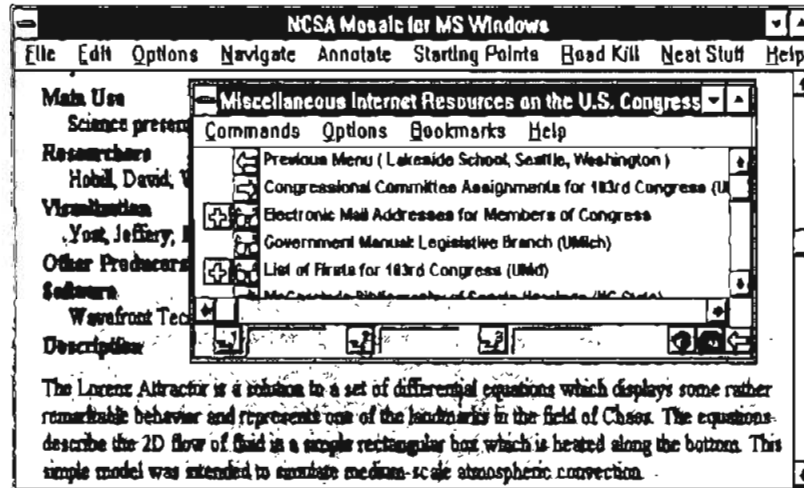


## Using TCP/IP for Connectivity to the Internet

Microsoft TCP/IP provides Windows networking with a set of internetworking protocols based on open standards.

Microsoft TCP/IP for Windows NT includes many common connectivity applications such as **ftp**, **rsh**, and **telnet** that support file transfer, remote process execution, and terminal emulation for communication on the Internet and between non-Microsoft network systems.

TCP/IP applications created by researchers and other users, such as Gopher and NCSA Mosaic, are in the public domain or are available through other vendors as both 16-bit and 32-bit Windows-based applications. Any of these applications that follow the Windows Sockets 1.1 standard are compatible with Windows NT. Such applications allow a Windows NT computer to act as a powerful Internet client using the extensive internetworking components with public-domain viewers and applications to access Internet resources.

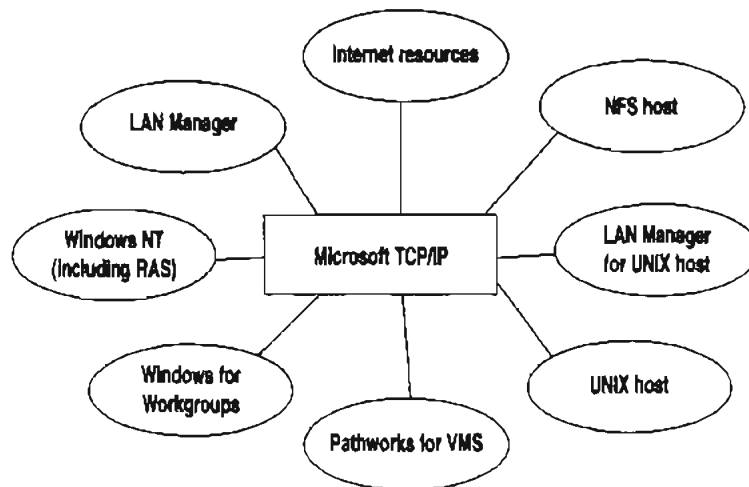


**Tip** Public-domain Windows-based utilities such as LPR and Gopher can be obtained on the Internet via <ftp:cica.indiana.edu> in the `/pub/win3/nt` or `/pub/win3/winsoc` directory, or via the same directories on <ftp.cdrom.com>.

## TCP/IP for Heterogeneous Networking

Because most modern operating systems (in addition to Windows NT) support TCP/IP protocols, an internetwork with mixed system types can share information using simple networking applications and utilities. With TCP/IP as a connectivity protocol, Windows NT can communicate with many non-Microsoft systems, including:

- Internet hosts
- Apple® Macintosh® systems
- IBM® mainframes
- UNIX systems
- Open VMS® systems
- Printers with network adapters connected directly to the network



### Microsoft TCP/IP Connectivity

Microsoft TCP/IP provides a framework for interoperable heterogeneous networking. The modular architecture of Windows NT networking with its transport-independent services contributes to the strength of this framework. For example, Windows NT supports these transport protocols, among many others:

- IPX/SPX for use in NetWare environments, using the Microsoft NWLink transport. Besides providing interoperability with NetWare networks, IPX/SPX is a fast LAN transport for Windows networking as well.
- TCP/IP for internetworks based on IP technologies. TCP/IP is the preferred transport for internetworks and provides interoperability with UNIX and other TCP/IP-based networks.

- NetBEUI as the protocol for local area networking on smaller networks and compatibility with existing LAN Manager and Lan Server networks.
- AppleTalk<sup>®</sup> for connecting to and sharing resources with Macintosh systems.

Other transport protocols provided by third-party vendors, such as DECnet™ and OSI, can also be used by Windows NT networking services.

Windows NT provides standard network programming interfaces through the Windows Sockets, RPC, and NetBIOS interfaces. Developers can take advantage of this heterogeneous client-server platform to create custom applications that will run on any system in the enterprise. An example of such a service is Microsoft SQL Server, which uses Windows Sockets 1.1 to provide access to NetWare, MS-DOS-based, Windows NT, and UNIX clients.

## Using TCP/IP with Third-Party Software

TCP/IP is a common denominator for heterogeneous networking, and Windows Sockets is a standard used by application developers. Together they provide a framework for cross-platform client-server development. TCP/IP-aware applications from vendors that comply with the Windows Sockets standards can run over virtually any TCP/IP implementation.

The Windows Sockets standard ensures compatibility with Windows-based TCP/IP utilities developed by more than 30 vendors. This includes third-party applications for the X Window System, sophisticated terminal emulation software, NFS, electronic mail packages, and more. Because Windows NT offers compatibility with 16-bit Windows Sockets, applications created for Windows 3.x Windows Sockets will run over Windows NT without modification or recompilation.

For example, third-party applications for X Window provide strong connectivity solutions by means of X Window servers, database servers, and terminal emulation. With such applications, a Windows NT computer can work as an X Window server platform while retaining compatibility with applications created for Windows NT, Windows 3.1, and MS-DOS on the same system. Other third-party software includes X Window client libraries for Windows NT, which allow developers to write X Window client applications on Windows NT that can be run and displayed remotely on X Window server systems.

The Windows Sockets API is a networking API used by programmers creating applications for both the Microsoft Windows NT and Windows operating systems. Windows Sockets is an open standard that is part of the Microsoft Windows Open System Architecture (WOSA) initiative. It is a public specification based on Berkeley UNIX sockets, which means that UNIX applications can be quickly ported to Microsoft Windows and Windows NT. Windows Sockets provides a single standard programming interface supported by all the major vendors implementing TCP/IP for Windows systems.



The Windows NT TCP/IP utilities use Windows Sockets, as do 32-bit TCP/IP applications developed by third parties. Windows NT also uses the Windows Sockets interface to support Services for Macintosh and IPX/SPX in NWLink. Under Windows NT, 16-bit Windows-based applications created under the Windows Sockets standard will run without modification or recompilation. Most TCP/IP users will use programs that comply with the Windows Sockets standard, such as **ftp** or **telnet** or third-party applications.

The Windows Sockets standard allows a developer to create an application with a single common interface and a single executable that can run over many of the TCP/IP implementations provided by vendors. The goals for Windows Sockets are the following:

- Provide a familiar networking API to programmers using Windows NT, Windows for Workgroups, or UNIX
- Offer binary compatibility between vendors for heterogeneous Windows-based TCP/IP stacks and utilities
- Support both connection-oriented and connectionless protocols

Typical Windows Sockets applications include graphic connectivity utilities, terminal emulation software, Simple Mail Transfer Protocol (SMTP) and electronic mail clients, network printing utilities, SQL client applications, and corporate client-server applications.

If you are interested in developing a Windows Sockets application, specifications for Windows Sockets are available on the Internet from <ftp.microsoft.com>, on CompuServe® in the MSL library, and in the Microsoft Win32® Software Developers Kit.

- ▶ **To get a copy of the Windows Sockets specification via anonymous FTP**
  1. Make sure you have write permission in your current working directory.
  2. Start **ftp** and connect to **ftp.microsoft.com** (or **198.105.232.1**).
  3. Log on as **anonymous**.
  4. Type your electronic mail address for the *password*.
  5. Type **cd \advsys\winsock\spec11** and press ENTER.
  6. Use the **dir** command to see the list of available file types. If you want binary data such as in the Microsoft Word version, type **bin** and press ENTER.
  6. Determine the file with the format you want [for example, ASCII (.TXT), PostScript® (.PS), or Microsoft Word (.DOC)], and then type **get winsock.ext** where *ext* is the format that you want, such as **winsock.doc** for the Microsoft Word version.

► **To get a copy of the Windows Sockets specification from CompuServe**

1. Type `go msl` and press ENTER.
2. Browse using the keywords **windows sockets**.
3. Choose the file with the format you want [ASCII (.TXT), PostScript (.PS), or Microsoft Word for Windows (.DOC)], and then type `get winsock.ext`.

There is also an electronic mailing list designed for discussion of Windows Sockets programming.

► **To subscribe to the Windows Sockets mailing list**

- Send electronic mail to `listserv@sunsite.unc.edu` with a message body that contains **subscribe winsock user's-email-address**.

You can use the same procedure to subscribe to two mailing lists called **winsock-hackers** and **winsock-users**.



## CHAPTER 2

# Installing and Configuring Microsoft TCP/IP and SNMP



This chapter explains how to install TCP/IP and the SNMP service for Windows NT and how to configure the protocols on your computer.

The TCP/IP protocol family can be installed as part of Custom Setup when you install Windows NT, following the steps described in this chapter. Also, if you upgrade to a new version of Windows NT, Setup automatically installs the new TCP/IP protocol and preserves your previous TCP/IP settings. This chapter assumes that Windows NT has been successfully installed on your computer but TCP/IP has not been installed.

The following topics appear in this chapter:

- Before installing Microsoft TCP/IP
- Installing TCP/IP
- Configuring TCP/IP
- Configuring TCP/IP to use DNS
- Configuring advanced TCP/IP options
- Configuring SNMP
- Removing TCP/IP components
- Configuring Remote Access Service (RAS) for use with TCP/IP



You must be logged on as a member of the Administrators group to install and configure all elements of TCP/IP.

## Before Installing Microsoft TCP/IP

---

**Important** The values that you will use for manually configuring TCP/IP and SNMP must be supplied by the network administrator.

---

Check with your network administrator to find out the following information before you install Microsoft TCP/IP on a Windows NT computer:

- Whether you can use Dynamic Host Configuration Protocol (DHCP) to configure TCP/IP. You can choose this option if a DHCP server is installed on your internetwork. You cannot choose this option if this computer will be a DHCP server. For information, see “Using Dynamic Host Configuration Protocol” later in this chapter.
- Whether this computer will be a DHCP server. This option is available only for Windows NT Server. For information, see Chapter 4, “Installing and Configuring DHCP Servers.”
- Whether this computer will be a Windows Internet Name Service (WINS) server. This option is available only for Windows NT Server. For information, see Chapter 5, “Installing and Configuring WINS Servers.”
- Whether this computer will be a WINS proxy agent. For information, see “Windows Internet Name Service and Broadcast Name Resolution” in Chapter 3, “Networking Concepts for TCP/IP.”

If you cannot use DHCP for automatic configuration, you need to obtain these values from the network administrator so you can configure TCP/IP manually:

- The IP address and subnet mask for each network adapter card installed on the computer. For information, see “IP Addressing” in Chapter 3.
- The IP address for the default local gateways (IP routers).
- Whether your computer will use Domain Name System (DNS) and, if so, the IP addresses and DNS domain name of the DNS servers on the internetwork. For information, see “Domain Name System Addressing” in Chapter 3.
- The IP addresses for WINS servers, if WINS servers are available on your network.

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer, as described in “Configuring SNMP” later in this chapter:

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

## Installing TCP/IP



You must be logged on as a member of the Administrators group for the local computer to install and configure TCP/IP.

### ► To install Microsoft TCP/IP on a Windows NT computer

1. Start the Network option in Control Panel.
2. In the Network Settings dialog box, choose the Add Software button.
3. In the Add Network Software dialog box, select TCP/IP Protocol And Related Components from the Network Software list, and then choose the Continue button.
4. In the Windows NT TCP/IP Installation Options dialog box, check the options for the TCP/IP components you want to install, as described in the table that follows this procedure, and then choose the Continue button.

If any TCP/IP elements have been installed previously, these are dimmed and not available in the Windows NT TCP/IP Installation Options dialog box.

You can read the hint bar at the bottom of each TCP/IP dialog box for information about a selected item, or choose the Help button to get detailed online information while you are installing or configuring TCP/IP.

5. Windows NT Setup displays a message asking for the full path to the Windows NT distribution files. Provide the appropriate location, and choose the Continue button.

You can specify a drive letter for floppy disks, a CD-ROM drive, or a shared network directory, or you can specify the Universal Naming Convention (UNC) path name for a network resource, such as \\NTSETUPMASTER.

All necessary files are copied to your hard disk.

---

**Note** If you are installing from floppy disks, Windows NT Setup may request disks more than once. This is normal and is not an error condition.

---

6. If you selected the options for installing the SNMP and FTP Server services, you are automatically asked to configure these services. Follow the directions provided in the online Help for these dialog boxes. For additional details, see "Configuring SNMP" later in this chapter, and see also Chapter 7, "Using the Microsoft FTP Server Service."
7. In the Network Settings dialog box, choose OK.

If you checked the Enable Automatic DHCP Configuration option and a DHCP server is available on your network, all configuration settings for TCP/IP are completed automatically, as described in "Using Dynamic Host Configuration Protocol" later in this chapter.

If you did not check the Enable Automatic DHCP Configuration option, continue with the configuration procedures described in "Configuring TCP/IP Manually" later in this chapter. TCP/IP must be configured in order to operate.

If you checked the DHCP Server Service or WINS Server Service options, you must complete the configuration steps described in Chapters 4 and 5.

#### Windows NT TCP/IP Installation Options

Option	Usage
TCP/IP Internetworking	Includes the TCP/IP protocol, NetBIOS over TCP/IP and Windows Sockets interfaces, and the TCP/IP diagnostic utilities. These elements are installed automatically.
Connectivity Utilities	Installs the TCP/IP utilities. Select this option to install the connectivity utilities described in Chapter 11, "Utilities Reference."
SNMP Service	Installs the SNMP service. Select this option to allow this computer to be administered remotely using management tools such as Sun Net Manager or HP Open View. This option also allows you to monitor statistics for the TCP/IP services and WINS servers using Performance Monitor, as described in Chapter 8, "Using Performance Monitor with TCP/IP Services."

**Windows NT TCP/IP Installation Options** *(continued)*

Option	Usage
TCP/IP Network Printing Support	<p>Allows this computer to print directly over the network using TCP/IP. Select this option if you want to print to UNIX print queues or TCP/IP printers that are connected directly to the network, as described in Chapter 9, "Internetwork Printing with TCP/IP."</p> <p>This option must be installed if you want to use the Lpdsvr service so that UNIX computers can print to Windows NT printers.</p>
FTP Server Service	<p>Allows files on this computer to be shared over the network with remote computers that support FTP and TCP/IP (especially non-Microsoft network computers). Select this option if you want to use TCP/IP to share files with other computers, as described in Chapter 7, "Using the Microsoft FTP Server Service."</p>
Simple TCP/IP Services	<p>Provides the client software for the Character Generator, Daytime, Discard, Echo, and Quote of the Day services. Select this option to allow this computer to respond to requests from other systems that support these protocols.</p>
DHCP Server Service	<p>Installs the server software to support automatic configuration and addressing for computers using TCP/IP on your internetwork. This option is available only for Windows NT Server. Select this option if this computer is to be a DHCP Server, as described in Chapter 4, "Installing and Configuring DHCP Servers."</p> <p>If you select this option, you must manually configure the IP address, subnet mask, and default gateway for this computer.</p>
WINS Server Service	<p>Installs the server software to support WINS, a dynamic name resolution service for computers on a Windows internetwork. This option is available only for Windows NT Server. Select this option if this computer is to be installed as a primary or secondary WINS server, as described in Chapter 5, "Installing and Configuring WINS Servers."</p> <p>Do not select this option if this computer will be a WINS proxy agent.</p>
Enable Automatic DHCP Configuration	<p>Turns on automatic configuration of TCP/IP parameters for this computer. Select this option if there is a DHCP server on your internetwork to support dynamic host configuration. This is the preferred method for configuring TCP/IP on most Windows NT computers.</p> <p>This option is not available if the DHCP Server Service or WINS Server Service option is selected.</p>



► **To configure TCP/IP using DHCP**

1. Make sure the Enable Automatic DHCP Configuration option is checked in either the Windows NT TCP/IP Installation Options dialog box or the TCP/IP Configuration dialog box.
2. When you restart the computer after completing TCP/IP installation, the DHCP server automatically provides the correct configuration information for your computer.

If you subsequently attempt to configure TCP/IP in the Network Settings dialog box, the system will warn you that any manual settings will override the automatic settings provided by DHCP. As a general rule, you should not change the automatic settings unless you specifically want to override a setting provided by DHCP. For detailed information about DHCP, see “Dynamic Host Configuration Protocol” in Chapter 3, “Networking Concepts for TCP/IP.”

## Configuring TCP/IP Manually

After the Microsoft TCP/IP protocol software is installed on your computer, you must manually provide valid addressing information if you are installing TCP/IP on a DHCP server or if you cannot use automatic DHCP configuration.



You must be logged on as a member of the Administrators group for the local computer to configure TCP/IP.

---

**Caution** Be sure to use the values for IP addresses and subnet masks that are supplied by your network administrator to avoid duplicate addresses. If duplicate addresses do occur, this can cause some computers on the network to function unpredictably. For more information, see “IP Addressing” in Chapter 3, “Networking Concepts for TCP/IP.”

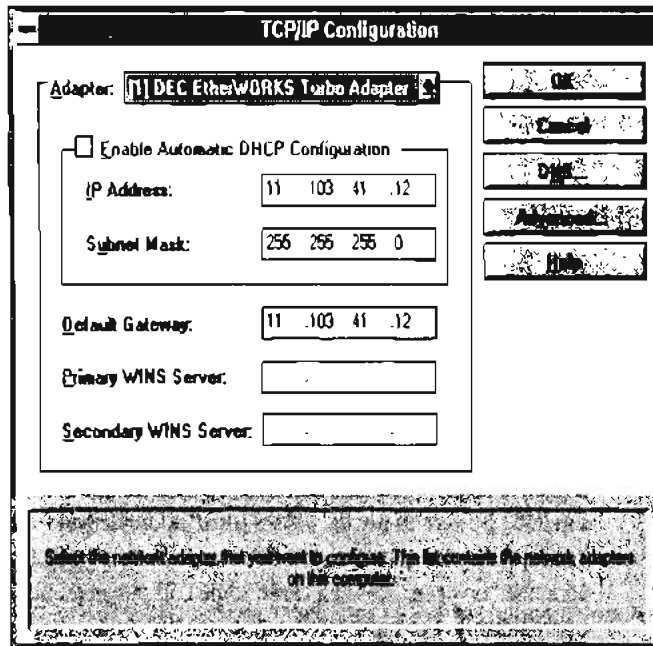
---

► To manually configure the TCP/IP protocol

1. When you are installing TCP/IP, the Microsoft TCP/IP Configuration dialog box appears automatically when you choose the OK button in the Network Settings dialog box after completing all options in the Windows NT TCP/IP Installation Options dialog box.

–Or–

If you are reconfiguring TCP/IP, start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select TCP/IP Protocol, and choose the Configure button.



2. In the Adapter list of the TCP/IP Configuration dialog box, select the network adapter for which you want to set IP addresses.

The Adapter list contains all network adapters to which IP is bound on this computer. This list includes all adapters installed on this computer.

You must set specific IP addressing information for each bound adapter with correct values provided by the network administrator. The bindings for a network adapter determine how network protocols and other layers of network software work together.

3. For each bound network adapter, type values in the IP Address and Subnet Mask boxes.

- The value in the IP Address box identifies the IP address for your local computer or, if more than one network card is installed in the computer, for the network adapter card selected in the Adapter box.
- The value in the Subnet Mask box identifies the network membership for the selected network adapter and its host ID. This allows the computer to separate the IP address into host and network IDs. The subnet mask defaults to an appropriate value, as shown in the following list:

Address class	Range of first octet in IP address	Subnet mask
Class A	1–126	255.0.0.0
Class B	128–191	255.255.0.0
Class C	192–223	255.255.255.0

4. For each network adapter on the computer, type the correct IP address value in the Default Gateway box, as provided by the network administrator.

This value specifies the IP address of the default gateway (or IP router) used to forward packets to other networks or subnets. This value should be the IP address of your local gateway.

This parameter is required only for systems on internetworks. If this parameter is not provided, IP functionality will be limited to the local subnet unless a route is specified with the TCP/IP route utility, as described in Chapter 11, “Utilities Reference.”

If your computer has multiple network cards, additional default gateways can be added using the Advanced Microsoft TCP/IP Configuration dialog box, as described later in this chapter.

5. If there are WINS servers installed on your network and you want to use WINS in combination with broadcast name queries to resolve computer names, type IP addresses in the boxes for the primary and, optionally, the secondary WINS servers. The network administrator should provide the correct values for these parameters. These are global values for the computer, not just individual adapters.

If an address for a WINS server is not specified, this computer will use name query broadcasts (the b-node mode for NetBIOS over TCP/IP) plus the local LMHOSTS file to resolve computer names to IP addresses. Broadcast resolution is limited to the local network.

---

**Note** WINS name resolution is enabled and configured automatically for a computer that is configured with DHCP.

On a WINS server, NetBIOS over TCP/IP (NETBT.SYS) uses WINS on the local computer as the primary name server, regardless of how name resolution may be configured. Also, NetBIOS over TCP/IP binds to the first IP address on a network adapter and ignores any additional addresses.

---

For overview information about name resolution options, see “Name Resolution for Windows Networking” in Chapter 3. For detailed information about installing and configuring WINS servers, see Chapter 5.

6. If you want to configure the advanced TCP/IP options for multiple gateways and other items, choose the Advanced button, and continue with the configuration procedure, as described in “Configuring Advanced TCP/IP Options” later in this chapter.
7. If you want to use DNS for host name resolution, choose the DNS button, and continue with the configuration procedure, as described in the next section.
8. If you do not want to configure DNS or advanced options, or if you have completed the other configuration procedures, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

Microsoft TCP/IP has been configured. If you are installing TCP/IP for the first time, you must restart the computer for the configuration to take effect. If you are changing your existing configuration, you do not have to restart your computer.

After TCP/IP is installed, the `\systemroot\SYSTEM32\DRIVERS\ETC` directory contains a default HOSTS file and a sample LMHOSTS.SAM file. The network administrator may require that replacement HOSTS and LMHOSTS files be used instead of these default files.

## Configuring TCP/IP to Use DNS

Although TCP/IP uses IP addresses to identify and reach computers, users typically prefer to use computer names. DNS is a naming service generally used in the UNIX networking community to provide standard naming conventions for IP workstations. Windows Sockets applications and TCP/IP utilities, such as `ftp` and `telnet`, can also use DNS in addition to the HOSTS file to find systems when connecting to foreign hosts or systems on your network.

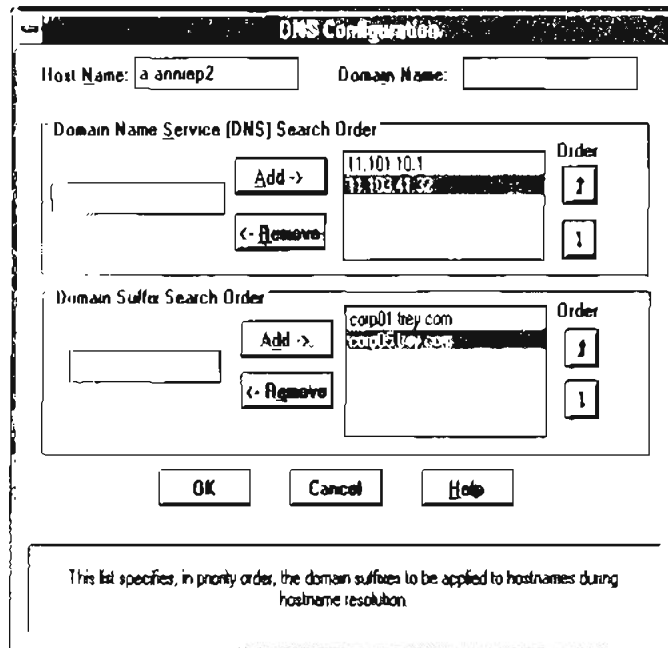
Contact the network administrator to find out whether you should configure your computer to use DNS. Usually you will use DNS if you are using TCP/IP to communicate over the Internet or if your private internetwork uses DNS to distribute host information. For information, see "Domain Name System Addressing" in Chapter 3.

Microsoft TCP/IP includes DNS client software for resolving Internet or UNIX system names. Microsoft Windows networking provides dynamic name resolution for NetBIOS computer names via WINS servers and NetBIOS over TCP/IP.

DNS configuration is global for all network adapters installed on a computer.

### ► To configure TCP/IP DNS connectivity

1. Start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select TCP/IP Protocol, and then choose the Configure button.
2. In the TCP/IP Configuration dialog box, choose the DNS button.



3. In the DNS Configuration dialog box, you can, optionally, type a name in the Host Name box (usually your computer name).

The name can be any combination of A–Z letters, 0–9 numerals, and the hyphen (-) plus the period (.) character used as a separator. By default, this value is the Windows NT computer name, but the network administrator can assign another host name without affecting the computer name.

---

**Note** Some characters that can be used in Windows NT computer names, particularly the underscore, cannot be used in host names.

---

The host name is used to identify the local computer by name for authentication by some utilities. Other TCP/IP-based utilities, such as `rexec`, can use this value to learn the name of the local computer. Host names are stored on DNS servers in a table that maps names to IP addresses for use by DNS.

4. Optionally, type a name in the Domain Name box. This is usually an organization name followed by a period and an extension that indicates the type of organization, such as `microsoft.com`.

The name can be any combination of A–Z letters, 0–9 numerals, and the hyphen (-) plus the period (.) character used as a separator.

This DNS Domain Name is used with the host name to create a fully qualified domain name (FQDN) for the computer. The FQDN is the host name followed by a period (.) followed by the domain name. For example, this could be `corp01.research.trey.com`, where `corp01` is the host name and `research.trey.com` is the domain name. During DNS queries, the local domain name is appended to short names.

---

**Note** A DNS domain is not the same as a Windows NT or LAN Manager domain.

---

5. In the Domain Name System (DNS) Search Order box, type the IP address of the DNS server that will provide name resolution. Then choose the Add button to move the IP address to the list on the right. The network administrator should provide the correct values for this parameter.

You can add up to three IP addresses for DNS servers. The servers running DNS will be queried in the order listed. To change the order of the IP addresses, select an IP address to move, and then use the up- and down-arrow buttons. To remove an IP address, select it and choose the Remove button.

- In the Domain Suffix Search Order box, type the domain suffixes to add to your domain suffix search list, and then choose the Add button.

This list specifies the DNS domain suffixes to be appended to host names during name resolution. You can add up to six domain suffixes. To change the search order of the domain suffixes, select a domain name to move, and use the up- and down-arrow buttons. To remove a domain name, select it and choose the Remove button.

- When you are done setting DNS options, choose the OK button.
- When the TCP/IP Configuration dialog box reappears, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

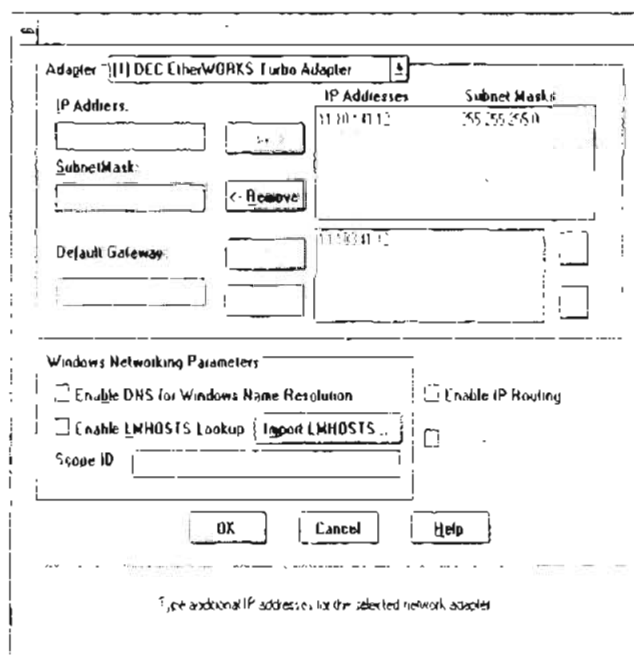
The settings take effect after you restart the computer.

## Configuring Advanced TCP/IP Options

If your computer has multiple network adapters connected to different networks using TCP/IP, you can choose the Advanced button in the TCP/IP Configuration dialog box to configure options for the adapters or to configure alternate default gateways.

### ► To configure or reconfigure advanced TCP/IP options

- Start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select TCP/IP Protocol and choose the Configure button.
- In the TCP/IP Configuration dialog box, choose the Advanced button.



3. In the Adapter box of the Advanced Microsoft TCP/IP Configuration dialog box, select the network adapter for which you want to specify advanced configuration values. The IP address and default gateway settings in this dialog box are defined only for the selected network adapter.
4. In the IP Address and SubnetMask boxes, type an additional IP address and subnet mask for the selected adapter. Then choose the Add button to move the IP address to the list on the right. The network administrator should provide the correct values for this parameter.

Optionally, if your network card uses multiple IP addresses, repeat this process for each additional IP address. You can specify up to five additional IP addresses and subnet masks for identifying the selected network adapter. This can be useful for a computer connected to one physical network that contains multiple logical IP networks.

5. In the Default Gateway box, type the IP address for an additional gateway that the selected adapter can use. Then choose the Add button to move the IP address to the list on the right. Repeat this process for each additional gateway. The network administrator should provide the correct values for this parameter.

This list specifies up to five additional default gateways for the selected network adapter.

To change the priority order for the gateways, select an address to move and use the up- or down-arrow buttons. To remove a gateway, select it and choose the Remove button.

6. If you want to use DNS for DNS name resolution on Windows networks, check the Enable DNS For Windows Name Resolution option.

If this option is checked, the system finds the DNS server by using the IP address specified in the DNS Configuration dialog box, as described earlier in this chapter. Checking this option enables DNS name resolution for use by Windows networking applications.

7. If you want to use the LMHOSTS file for NetBIOS name resolution on Windows networks, check the Enable LMHOSTS Lookup option. If you already have a configured LMHOSTS file, choose the Import LMHOSTS button and specify the directory path for the LMHOSTS file you want to use. By default, Windows NT uses the LMHOSTS file found in `\systemroot\SYSTEM32\DRIVERS\ETC`.

For any method of name resolution used in a Windows NT network, the LMHOSTS file is consulted last after querying WINS or using broadcasts, but before DNS is consulted.



8. In the Scope ID box, type the computer's scope identifier, if required on an internetwork that uses NetBIOS over TCP/IP.

To communicate with each other, all computers on a TCP/IP internetwork must have the same scope ID. Usually this value is left blank. A scope ID may be assigned to a group of computers that will communicate only with each other and no other systems. Such computers can find each other if their scope IDs are identical. Scope IDs are used only for communication based on NetBIOS over TCP/IP.

The network administrator should provide the correct value, if required.

9. To turn on static IP routing, check the Enable IP Routing option.

This option allows this computer to participate with other static routers on a network. You should check this option if you have two or more network cards and your network uses static routing, which also requires the addition of static routing tables. For information about creating static routing tables, see the *route* utility in Chapter 11, "Utilities Reference."

This option is not available if your computer has only one network adapter and one IP address. Also, this option does not support routers running the Routing Information Protocol (RIP).

10. If you want this computer to be used to resolve names based on the WINS database, check the Enable WINS Proxy Agent option.

This option allows the computer to answer name queries for remote computers, so other computers configured for broadcast name resolution can benefit from the name resolution services provided by a WINS server.

This option is available only if you entered a value for a primary WINS server in the TCP/IP Configuration dialog box, as described in "Configuring TCP/IP" earlier in this chapter. However, the proxy agent cannot be run on a computer that is also a WINS server.

Consult with the network administrator to determine whether your computer should be configured as a WINS proxy agent, as only a few computers on each subnetwork should be configured for this feature.

11. When you are done setting advanced options, choose the OK button. When the TCP/IP Configuration dialog box reappears, choose the OK button. When the Network Settings dialog box reappears, choose the OK button to complete advanced TCP/IP configuration.

You must restart the computer for the changes to take effect.

## Configuring SNMP

The SNMP service is installed when you check the SNMP Service option in the Windows NT TCP/IP Installation Options dialog box. After the SNMP service software is installed on your computer, you must configure it with valid information for SNMP to operate.



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

The SNMP configuration information identifies communities and trap destinations.

- A *community* is a group of hosts to which a Windows NT computer running the SNMP service belongs. You can specify one or more communities to which the Windows NT computer using SNMP will send traps. The community name is placed in the SNMP packet when the trap is sent.

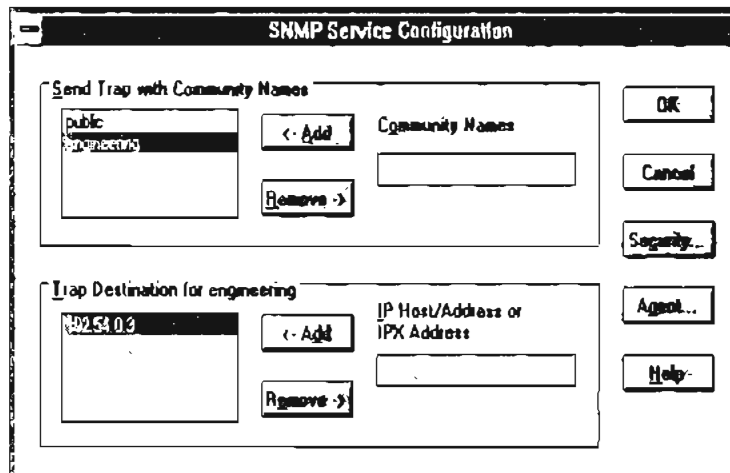
When the SNMP service receives a request for information that does not contain the correct community name and does not match an accepted host name for the service, the SNMP service can send a trap to the trap destination(s), indicating that the request failed authentication.

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

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

### ► To configure the SNMP service

1. Start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select SNMP Service, and choose the Configure button. The SNMP Service Configuration dialog box appears.



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

Typically, all hosts belong to public, which is the standard name for the common community of all hosts. To delete an entry in the list, select it and choose the Remove button.

---

**Note** Community names are case sensitive.

---

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

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

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

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

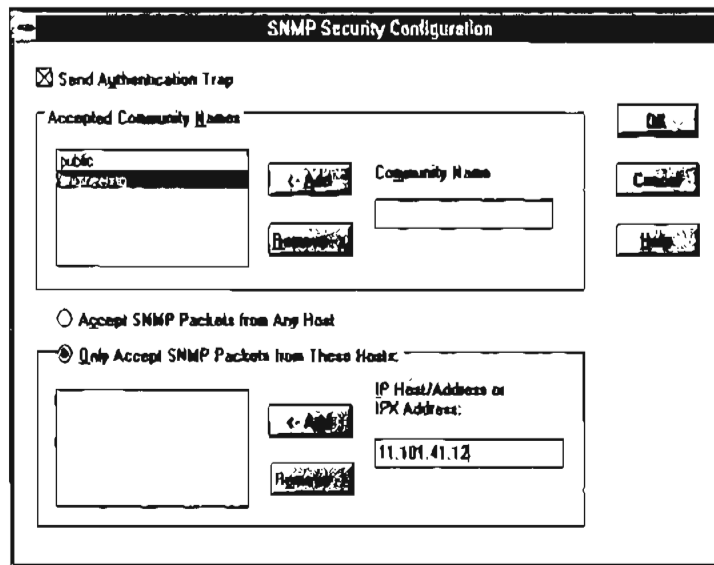
The Microsoft SNMP service has been configured and is ready to start. It is not necessary to reboot the computer.

## Configuring SNMP Security

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

► **To configure SNMP security**

1. Start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select SNMP Service and choose the Configure button.
2. In the SNMP Service Configuration dialog box, choose the Security button.



3. If you want to send a trap for failed authentications, select the Send Authentication Trap check box in the SNMP Security Configuration dialog box.

4. In the Community Name box, type the community names you will accept requests from. Choose the Add button after typing each name to move the name to the Accepted Community Names list on the left.

A host must belong to a community that appears on this list for the SNMP service to accept requests from that host. Typically, all hosts belong to public, which is the standard name for the common community of all hosts. To delete an entry in the list, select it and choose the Remove button.

5. Select an option to specify whether to accept SNMP packets from any host or from only specified hosts.
  - If the Accept SNMP Packets From Any Host option is selected, no SNMP packets are rejected on the basis of source host ID. The list of hosts under Only Accept SNMP Packets From These Hosts has no effect.
  - If the Only Accept SNMP Packets From These Hosts option is selected, SNMP packets will be accepted only from the hosts listed. In the IP Host/Address Or IPX Address box, type the host names, IP addresses, or IPX addresses of the hosts from which you will accept requests. Then choose the Add button to move the host name or IP address to the list box on the left. To delete an entry in the list, select it and choose the Remove button.
6. Choose the OK button. The SNMP Service Configuration dialog box reappears. To specify Agent information (comments about the user, location, and services), choose the Agent button. Continue with the configuration procedure, as described in the next section.
7. After you complete all procedures, choose the OK button. When the Network Settings dialog box reappears, choose the OK button.

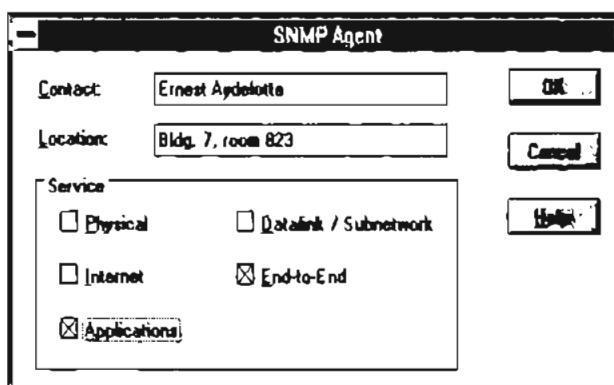
The Microsoft SNMP service and SNMP security have been configured and are ready to start. You do not need to reboot the computer.

## Configuring SNMP Agent Information

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

### ► To configure SNMP agent information

1. Start the Network option in Control Panel to display the Network Settings dialog box. In the Installed Network Software list box, select SNMP Service and choose the Configure button.
2. In the SNMP Service Configuration dialog box, choose the Agent button.



3. In the SNMP Agent dialog box, type the computer user's name in the Contact box and the computer's physical location in the Location box. These are comments that will be used as text and cannot include embedded control characters.
4. Select the services to report in the Service box. Check all boxes that indicate network capabilities provided by your Windows NT computer. SNMP must have this information to manage the enabled services.

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

Option	Meaning
Physical	Select this option if this Windows NT computer manages any physical TCP/IP device, such as a repeater.
DataLink/Subnetwork	Select this option if this Windows NT computer manages a TCP/IP subnetwork or datalink, such as a bridge.

---

Option	Meaning
Internet	Select this option if this Windows NT computer acts as an IP gateway.
End-to-End	Select this option if this Windows NT computer acts as an IP host. This option should be selected for all Windows NT installations.
Applications	Select this option if this Windows NT computer includes any applications that use TCP/IP, such as electronic mail. This option should be selected for all Windows NT installations.

5. Choose the OK button.
6. When the SNMP Service Configuration dialog box reappears, choose the OK button. When the Network Settings dialog box reappears, choose the OK button. SNMP is now ready to operate without rebooting the computer.

## Removing TCP/IP Components

If you want to remove the TCP/IP protocols or any of the services installed on a computer, use the Network option in Control Panel to remove it.

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

### ► To remove any TCP/IP component

1. In Control Panel, choose the Network option.
2. In the Installed Network Software list in the Network Settings dialog box, select the component that you want to remove.
3. Choose the Remove button.

## Configuring RAS for Use with TCP/IP

Windows NT users who install Remote Access Service (RAS) for remote networking maintain all the benefits of TCP/IP networking, including access to the WINS and DNS capabilities of Microsoft TCP/IP. RAS clients can be configured to use Point to Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) to allow TCP/IP dial-up support for existing TCP/IP internetworks and the Internet. When PPP is configured on a Windows NT Remote Access server, it can function as a router for RAS clients. SLIP client software is provided to support older implementations; it does not support multiple protocols.

As with all network services, you install RAS by using the Network option in Control Panel. During RAS installation and configuration, you can specify the network protocol settings to use for RAS connections, which also allows you to specify TCP/IP configuration settings. When the network administrator installs a Microsoft RAS server, IP addresses are reserved for use by RAS clients.

Users with RAS client computers can use the Remote Access program to enter and maintain names and telephone numbers of remote networks. RAS clients can connect to and disconnect from these networks through the Remote Access program. You can also use the Remote Access Phone Book application to select the network protocols to use for a specific Phone Book entry. If TCP/IP is installed, the Phone Book automatically selects TCP/IP over PPP as the protocol.

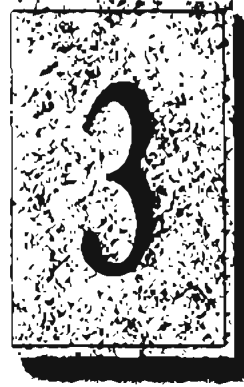
If a RAS client computer has a serial COM port, you can use the Remote Access Phone Book application to configure SLIP for use with a selected Phone Book entry. If you configure a RAS client computer to use the SLIP option, when you dial in for a connection to the selected Phone Book entry, the Terminal screen appears, and you can begin an interactive session with a SLIP server. When you use SLIP, Remote Access Phone Book bypasses user authentication. You will not be asked for a username and password.

For complete information about setting up RAS servers and clients and using RAS with Windows NT, see *Windows NT Server Remote Access Service*.



## CHAPTER 3

# Networking Concepts for TCP/IP



This chapter describes how TCP/IP fits in the Windows NT network architecture and explains the various components of the Internet Protocol suite and IP addressing. As part of the discussion on name resolution in Windows networking, this chapter also describes NetBIOS over TCP/IP and Domain Name System (DNS). For additional information about these topics, see the books listed in "Finding More Information" in "Welcome."

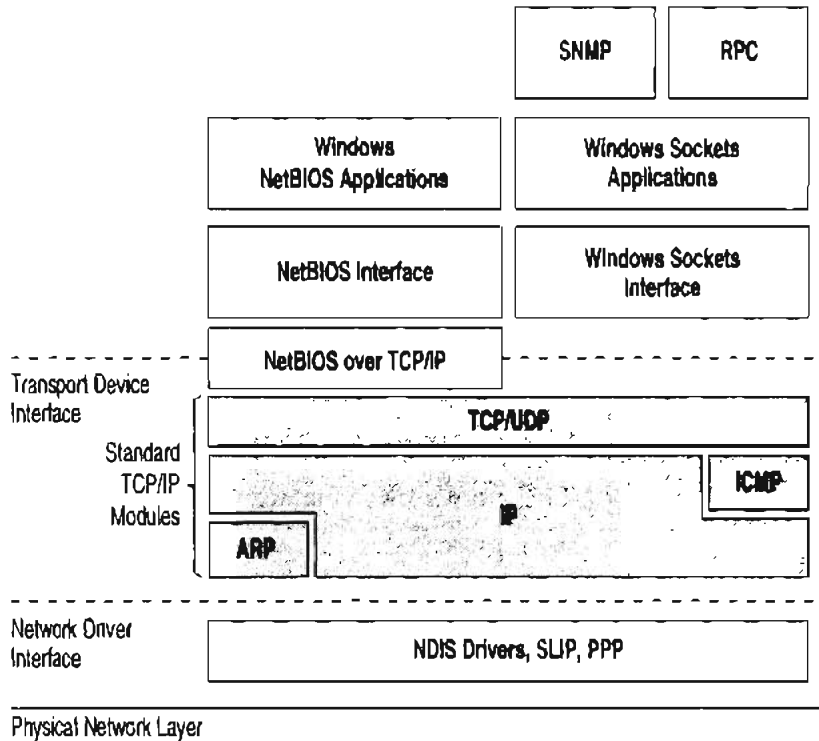
This chapter also provides conceptual information about two key features for Microsoft TCP/IP: Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS).

The following topics appear in this chapter:

- TCP/IP and Windows NT networking
- Internet protocol suite
- IP addressing
- Name resolution for Windows networking
- SNMP

## TCP/IP and Windows NT Networking

The architecture of the Microsoft Windows NT operating system with integrated networking is protocol-independent. This architecture, illustrated in the following figure, provides Windows NT file, print, and other services over any network protocol that uses exports from the TDI interface. The protocols package network requests for applications in their respective formats and send the requests to the appropriate network adapter via the *network device interface specification* (NDIS) interface. The NDIS specification allows multiple network protocols to reside over a wide variety of network adapters and media types.



### Architectural Model of Windows NT with TCP/IP

Under the Windows NT transport-independent architecture, TCP/IP is a protocol family that can be used to offer Windows networking capabilities. The TCP/IP protocol gives Windows NT, Windows for Workgroups, and LAN Manager computers transparent access to each other and allows communication with non-Microsoft systems in the enterprise network.

## Internet Protocol Suite

TCP/IP refers to the Internet suite of protocols. It includes a set of standards that specify how computers communicate and gives conventions for connecting networks and routing traffic through the connections.

The Internet protocols are a result of a Defense Advanced Research Projects Agency (DARPA) research project on network interconnection in the late 1970s. It was mandated on all United States defense long-haul networks in 1983 but was not widely accepted until it was integrated with 4.2 Berkeley Software Distribution (BSD) UNIX. The popularity of TCP/IP is based on:

- Robust client-server framework. TCP/IP is an excellent client-server application platform, especially in wide-area network (WAN) environments.
- Information sharing. Thousands of academic, military, scientific, and commercial organizations share data, electronic mail, and services on the Internet using TCP/IP.
- General availability. Implementations of TCP/IP are available on nearly every popular computer operating system. Source code is widely available for many implementations. Vendors for bridges, routers, and network analyzers all offer support for the TCP/IP protocol suite within their products.

The following discussion introduces the components of the IP protocol suite. Some knowledge of the architecture and interaction between TCP/IP components is useful for both administrators and users, but most of the details discussed here are transparent when you are actually using TCP/IP.

## Transmission Control Protocol and Internet Protocol

Transmission Control Protocol (TCP) and Internet Protocol (IP) are only two members of the IP protocol suite. IP is a protocol that provides packet delivery for all other protocols within the TCP/IP family. IP provides a best-effort, connectionless delivery system for computer data. That is, IP packets are not guaranteed to arrive at their destination, nor are they guaranteed to be received in the sequence in which they were sent. The protocol's checksum feature confirms only the IP header's integrity. Thus, responsibility for the data contained within the IP packet (and the sequencing) is assured only by using higher-level protocols.

Perhaps the most common higher-level IP protocol is TCP. TCP supplies a reliable, connection-based protocol over (or encapsulated within) IP. TCP guarantees the delivery of packets, ensures proper sequencing of the data, and provides a checksum feature that validates both the packet header and its data for accuracy. In the event that the network either corrupts or loses a TCP/IP packet during transmission, TCP is responsible for retransmitting the faulty packet. This reliability makes TCP/IP the protocol of choice for session-based data transmission, client-server applications, and critical services such as electronic mail.

This reliability has a price. TCP headers require the use of additional bits to provide proper sequencing of information, as well as a mandatory checksum to ensure reliability of both the TCP header and the packet data. To guarantee successful data delivery, the protocol also requires the recipient to acknowledge successful receipt of data.

Such acknowledgments (or ACKs) generate additional network traffic, diminishing the level of data throughput in favor of reliability. To reduce the impact on performance, most hosts send an acknowledgment for every other segment or when an ACK timeout expires.

## User Datagram Protocol

If reliability is not essential, User Datagram Protocol (UDP), a TCP complement, offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like IP). Higher-level protocols or applications may provide reliability mechanisms in addition to UDP/IP. UDP data checksums are optional, providing a way to exchange data over highly reliable networks without unnecessarily consuming network resources or processing time. When UDP checksums are used, they validate both header and data. ACKs are also not enforced by the UDP protocol; this is left to higher-level protocols.

UDP also offers one-to-many service capabilities, because it can be either broadcast or multicast.

## Address Resolution Protocol and Internet Control Message Protocol

Two other protocols in the IP suite perform important functions, although these are not directly related to the transport of data: Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP). ARP and ICMP are maintenance protocols that support the IP framework and are usually invisible to users and applications.

IP packets contain both source and destination IP addresses, but the hardware address of the destination computer system must also be known. IP acquires a system's hardware address by broadcasting a special inquiry packet (an ARP *request packet*) containing the IP address of the system with which it is attempting to communicate. All of the ARP-enabled nodes on the local IP network detect these broadcasts, and the system that owns the IP address in question replies by sending its hardware address to the requesting computer system in an ARP reply packet. The hardware/IP address mapping is then stored in the requesting system's ARP cache for subsequent use. Because the ARP reply can also be broadcast to the network, it is likely that other nodes on the network can use this information to update their own ARP caches. (You can use the `arp` utility to view the ARP tables.)

ICMP allows two nodes on an IP network to share IP status and error information. This information can be used by higher-level protocols to recover from transmission problems or by network administrators to detect network trouble. Although ICMP packets are encapsulated within IP packets, they are not considered to be a higher-level protocol (ICMP is required in every TCP/IP implementation). The `ping` utility makes use of the ICMP *echo request* and *echo reply* packets to determine whether a particular IP node (computer system) on a network is functional. This is useful for diagnosing IP network or gateway failures.

## IP Addressing

A host is any device attached to the network that uses TCP/IP. To receive and deliver packets successfully between hosts, TCP/IP relies on three pieces of information that the user provides: IP address, subnet mask, and default gateway.

The network administrator provides each of these pieces of information for configuring TCP/IP on a computer. Windows NT users on networks with DHCP servers can take advantage of automatic system configuration and do not need to manually configure TCP/IP parameters. This section provides details about IP addresses, subnet masks, and IP gateways.

## IP Addresses

Every host interface, or node, on a TCP/IP network is identified by a unique IP address. This address is used to identify a host on a network; it also specifies routing information in an internetwork. The *IP address* identifies a computer as a 32-bit address that is unique across a TCP/IP network. An address is usually represented in dotted decimal notation, which depicts each octet (eight bits, or one byte) of an IP address as its decimal value and separates each octet with a period. An IP address looks like this:

102.54.94.97

---

**Important** Because IP addresses identify nodes on an interconnected network, each host on the internetwork must be assigned a unique IP address, valid for its particular network.

---

## Network ID and Host ID

Although an IP address is a single value, it contains two pieces of information: the network ID and the host (or system) ID for your computer.

- The *network ID* identifies a group of computers and other devices that are all located on the same logical network, which are separated or interconnected by routers. In internetworks (networks formed by a collection of local area networks), there is a unique network ID for each network.
- The *host ID* identifies your computer within a particular network ID. (A host is any device that is attached to the network and uses TCP/IP.)

Networks that connect to the public Internet must obtain an official network ID from the InterNIC to guarantee IP network ID uniqueness. The InterNIC can be contacted via electronic mail at [info@internic.net](mailto:info@internic.net) (for the United States, 1-800-444-4345 or, for Canada and overseas, 619-455-4600). Internet registration requests can be sent to [hostmaster@internic.net](mailto:hostmaster@internic.net). You can also use FTP to connect to [is.internic.net](http://is.internic.net), then log in as **anonymous**, and change to the /INFOSOURCE/FAQ directory.

After receiving a network ID, the local network administrator must assign unique host IDs for computers within the local network. Although private networks not connected to the Internet can choose to use their own network identifier, obtaining a valid network ID from InterNIC allows a private network to connect to the Internet in the future without reassigning addresses.

The Internet community has defined address *classes* to accommodate networks of varying sizes. Each network class can be discerned from the first octet of its IP address. The following table summarizes the relationship between the first octet of a given address and its network ID and host ID fields. It also identifies the total number of network IDs and host IDs for each address class that participates in the Internet addressing scheme. This sample uses w.x.y.z to designate the bytes of the IP address.

**IP Address Classes**

Class	w values <sup>1,2</sup>	Network ID	Host ID	Available networks	Available hosts per net
A	1–126	w	x.y.z	126	16,777,214
B	128–191	w.x	y.z	16,384	65,534
C	192–223	w.x.y	z	2,097,151	254

<sup>1</sup> Inclusive range for the first octet in the IP address.

<sup>2</sup> The address 127 is reserved for loopback testing and interprocess communication on the local computer; it is not a valid network address. Addresses 224 and above are reserved for special protocols (IGMP multicast and others), and cannot be used as host addresses.

A network host uses the network ID and host ID to determine which packets it should receive or ignore and to determine the scope of its transmissions (only nodes with the same network ID accept each other's IP-level broadcasts).

Because the sender's IP address is included in every outgoing IP packet, it is useful for the receiving computer system to derive the originating network ID and host ID from the IP address field. This is done by using subnet masks, as described in the following section.

**Subnet Masks**

Subnet masks are 32-bit values that allow the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID. Like an IP address, the value of a subnet mask is frequently represented in dotted decimal notation. Subnet masks are determined by assigning 1's to bits that belong to the network ID and 0's to the bits that belong to the host ID. Once the bits are in place, the 32-bit value is converted to dotted decimal notation, as shown in the following table.

**Default Subnet Masks for Standard IP Address Classes**

Address class	Bits for subnet mask	Subnet mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

The result allows TCP/IP to determine the host and network IDs of the local computer. For example, when the IP address is 102.54.94.97 and the subnet mask is 255.255.0.0, the network ID is 102.54 and the host ID is 94.97.

Although configuring a host with a subnet mask might seem redundant after examining the previous tables (since the class of a host is easily determined), subnet masks are also used to further segment an assigned network ID among several local networks.

For example, suppose a network is assigned the Class-B network address 144.100. This is one of over 16,000 Class-B addresses capable of serving more than 65,000 nodes. However, the worldwide corporate network to which this ID is assigned is composed of 12 international LANs with 75 to 100 nodes each. Instead of applying for 11 more network IDs, it is better to use subnetting to make more effective use of the assigned ID 144.100. The third octet of the IP address can be used as a subnet ID, to define the subnet mask 255.255.255.0. This splits the Class-B address into 254 subnets: 144.100.1 through 144.100.254, each of which can have 254 nodes. (Host IDs 0 and 255 should not be assigned to a computer; they are used as broadcast addresses, which are typically recognized by all computers.) Any 12 of these network addresses could be assigned to the international LANs in this example. Within each LAN, each computer is assigned a unique host ID, and they all have the subnet mask 255.255.255.0.

The preceding example demonstrates a simple (and common) subnet scheme for Class-B addresses. Sometimes it is necessary to segment only portions of an octet, using only a few bits to specify subnet IDs (such as when subnets exceed 256 nodes). Each user should check with the local network administrator to determine the network's subnet policy and the correct subnet mask. For all systems on the local network, the subnet mask must be the same for that network ID.

---

**Important** All computers on a logical network must use the same subnet mask and network ID; otherwise, addressing and routing problems can occur.

---

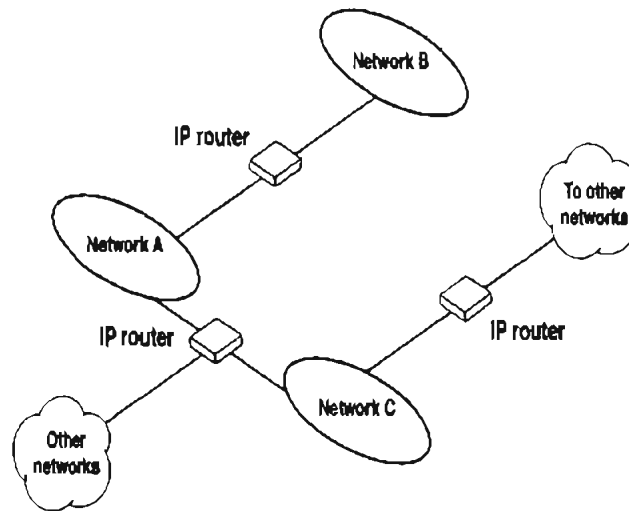
## Routing and IP Gateways

TCP/IP networks are connected by *gateways* (or routers), which have knowledge of the networks connected in the internetwork. Although each IP host can maintain static routes for specific destinations, usually the default gateway is used to find remote destinations. (The *default gateway* is needed only for computers that are part of an internetwork.)



When IP prepares to send a packet, it inserts the local (source) IP address and the destination address of the packet in the IP header and checks whether the network ID of the destination matches the network ID of the source. If they match, the packet is sent directly to the destination computer on the local network. If the network IDs do not match, the routing table is examined for static routes. If none are found, the packet is forwarded to the default gateway for delivery.

The default gateway is a computer connected to the local subnet and other networks that has knowledge of the network IDs for other networks in the internetwork and how to reach them. Because the default gateway knows the network IDs of the other networks in the internetwork, it can forward the packet to other gateways until the packet is eventually delivered to a gateway connected to the specified destination. This process is known as *routing*.



#### Internetwork Routing Through Gateways

On networks that are not part of an internetwork, IP gateways are not required. If a network is part of an internetwork and a system does not specify a default gateway (or if the gateway computer is not operating properly), only communication beyond the local subnet is impaired. Users can add static routes by using the `route` utility to specify a route for a particular system. Static routes always override the use of default gateways.

If the default gateway becomes unavailable, the computer cannot communicate outside its own subnet. Multiple default gateways can be assigned to prevent such a problem. When a computer is configured with multiple default gateways, retransmission problems result in the system trying the other routers in the configuration to ensure internetworking communications capabilities. To configure multiple default gateways in Windows NT, you must provide an IP address for each gateway in the Advanced Microsoft TCP/IP Configuration dialog box, as described in Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."

## Dynamic Host Configuration Protocol

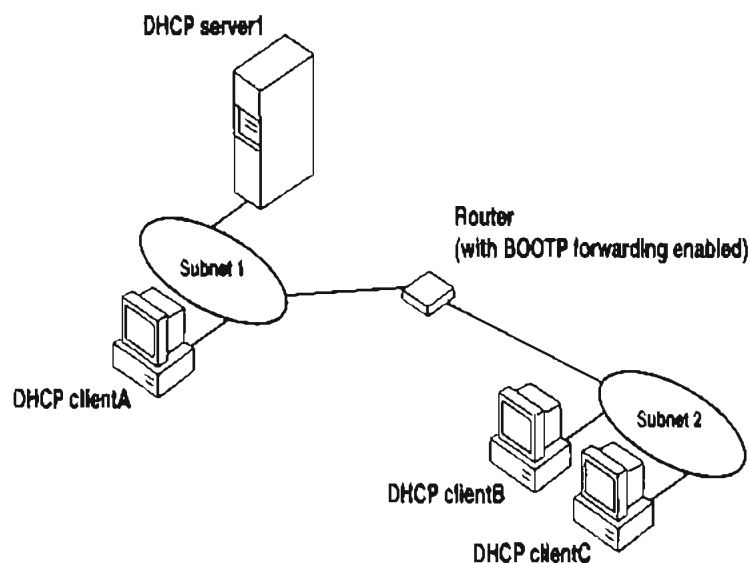
Assigning and maintaining IP address information can be an administrative burden for network administrators responsible for internetwork connections. Contributing to this burden is the problem that many users do not have the knowledge necessary to configure their own computers for internetworking and must therefore rely on their administrators.

The Dynamic Host Configuration Protocol (DHCP) was established to relieve this administrative burden. DHCP provides safe, reliable, and simple TCP/IP network configuration, ensures that address conflicts do not occur, and helps conserve the use of IP addresses through centralized management of address allocation. DHCP offers dynamic configuration of IP addresses for computers. The system administrator controls how IP addresses are assigned by specifying *lease* durations, which specify how long a computer can use an assigned IP address before having to renew the lease with the DHCP server.

As an example of how maintenance tasks are made easy with DHCP, the IP address is released automatically for a DHCP client computer that is removed from a subnet, and a new address for the new subnet is automatically assigned when that computer reconnects on another subnet. Neither the user nor the network administrator needs to intervene to supply new configuration information. This is a most significant feature for mobile computer users with portables that are docked at different computers, or for computers that are moved to different offices frequently.

The DHCP client and server services for Windows NT are implemented under Requests for Comments (RFCs) 1533, 1534, 1541, and 1542.

The following illustration shows an example of a DHCP server providing configuration information on two subnets. If, for example, ClientC is moved to Subnet 1, the DHCP server will automatically supply new TCP/IP configuration information the next time that ClientC is started.

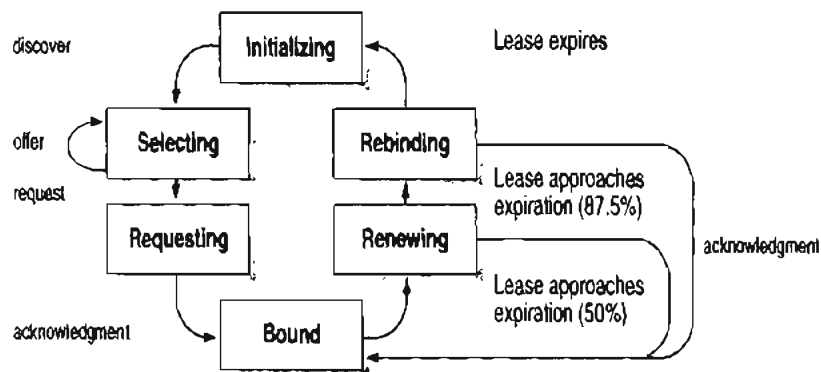


#### DHCP Clients and Servers on a Routed Network

DHCP uses a client-server model and is based on leases for IP addresses. During system startup (the *initializing* state), a DHCP client computer sends a *discover message* that is broadcast to the local network and may be relayed to all DHCP servers on the private internetwork. Each DHCP server that receives the discover message responds with an *offer message* containing an IP address and valid configuration information for the client that sent the request.

The DHCP client collects the configuration offerings from the servers and enters a *selecting* state. When the client enters the *requesting* state, it chooses one of the configurations and sends a *request message* that identifies the DHCP server for the selected configuration.

The selected DHCP server sends a *DHCP acknowledgment message* that contains the address first sent during the discovery stage, plus a valid lease for the address and the TCP/IP network configuration parameters for the client. After the client receives the acknowledgment, it enters a *bound* state and can now participate on the TCP/IP network and complete its system startup. Client computers that have local storage save the received address for use during subsequent system startup. As the lease approaches its expiration date, it attempts to renew its lease with the DHCP server, and is assigned a new address if the current IP address lease cannot be renewed.



#### DHCP Client State Transition During System Startup

In Windows NT Server, the network administrator uses DHCP Manager to define local policies for address allocation, leases, and other options. For information about using this tool, see Chapter 4, “Installing and Configuring DHCP Servers.” For information about the steps for setting up TCP/IP using DHCP, see “Configuring TCP/IP” in Chapter 2, “Installing and Configuring Microsoft TCP/IP and SNMP.” For information about setting up DHCP relaying, see the documentation for your router.

## Name Resolution for Windows Networking

Configuring Windows NT with TCP/IP requires the IP address and computer name, which are unique identifiers for the computer on the network. The IP address, as described earlier in this chapter, is the unique address by which all other TCP/IP devices on the internetwork recognize that computer. For TCP/IP and the Internet, the computer name is the globally known system name plus a DNS domain name. (On the local network, the computer name is the NetBIOS name that was defined during Windows NT Setup.)

Computers use IP addresses to identify each other, but users usually find it easier to work with computer names. A mechanism must be available on a TCP/IP network to resolve names to IP addresses. To ensure that both name and address are unique, the Windows NT computer using TCP/IP registers its name and IP address on the network during system startup. A Windows NT computer can use one or more of the following methods to ensure accurate name resolution in TCP/IP internetworks:

- Windows Internet Name Service

Windows NT computers can use WINS if one or more WINS servers are available that contain a dynamic database mapping computer names to IP addresses. WINS can be used in conjunction with broadcast name resolution for an internetwork where other name resolution methods are inadequate. As described in the following section, WINS is a NetBIOS over TCP/IP mode of operation defined in RFC 1001/1002 as p-node.

- Broadcast name resolution

Windows NT computers can also use broadcast name resolution, which is a NetBIOS over TCP/IP mode of operation defined in RFC 1001/1002 as b-node. This method relies on a computer making IP-level broadcasts to register its name by announcing it on the network. Each computer in the broadcast area is responsible for challenging attempts to register a duplicate name and for responding to name queries for its registered name.

- DNS name resolution

The Domain Name System (DNS) provides a way to look up name mappings when connecting a computer to foreign hosts using NetBIOS over TCP/IP or Windows Sockets applications such as FTP. DNS is a distributed database designed to relieve the traffic problems that arose with the exploding growth of the Internet in the early 1980s.

- An LMHOSTS file to specify the NetBIOS computer name and IP address mappings, or a HOSTS file to specify the DNS name and IP address

On a local computer, the HOSTS file (used by Windows Sockets applications to find TCP/IP host names) and LMHOSTS file (used by NetBIOS over TCP/IP to find Microsoft networking computer names) can be used to list known IP addresses mapped with corresponding computer names. LMHOSTS is still used for name resolution in Windows NT for small-scale networks or remote subnets where WINS is not available.

This section provides details about name resolution in Windows NT after first presenting some background information about the modes of NetBIOS over TCP/IP that can be used in Microsoft networks.

## NetBIOS over TCP/IP and Name Resolution

NetBIOS over TCP/IP is the session-layer network service that performs name-to-IP address mapping for name resolution. This section describes the modes of NetBIOS over TCP/IP, as defined in RFCs 1001 and 1002 to specify how NetBIOS should be implemented over TCP/IP.

The modes of NetBIOS over TCP/IP define how network resources are identified and accessed. The two most important aspects of the related naming activities are registration and resolution. *Registration* is the process used to acquire a unique name for each node (computer system) on the network. A computer typically registers itself when it starts. *Resolution* is the process used to determine the specific address for a computer name.

The NetBIOS over TCP/IP modes include the following:

- b-node, which uses broadcasts to resolve names
- p-node, which uses point-to-point communications with a name server to resolve names
- m-node, which uses b-node first (broadcasts), then p-node (name queries) if the broadcast fails to resolve a name
- h-node, which uses p-node first for name queries, then b-node if the name service is unavailable or if the name is not registered in the WINS database

For DHCP users on a Windows NT network, the node type is assigned by the DHCP server. When WINS servers are in place on the network, NetBIOS over TCP/IP resolves names on a client computer by communicating with the WINS server. When WINS servers are not in place, NetBIOS over TCP/IP uses b-node broadcasts to resolve names. NetBIOS over TCP/IP in Windows NT can also use LMHOSTS files and DNS for name resolution, depending on how TCP/IP is configured on a particular computer. In Windows NT 3.5, the NETBT.SYS module provides the NetBIOS over TCP/IP functionality that supports name registration and resolution modes.

Windows NT version 3.5 supports all of the NetBIOS over TCP/IP modes described in the following sections. NetBIOS over TCP/IP is also used with the LAN Manager 2.x Server message protocol.

## B-Node

The b-node mode uses broadcasts for name registration and resolution. That is, if NT\_PC1 wants to communicate with NT\_PC2 it will broadcast to all machines that it is looking for NT\_PC2 and then wait a specified time for NT\_PC2 to respond.

B-node has two major problems:

- In a large environment, it loads the network with broadcasts.
- Routers do not forward broadcasts, so computers that are on opposite sides of a router will never hear the requests.

## P-Node

The p-node mode addresses the issues that b-node does not solve. In a p-node environment, computers neither create nor respond to broadcasts. All computers register themselves with the WINS server, which is a NetBIOS Name Server (NBNS) with enhancements. The WINS server is responsible for knowing computer names and addresses and for ensuring no duplicate names exist on the network. All computers must be configured to know the address of the WINS server.

In this environment, when NT\_PC1 wants to communicate with NT\_PC2, it queries the WINS server for the address of NT\_PC2. When NT\_PC1 gets the appropriate address from the WINS server, it goes directly to NT\_PC2 without broadcasting. Because the name queries go directly to the WINS server, p-node avoids loading the network with broadcasts. Because broadcasts are not used and because the address is received directly, computers can span routers.

The most significant problems with p-node are the following:

- All computers must be configured to know the address of the WINS server (although this is typically configured via DHCP)
- If for any reason the WINS server is down, computers that rely on the WINS server to resolve addresses cannot get to any other systems on the network, even if they are on the local network

## M-Node

The m-node mode was created primarily to solve the problems associated with b-node and p-node. This mode uses a combination of b-node and p-node. In an m-node environment, a computer first attempts registration and resolution using b-node. If that is successful, it then switches to the p-node. Because this uses b-node first, it does not solve the problem of generating broadcast traffic on the network. However, m-node can cross routers. Also, because b-node is always tried first, computers on the same side of a router continue to operate as usual if the WINS server is down.

M-node uses broadcasts for performance optimization, because in most environments local resources are used more frequently than remote resources. Also, in a Windows NT network, m-node can cause problems with NetLogon in routed environments.

## H-Node

The h-node mode, which is currently in RFC draft form, is also a combination of b-node and p-node that uses broadcasts as a last effort. Because p-node is used first, no broadcasts are generated if the WINS server is running, and computers can span routers. If the WINS server is down, b-node is used, so computers on the same side of a router continue to operate as usual.

The h-node mode does more than change the order for using b-node and p-node. If the WINS server is down so that local broadcasts (b-node) must be used, the computer will continue to poll the WINS server. As soon as the WINS server can be reached again, the system switches back to p-node. Also, optionally on a Windows network, h-node can be configured to use LMHOSTS after broadcast name resolution fails.

The h-node mode solves the most significant problems associated with broadcasts and operating in a routed environment. For Microsoft TCP/IP users who configure TCP/IP manually, h-node is used by default, unless the user does not specify addresses for WINS servers when configuring TCP/IP.

## B-Node with LMHOSTS and Combinations

Another variation is also used in Microsoft networks to span routers without a WINS server and p-node mode. In this mode, b-node uses a list of computers and addresses stored in an LMHOSTS file. If a b-node attempt fails, the system looks in LMHOSTS to find a name and then uses the associated address to cross the router. However, each computer must have this list, which creates an administrative burden in maintaining and distributing the list. Both Windows for Workgroups 3.11 and LAN Manager 2.x used such a modified b-node system. Windows NT uses this method if WINS servers are not used on the network. In Windows NT, some extensions have been added to this file to make it easier to manage (as described in Chapter 6, "Setting Up LMHOSTS"), but modified b-node is not an ideal solution.



Some sites may need to use both b-node and p-node modes at the same site. Although this configuration can work, administrators must exercise extreme caution in doing so, using it only for transition situations. Because p-node hosts disregard broadcasts and b-node hosts rely on broadcasts for name resolution, the two hosts can potentially be configured with the same NetBIOS name, leading to unpredictable results. Notice that if a computer configured to use b-node has a static mapping in the WINS database, a computer configured to use p-node cannot use the same computer name.

Windows NT computers can also be configured as WINS proxy agents to help the transition to using WINS. For more details, see the next section.

## Windows Internet Name Service and Broadcast Name Resolution

WINS provides a distributed database for registering and querying dynamic computer name-to-IP address mappings in a routed network environment. If you are administering a routed network, WINS is your best first choice for name resolution, because it is designed to solve the problems that occur with name resolution in complex internetworks.

WINS reduces the use of local broadcasts for name resolution and allows users to easily locate systems on remote networks. Furthermore, when dynamic addressing through DHCP results in new IP addresses for computers that move between subnets, the changes are automatically updated in the WINS database. Neither the user nor the network administrator needs to make manual accommodations for name resolution in such a case.

The WINS protocol is based on and is compatible with the protocols defined for NBNS in RFCs 1001/1002, so it is interoperable with any other implementations of these RFCs.

This section provides an overview of how WINS and name query broadcasts provide name resolution on Windows networks. For information about setting up WINS servers, see Chapter 5, "Installing and Configuring WINS Servers."

### WINS in a Routed Environment

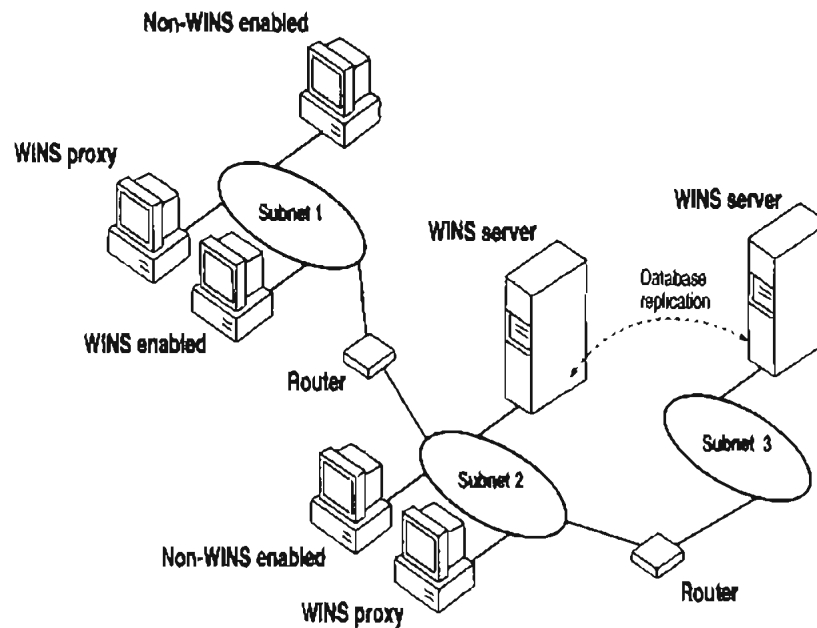
WINS consists of two components: the WINS server, which handles name queries and registrations, and the client software, which queries for computer name resolution.

Windows networking clients (WINS-enabled Windows NT or Windows for Workgroups 3.11 computers) can use WINS directly. Non-WINS computers on the internetwork that are b-node compatible as described in RFCs 1001 and 1002 can access WINS through proxies, which are WINS-enabled computers that listen to name query broadcasts and then respond for names that are not on the local subnet or are p-node computers.

On a Windows NT network, users can browse transparently across routers. To allow browsing without WINS, the network administrator must ensure that the users' primary domain has Windows NT Server or Windows NT Workstation computers on both sides of the router to act as master browsers. These computers need correctly configured LMHOSTS files with entries for the domain controllers across the subnet.

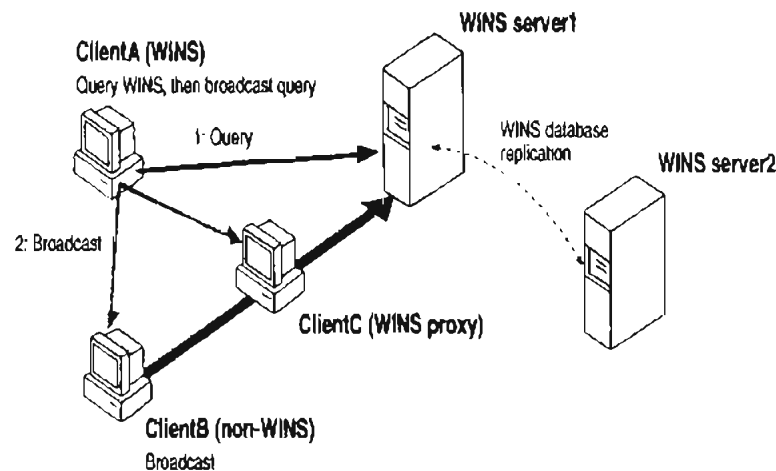
With WINS, such strategies are not necessary because the WINS servers and proxies transparently provide the support necessary for browsing across routers where domains span the routers.

The following illustration shows a small internetwork, with three local area networks connected by a router. Two of the subnets include WINS name servers, which can be used by clients on both subnets. WINS-enabled computers, including proxies, access the WINS server directly, and the computers using broadcasts access the WINS server through proxies. Proxies only pass name query packets and verify that registrations do not duplicate existing systems in the WINS database. Proxies, however, do not register b-node systems in the WINS database.



Example of an Internetwork with WINS Servers

The proxy communicates with the WINS server to resolve names (rather than maintaining its own database) and then caches the names for a certain time. The proxy serves as an intermediary, by either communicating with the WINS server or supplying a name-to-IP address mapping from its cache. The following illustration shows the relationships among WINS servers and clients, including proxies for non-WINS computers and the replication between WINS servers.



#### Example of Clients and Servers Using WINS

In the above illustration, ClientA can resolve names by first querying the WINS server and, if that fails, then using broadcast name queries. ClientB, which is not WINS-enabled, can only resolve names using broadcast name queries, but when ClientC receives the broadcast, it forwards the request to the WINS server and returns the address to ClientB.

However, a complex environment presents additional problems. For example, an internetwork might consist of two subnets, with all the computers belonging to DomainA attached to Subnet1, all the computers in DomainB attached to Subnet2, and computers from DomainC attached to either of the subnets. In this case, without WINS, DomainA computers can browse Subnet1, DomainB computers can browse Subnet2, and DomainC computers can browse both subnets as long as the primary domain controller for DomainC is available. With WINS, computers from all domains can browse all subnets if their WINS servers share databases.

If the Windows NT client computer is also DHCP-enabled and the administrator specifies WINS server information as part of the DHCP options, the computer will usually be automatically configured with WINS server information. You can manually configure WINS settings, as described in Chapter 2, “Installing and Configuring Microsoft TCP/IP and SNMP”:

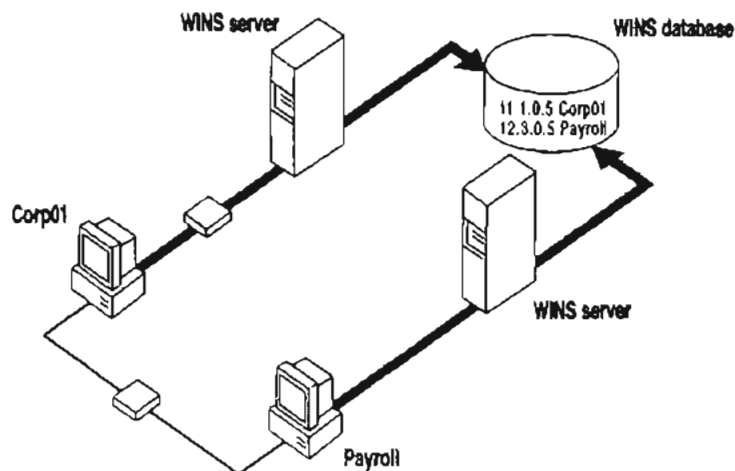
- To enable WINS name resolution for a computer that does not use DHCP, specify WINS server addresses in the TCP/IP Configuration dialog box
- To designate a proxy, check the Enable WINS Proxy Agent option in the Advanced Microsoft TCP/IP Configuration dialog box

With WINS servers in place on the internetwork, names are resolved using two basic methods, depending on whether WINS resolution is available and enabled on the particular computer. Whatever name resolution method is used, the process is transparent to the user after the system is configured.

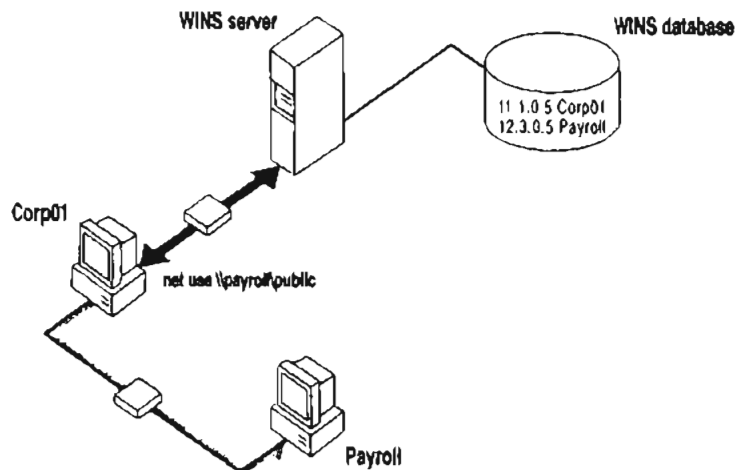
**If WINS is not enabled** The computer registers its name by broadcasting *name registration request* packets to the local subnet via UDP datagrams. To find a particular computer, the non-WINS computer broadcasts *name query request* packets on the local subnet, although this broadcast cannot be passed on through IP routers. If local name resolution fails, the local LMHOSTS file is consulted. These processes are followed whether the computer is a network server, a workstation, or other device.

**If WINS is enabled** The computer first queries the WINS server, and if that does not succeed, it broadcasts its name registration and query requests via UDP datagrams (h-node), in the following series of steps:

1. During TCP/IP configuration, the computer’s name is registered with the WINS server, and the IP address of the WINS server is stored locally so the WINS server can be found on the internetwork. The WINS database is replicated among all WINS servers on the internetwork.



2. A *name query request* is sent first to the WINS server, including requests from remote clients that are routed through an IP router. This request is a UDP datagram. If the name is found in the WINS database, the client can establish a session based on the address mapping received from WINS.



3. If querying the WINS server does not succeed and if the client computer is configured as an h-node, the computer broadcasts *name query request* packets in the same manner as a non-WINS-enabled computer.
4. Finally, if other methods fail, the local LMHOSTS file is checked. This also includes a search of any centralized LMHOSTS files referred to in #INCLUDE statements, as described in Chapter 6, "Setting Up LMHOSTS."

WINS servers accept and respond to UDP name queries. Any name-to-IP address mapping registered with a WINS server can be provided reliably as a response to a name query. However, a mapping in the database does not ensure that the related device is currently running, only that a computer claimed the particular IP address and it is a currently valid mapping.

## WINS Name Registration

Name registration ensures that the computer's name and IP address are unique for each device.

**If WINS is enabled** The name registration request is sent directly to the WINS server to be added to the database. A WINS server accepts or rejects a computer name registration depending on the current contents of its database. If the database contains a different address for that name, WINS challenges the current entry to determine whether that device still claims the name. If another device is using that name, WINS rejects the new name registration request. Otherwise, WINS accepts the entry and adds it to its local database together with a timestamp, an incremental unique version number, and other information.

**If WINS is not enabled** For a non-WINS computer to register its name, a *name registration request* packet is broadcast to the local network, stating its computer name and IP address. Any device on the network that previously claimed that name challenges the name registration with a *negative name registration response*, resulting in an error. If the registration request is not contested within a specific time period, the computer adopts that name and address.

Once a non-WINS computer has claimed a name, it must challenge duplicate name registration attempts and respond positively to name queries issued on its registered name by sending a *positive name query response*. This response contains the IP address of the computer so that the two systems can establish a session.

## WINS Name Release

When a computer finishes with a particular name (such as when the Workstation service or Server service is stopped), it no longer challenges other registration requests for the name. This is referred to as *releasing a name*.

**If WINS is enabled** Whenever a computer is shut down properly, it releases its name to the WINS server, which marks the related database entry as *released*. If the entry remains released for a certain period of time, the WINS server marks it as *extinct*, and the version number is updated so that the database changes will be propagated among the WINS servers. *Extinct* entries remain in the database for a designated period of time to enable the change to be propagated to all WINS servers.

If a name is marked released at a WINS server and a new registration arrives using that name but a different address, the WINS server can immediately give that name to the requesting client because it knows that the old client is no longer using that name. (This might happen, for example, when a DHCP-enabled laptop changes subnets.) If that computer released its name during an orderly shutdown, the WINS server will not challenge the name. If the computer restarts because of a system reset, the name registration with a new address will cause the WINS server to challenge the registration, but the challenge will fail and the registration will succeed, because the computer no longer has the old address.

**If WINS is not enabled** When a non-WINS computer releases a name, a broadcast is made to allow any systems on the network that might have cached the name to remove it. Upon receiving name query packets specifying the deleted name, the computer simply ignores the request, allowing other computers on the network to acquire the name that it has released.

For non-WINS computers to be accessible from other subnets, their names must be added as static entries to the WINS database or in the LMHOSTS file(s) on the remote system(s), because they will only respond to name queries that originate on their local subnet.

## WINS Name Renewal

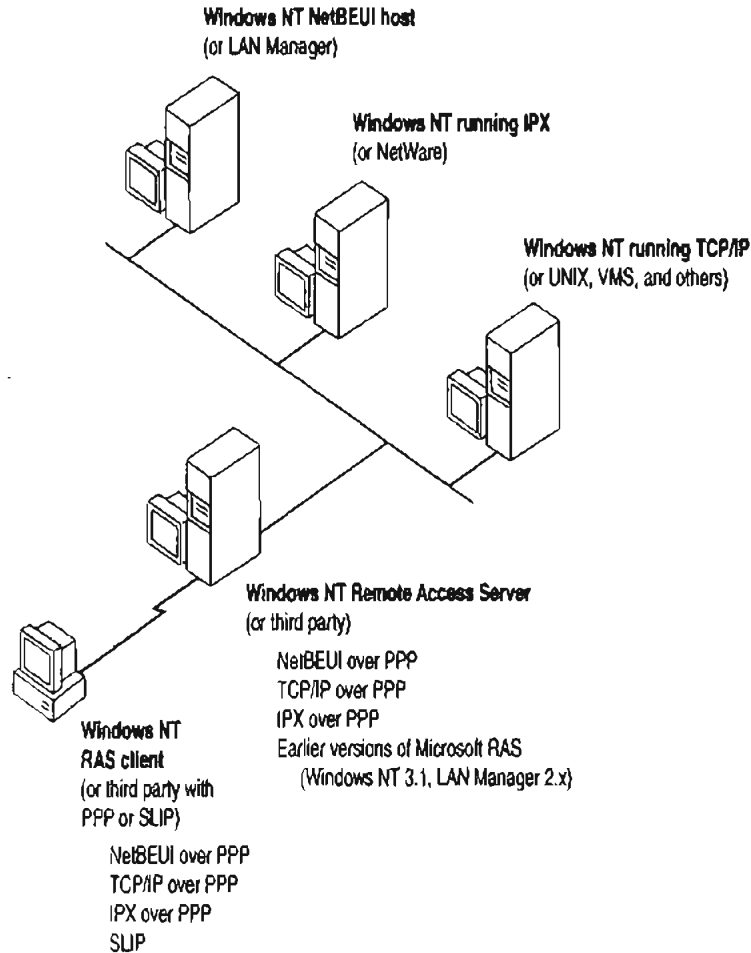
A *renewal* is a timed reregistration of a computer's name with the WINS server. When the WINS server registers a name, it returns a renewal interval for the name, and the client must reregister within that time; otherwise, the WINS server will mark the name as released and available for use. A request for name renewal is treated the same as a new name registration.

Renewal provides registration reliability through periodic reregistering of names with the WINS servers.

## IP Addressing for RAS

Remote Access Service (RAS) provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a Windows NT computer can dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

Windows NT RAS works with IP routing for RAS servers so that RAS clients can use TCP/IP networks. (RAS can also work with IPX routing for clients that use NetWare networks.) Windows NT also uses the industry-standard Point to Point Protocol (PPP) and Serial Line IP (SLIP) standards. These standards ensure that Windows NT is interoperable with third-party remote-access server and client software. RAS clients can use DNS and WINS for name resolution services, and it can create TCP sessions with systems on the local network.



Network Access with RAS in Windows NT



The RAS server provides a pool of IP addresses that are reserved for static configuration during RAS installation. The IP addresses are automatically assigned to RAS clients using PPP when they dial in. If the administrator sets up the RAS server to use a static pool of addresses, all clients dialing into a particular RAS server are assigned the same network ID as the RAS server plus unique host IDs. (Of course, the network administrator must also reserve that range of static addresses on the DHCP server, if present, to make sure that those addresses are not assigned.)

RAS clients can connect to multiple TCP/IP networks that are logically joined (but physically separate) networks sharing the same address space. When using multiple connections, the RAS client can still use DNS and WINS for name resolution.

For complete details about RAS, see the *Windows NT Server Remote Access Service* manual.

## Name Resolution with Host Files

For computers located on remote subnets where WINS is not used, the HOSTS and LMHOSTS files provide mappings for names to IP addresses. This is the name resolution method used on internetworks before DNS and WINS were developed. The HOSTS file can be used as a local DNS equivalent. The LMHOSTS file can be used as a local WINS equivalent. Each of these files is also known as a *host table*. Sample versions of LMHOSTS and HOSTS files are added to the `\systemroot\SYSTEM32\DRIVERS\ETC` directory when you install Microsoft TCP/IP. These files can be edited using any ASCII editor, such as Notepad or Edit, which are part of Windows NT.

Microsoft TCP/IP can be configured to search HOSTS, the local host table file, for mappings of remote host names to IP addresses. The HOSTS file format is the same as the format for host tables in the 4.3 Berkeley Software Distribution (BSD) UNIX `/etc/hosts` file. For example, the entry for a computer with an address of 192.102.73.6 and a host name of `trey-research.com` looks like this:

```
192.102.73.6      trey-research.com
```

Edit the sample HOSTS file that is created when you install TCP/IP to include remote host names and their IP addresses for each computer with which you will communicate. This sample file also explains the syntax of the HOSTS file.

The LMHOSTS file is a local text file that maps IP addresses to NetBIOS computer names for Windows-networking computers that you will communicate with outside of the local subnet. For example, the LMHOSTS table file entry for a computer with an address of 192.45.36.5 and a computer name of `Finance1` looks like this:

```
192.45.36.5      finance1
```

The LMHOSTS file is read when WINS or broadcast name resolution fails, and resolved entries are stored in a system cache for later access.

When the computer uses the replicator service and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnets participating in the replication. LMHOSTS is also used for small-scale networks that do not have servers. For more information about the LMHOSTS file, see Chapter 6, "Setting Up LMHOSTS."

## Domain Name System Addressing

The Domain Name System (DNS) is a distributed database providing a hierarchical naming system for identifying hosts on the Internet. DNS was developed to solve the problems that arose when the number of hosts on the Internet grew dramatically in the early 1980s. The specifications for DNS are defined in RFCs 1034 and 1035. Although DNS may seem similar to WINS, there is a major difference: DNS requires static configuration for computer name-to-IP address mapping, while WINS is fully dynamic and requires far less administration.

The DNS database is a tree structure called the domain name space, where each domain (node in the tree structure) is named and can contain subdomains. The domain name identifies the domain's position in the database in relation to its parent domain, with a period (.) separating each part of the names for the network nodes of the DNS domain.

The root of the DNS database is managed by the Internet Network Information Center. The top-level domains were assigned organizationally and by country. These domain names follow the international standard ISO 3166. Two-letter and three-letter abbreviations are used for countries, and various abbreviations are reserved for use by organizations, as shown in the following example.

DNS domain name abbreviation	Type of organization
com	Commercial (for example, microsoft.com)
edu	Educational (for example, mit.edu for Massachusetts Institute of Technology)
gov	Government (for example, nsf.gov for the National Science Foundation)
org	Noncommercial organizations (for example, fidonet.org for FidoNet)
net	Networking organizations (for example nsf.net for NSFNET)

Each DNS domain is administered by different organizations, which usually break their domains into subdomains and assign administration of the subdomains to other organizations. Each domain has a unique name, and each of the subdomains have unique names within their domains. The label for each network domain is a name of up to 63 characters. The *fully qualified domain name* (FQDN), which includes the names of all network domains leading back to the root, is unique for each host on the Internet. A particular DNS name could be similar to the following, for a commercial host:

```
accounting.trey.com
```

DNS uses a client-server model, where the DNS servers contain information about a portion of the DNS database and make this information available to clients, called *resolvers*, that query the name server across the network. DNS *name servers* are programs that store information about parts of the domain name space called *zones*. The administrator for a domain sets up name servers that contain the database files with all the resource records describing all hosts in their zones. DNS resolvers are clients that are trying to use name servers to gain information about the domain name space.

Windows NT includes the DNS resolver functionality used by NetBIOS over TCP/IP and by Windows Sockets connectivity applications such as `ftp` and `telnet` to query the name server and interpret the responses.

The key task for DNS is to present friendly names for users and then resolve those names to IP addresses, as required by the internetwork. Name resolution is provided through DNS by the name servers, which interpret the information in a FQDN to find its specific address. If a local name server doesn't contain the data requested in a query, it sends back names and addresses of other name servers that could contain the information. The resolver then queries the other name servers until it finds the specific name and address it needs. This process is made faster because name servers continuously cache the information learned about the domain name space as the result of queries.

All the resolver software necessary for using DNS on the Internet is installed with Microsoft TCP/IP. To use DNS for TCP/IP name resolution, you specify options in the DNS Configuration dialog box. For more information, see Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."

On computers with Windows NT Server 3.5, Windows NT Workstation 3.5, or Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed, Windows Socket applications can use either DNS or NetBIOS over TCP/IP for name resolution.

The following table compares DNS versus WINS name resolution.

#### WINS Versus DNS Name Resolution

Name provider capabilities	WINS	DNS
Provides scalable naming authority for large internetworks	Yes	Yes
Provides a dynamic, distributed naming authority for TCP/IP network names	Yes	Not dynamic
Supports MX records for electronic mail	No	Yes
Supports recursion and referral for name resolution	No	Yes
Provides hierarchical naming and resolution scheme	No	Yes
Includes DNS name server	No	Yes
Includes DNS name resolution client	Yes	Yes
Provides static name resolution	Yes (optional)	Yes (only)
Queries DNS servers	Yes <sup>1</sup>	Yes
Provides name server in operating system	Yes	No
Resolves NetBIOS-compatible names	Yes	No
Provides a name resolution solution for large peer-based TCP/IP networks (50,000+ systems)	Yes	No
Supports automatic name registration	For WINS clients only	No
Supports dynamic NetBIOS name registration and resolution	Yes	No
Supports managing hosts configured via DHCP	Yes	No
Supports easy administration, including browsing and managing dynamic and static registrations	Yes	No
Centralizes management of the name database	Yes	No
Defines server replication partners and policies	Yes	No
Alleviates LMHOSTS management requirements	Yes	No
Reduces IP broadcast traffic in Windows-based internetworks	Yes	No

<sup>1</sup> Queries DNS servers via Windows Sockets applications or, for Windows networking applications, via NetBIOS over TCP/IP (after using WINS first)

## SNMP

Simple Network Management Protocol (SNMP) is used by administrators to monitor and control remote hosts and gateways on an internetwork. The Windows NT SNMP service allows a Windows NT computer to be monitored remotely but does not include an application to monitor other SNMP systems on the network.

---

**Note** You must install the SNMP service to use the TCP/IP performance counters in Performance Monitor, as described in Chapter 8, "Using Performance Monitor with TCP/IP Services."

---

SNMP is a network management protocol widely used in TCP/IP networks. These kinds of protocols are used to communicate between a management program run by an administrator and the network management agent running on a host or gateway. These protocols define the form and meaning of the messages exchanged, the representation of names and values in the messages, and administrative relationships among hosts being managed. SNMP defines a set of variables that the host must keep and specifies that all operations on the gateway are side effects of getting, putting, or setting the data variables. Because different network-management services are used for different types of devices or for different network-management protocols, each service has its own set of objects. The entire set of objects that any service or protocol uses is referred to as its *management information base (MIB)*.

The Windows NT SNMP service includes MIB II (based on RFC 1213) and LAN Manager MIB II plus MIBs for DHCP and WINS servers, as described in Appendix A, "MIB Object Types for Windows NT." The SNMP service allows SNMP-based managers to perform standard SNMP commands, such as reading the counters in the standard MIBs included with the service. Windows NT SNMP has an extensible architecture, so it can be used to create custom functionality on a Windows NT computer, such as starting and stopping specific services or shutting down the system.

The SNMP service works with any computer running Windows NT and the TCP/IP protocol. With the SNMP service, a Windows NT computer can report its current status to an SNMP management system on a TCP/IP network. The service sends status information to a host in two cases:

- When a management system requests such information
- When a significant event occurs on the Windows NT computer

The SNMP service can handle requests from one or more hosts, and it can also report network-management information to one or more hosts, in discrete blocks of data called *traps*.

The SNMP service uses the unique host names and IP addresses of devices to recognize the host(s) to which it reports information and from which it receives requests.

When a network manager requests information about a device on the network, SNMP management software can be used to determine object values that represent network status. MIB objects represent various types of information about the device. For example, the management station might request an object called **SvStatOpen**, which would be the total number of files open on the Windows NT computer.

The SNMP service for Windows NT supports multiple MIBs through an agent Application Programming Interface (API) extension interface. At SNMP service startup time, the SNMP service loads all of the extension-agent dynamic link libraries (DLLs) that are defined in the Windows NT Registry. Two extension-agent DLLs come with Windows NT; others may be developed and added by users.

## CHAPTER 4

# Installing and Configuring DHCP Servers



A Dynamic Host Configuration Protocol (DHCP) server is a Windows NT Server computer running Microsoft TCP/IP and the DHCP-compatible server software. DHCP is defined in Requests for Comments (RFCs) 1533, 1534, 1541, and 1542.

This chapter describes how to install and manage servers to support DHCP in Windows NT and also presents strategies for implementing DHCP. The following topics are included in this chapter:

- Overview of the DHCP client-server model
- Installing DHCP servers and using DHCP Manager
- Defining DHCP scopes
- Configuring DHCP options
- Administering DHCP clients
- Managing the DHCP database files
- Troubleshooting DHCP
- Advanced configuration parameters for DHCP
- Guidelines for setting local policies
- Planning a strategy for DHCP

---

**Important** If you want to use a DHCP server to support subnetworks that span multiple routers, you may need a firmware upgrade for your routers. Your routers must support RFCs 1533, 1534, 1541, and 1542.

To find out about DHCP-relay agent support, contact your router vendor. For more information, refer to RFC1542.TXT available via anonymous FTP from <ftp.internic.net/rfc>.

---

## Overview of DHCP Clients and Servers

Configuring DHCP servers for a network provides these benefits:

- The administrator can centrally define global and subnet TCP/IP parameters for the entire internetwork and define parameters for reserved clients.
- Client computers do not require manual TCP/IP configuration. When a client computer moves between subnets, it is reconfigured for TCP/IP automatically at system startup time.

DHCP uses a client-server model. The network administrator establishes one or more DHCP servers that maintain TCP/IP configuration information to be provided to clients that make requests.

The DHCP server database includes the following:

- Valid configuration parameters for all clients on the internetwork.
- Valid IP addresses maintained in a pool for assignment to clients, plus reserved addresses for manual assignment.
- Duration of leases and other configuration parameters offered by the server. The lease defines the length of time for which the assigned IP address can be used.

A Windows NT computer becomes a DHCP client if the Enable Automatic DHCP Configuration option is checked in the Windows NT TCP/IP Installation Options dialog box. When a DHCP client computer is started, it communicates with a DHCP server to receive the required TCP/IP configuration information. This configuration information includes at least an IP address and submask plus the lease associated with the configuration.

---

**Note** DHCP client software is part of the Microsoft TCP/IP-32 for Windows for Workgroups software and the Microsoft Network Client 2.0 software that are included on the Windows NT Server compact disc. For information about installing this software, see the *Windows NT Server Installation Guide*.

---

For an overview of how DHCP works, see “Dynamic Host Configuration Protocol” in Chapter 3, “Networking Concepts for TCP/IP.”

---

**Note** DHCP can be monitored using SNMP. For a list of DHCP MIB object types, see Appendix A, “MIB Object Types for Windows NT.”

---



## Installing DHCP Servers

You install a DHCP server as part of the process of installing Microsoft TCP/IP. These instructions assume you have already installed the Windows NT Server operating system on the computer.

---

**Caution** Before installing a new DHCP server, check for other DHCP servers on the network to avoid interfering with them.

---



You must be a member of the Administrators group for the computer you are installing or administering as a DHCP server.

► **To install a DHCP server**

1. Start the Network option in Control Panel. When the Network Settings dialog box appears, choose the Add Software button to display the Add Network Software dialog box.
2. In the Network Software list box, select TCP/IP Protocol And Related Components, and then choose the Continue button.
3. In the Windows NT TCP/IP Installation Options dialog box, check the appropriate options to be installed, including at least DHCP Server Service. Also check SNMP Service if you want to use Performance Monitor or SNMP to monitor DHCP.
4. Choose the OK button. Windows NT Setup displays a message asking for the full path to the Windows NT Server distribution files. Provide the appropriate location, and choose the Continue button.

All necessary files are copied to your hard disk. When the Network Settings dialog box reappears after you finishing configuring TCP/IP, choose the OK button.

5. Complete all the required procedures for manually configuring TCP/IP as described in “Configuring TCP/IP” in Chapter 2, “Installing and Configuring Microsoft TCP/IP and SNMP.”

If this DHCP server is multihomed (has multiple network adapters), you must use the Advanced Microsoft TCP/IP Configuration dialog box to specify IP addresses and other information for each network adapter.

Also, if any adapter on the DHCP server is connected to a subnet that you do not want this server to support, then you must disable the bindings to that subnet for the particular adapter. To do this, choose the Network option in Control Panel, then choose the Bindings button in the Network Settings dialog box and disable the related binding.

---

**Note** You cannot use DHCP to automatically configure a new DHCP server, because a computer cannot be a DHCP client and server simultaneously.

---

All the appropriate TCP/IP and DHCP software is ready for use after you reboot the computer.

The DHCP Client service is a Windows NT service running on a Windows NT computer. The supporting DHCP client software is automatically installed for computers running Windows NT Server or Windows NT Workstation when you install the basic operating system software.

The Microsoft DHCP Server service starts automatically during system startup if you have installed this service. You will probably want to pause the service while you are configuring scopes for the first time.

► **To pause the DHCP Server service at any Windows NT computer**

1. In Control Panel, choose the Services icon.

–Or–

In Server Manager, choose Services from the Computer menu.

2. In the Services dialog box, select the Microsoft DHCP Server service.

3. Choose the Pause button, and then choose the Close button.

You can also start, stop, and pause the DHCP service at the command prompt using the commands `net start dhcpserver` or `net stop dhcpserver` or `net pause dhcpserver`.

## Using DHCP Manager

The DHCP Manager icon is added to the Network Administration Tools group in Program Manager when you set up a Windows NT Server computer to be a DHCP server. You must use DHCP Manager to perform these basic tasks:

- Create one or more DHCP scopes to begin providing DHCP services
- Define properties for the scope, including the lease duration and IP address ranges to be distributed to potential DHCP clients in the scope
- Define default values for options such as the default gateway, DNS server, or WINS server to be assigned together with an IP address, or add any custom options

The procedures for completing these tasks are described in the following sections.

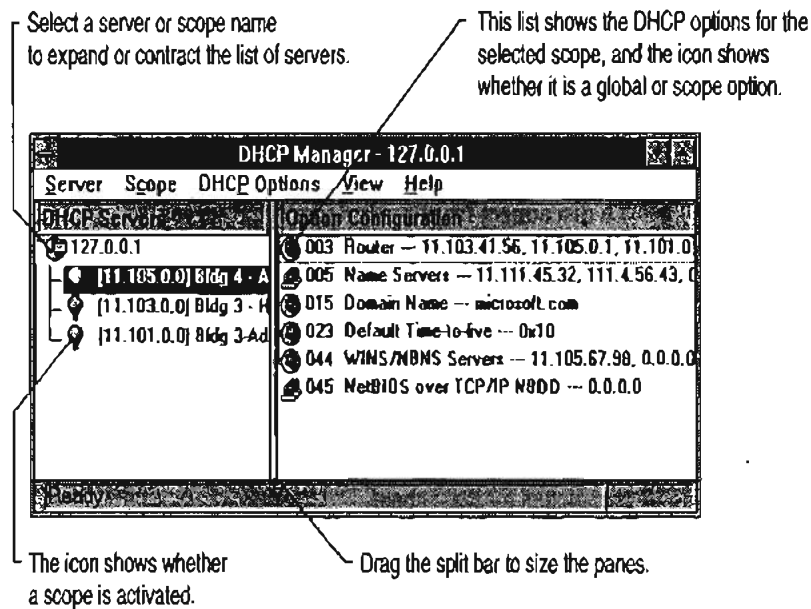
► To start DHCP Manager

- Double-click the DHCP Manager icon in the Network Administration group in Program Manager.

–Or–

At the command prompt, type `start dhcpadmin` and press ENTER.

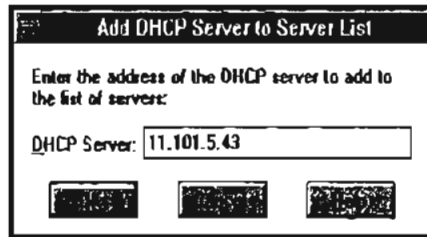
DHCP Manager window shows the local computer the first time you start DHCP Manager. Subsequently, the window shows a list of the DHCP servers to which DHCP Manager has connected, plus their scopes. The status bar reports the current DHCP Manager activities.



**Important** When you are working with DHCP Manager, all computer names are DNS host names only, such as `accounting.trey.com`. The NetBIOS computer names used in Windows networking are not allowed.

► **To connect to a DHCP server**

1. From the Server menu, choose the Add command.



2. In the Add DHCP Server To Known Server List dialog box, type the DNS short name or IP address for the DHCP server you want to connect to, and then choose the OK button.

For example, type an address such as **11.1.26.30** or type a DNS name such as **corp01.trey.com** in this box.

► **To disconnect from a selected DHCP server**

- From the Server menu, choose Remove, or press DEL.

## Defining DHCP Scopes

A DHCP scope is an administrative grouping of computers running the DHCP Client service. You will create a scope for each subnet on the network to define parameters for that subnet.

Each scope has the following properties:

- A unique subnet mask used to determine the subnet related to a given IP address
- A scope name assigned by the administrator when the scope is created
- Lease duration values to be assigned to DHCP clients with dynamic addresses

## Creating Scopes

You must use DHCP Manager to create, manage, or remove scopes.

► **To create a new DHCP scope**

1. In the DHCP Servers list in the DHCP Manager window, select the server for which you want to create a scope.
2. From the Scope menu, choose Create.

3. To define the available range of IP addresses for this scope, type the beginning and ending IP addresses for the range in the Start Address and End Address boxes.

The IP address range will include the Start and End values.

---

**Note** You must supply this information before this scope can be activated.

---

4. In the Subnet Mask box, DHCP Manager proposes a subnet mask, based on the IP address of the Start and End addresses. Accept the proposed value, unless you know that a different value is required.

5. To define excluded addresses within the IP address pool range, use the Exclusion Range controls, as follows:
  - Type the first IP address that is part of the excluded range in the Start Address box, and type the last number in the End Address box. Then choose the Add button. Continue to define any other excluded ranges in the same way.
  - To exclude a single IP address, type the number in the Start Address box. Leave the End Address box empty and choose the Add button.
  - To remove an IP address or range from the excluded range, select it in the Excluded Addresses box, and then choose the Remove button.

The excluded ranges should include all IP addresses that you assigned manually to other DHCP servers, non-DHCP clients, diskless workstations, or RAS and PPP clients.
6. To specify the lease duration for IP addresses in this scope, select Limited To. Then type values defining the number of days, hours, and seconds for the length of the address lease.

If you do not want IP address leases in this scope to expire, select the Unlimited option.
7. In the Name box, type a scope name.

This is any name you want to use to describe this subnet. The name can include any combination of letters, numbers, and hyphens. Blank spaces and underscore characters are also allowed. You cannot use Unicode characters.
8. Optionally, in the Comment box, type any string to describe this scope, and then choose the OK button.

---

**Note** When you finish creating a scope, a message reminds you that the scope has not been activated and allows you to choose Yes to activate the scope immediately. However, you should not activate a new scope until you have defined the DHCP options to be configured for this scope.

---

Now you can continue with the procedures described in “Configuring DHCP Option Types” and “Administering DHCP Clients” later in this chapter. After you have configured the options for this scope, you must activate it so that DHCP client computers on the related subnet can begin using DHCP for dynamic TCP/IP configuration.

► **To activate a DHCP scope**

- From the Scope menu, choose the Activate command to make this scope active. The menu command name changes to Deactivate when the selected scope is currently active.

## Changing Scope Properties

The subnet identifiers and address pool make up the properties of scopes. You can change the properties of an existing scope.

► **To change the properties of a DHCP scope**

1. In the DHCP Servers list in the DHCP Manager window, select the scope for which you want to change properties, and then from the Scope menu, choose Properties.

–Or–

In the DHCP Servers list, double-click the scope you want to change.

2. In the Scope Properties dialog box, change any values for the IP address pool, lease duration, or name and comment as described earlier in “Creating Scopes” or in online Help.
3. Choose the OK button.

## Removing a Scope

When a subnet is no longer in use, or any other time you want to remove an existing scope, you can remove it using DHCP Manager. If any IP address in the scope is still leased or in use, you must first deactivate the scope until all client leases expire or all client lease extension requests are denied.

► **To remove a scope**

1. In the DHCP Servers list in the DHCP Manager window, select the scope you want to remove.
2. From the Scope menu, choose Deactivate. (This command name changes to Activate when the scope is not active.)

The scope must remain deactivated until you are sure the scope is not in use.

3. From the Scope menu, choose Delete.

The Delete command is not available for an active scope.

## Configuring DHCP Options

The configuration parameters that a DHCP server assigns to a client are defined as *DHCP options* using DHCP Manager. Most options you will want to specify are predefined, based on standard parameters defined in RFC 1542.

When you configure a DHCP scope, you can assign DHCP options to govern all configuration parameters. You can also define, edit, or delete DHCP options. These tasks are described in the following sections.

## Assigning DHCP Configuration Options

Besides the IP addressing information, other DHCP configuration options to be passed to DHCP clients must be configured for each scope. Options can be defined globally for all scopes on the current server, specifically for a selected scope, or for individual DHCP clients with reserved addresses.

- Active global options always apply unless overridden by scope options or DHCP client settings.
- Active options for a scope apply to all computers in that scope, unless overridden for an individual DHCP client.

The built-in options are described in “Predefined DHCP Client Configuration Options” later in this chapter.

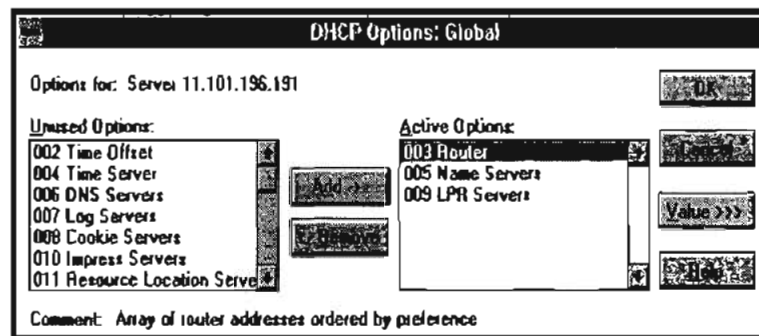
---

**Note** Lease duration is defined for the scope in the Create Scope dialog box.

---

► **To assign DHCP configuration options**

1. In the DHCP Servers list in the DHCP Manager window, select the scope you want to configure.
2. From the DHCP Options menu, choose the Global or Scope command, depending on whether you want to define option settings for all scopes on the currently selected server or the scope currently selected in the DHCP Manager window.





3. In the Unused Options list in the DHCP Options dialog box, select the name of the DHCP option that you want to apply, and then choose the Add button to move the name to the Active Options list.

This list shows both predefined options and any custom options that you added.

For example, if you want to specify DNS servers for computers, select the option named DNS Servers in the Unused Options list and choose the Add button.

If you want to remove an active DHCP option, select its name in the Active Options box, and then choose the Remove button.

4. To define the value for an active option, select its name in the Active Options box, and choose the Values button. Then choose the Edit button, and edit the information in the Current Value box, depending on the data type for the option, as follows:
  - For an IP address, type the assigned address for the selected option
  - For a number, type an appropriate decimal or hexadecimal value for the option
  - For a string, type an appropriate ASCII string containing letters and numbers for the option

For example, to specify the DNS name servers to be used by DHCP clients, select DNS Servers in the Active Options list. Then choose the Edit button and type a list of IP addresses for DNS servers. The list should be in the order of preference.

For details about the Edit Array and Edit Address dialog boxes, see the online Help.

5. When you have completed all your changes, choose the OK button.

---

**Tip** If you are using DHCP to configure WINS clients, be sure to set options #44 WINS Servers and #46 Node Type. These options will allow DHCP-configured computers to find and use the WINS server automatically.

---

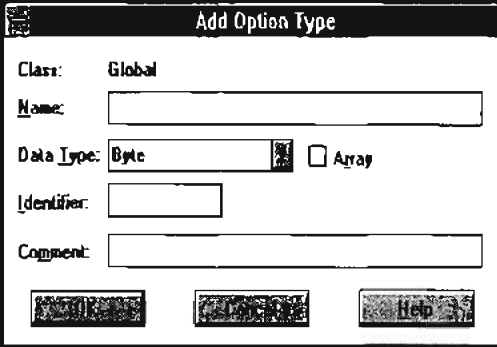
## Creating New DHCP Options

You can add custom parameters to be included with DHCP client configuration information. You can also change values or other elements of the predefined DHCP options. The option you add will appear in the list of available DHCP options in the DHCP Options dialog boxes for defining options globally, per scope, and per individual reserved DHCP client.

► **To add new DHCP options**

1. From the DHCP Options menu, choose Defaults.
2. In the Option Class list in the DHCP Options: Default Values dialog box, select the class for which you want to add new DHCP options, and then choose the New button.

The option class can include the DHCP standard options or any custom options that you add.



The screenshot shows a dialog box titled "Add Option Type". It contains the following fields and controls:

- Class:** A dropdown menu currently showing "Global".
- Name:** An empty text input field.
- Data Type:** A dropdown menu showing "Byte" and a radio button next to "Array".
- Identifier:** An empty text input field.
- Comment:** An empty text input field.
- Buttons:** Three buttons at the bottom: "OK", "Cancel", and "Help".

3. In the Name box of the Add Option Type dialog box, type a new option name.

- From the Data Type list, select the data type for this option as described in the following list. If this data type represents an array, check the Array box.

Data type	Meaning
Binary	Value expressed as an array of bytes
Byte	An 8-bit, unsigned integer
Encapsulated	An array of unsigned bytes
IP address	An IP address of the form w.x.y.z
Long	A 32-bit, signed integer
Long integer	A 32-bit, unsigned integer
String	An ASCII text string
Word	A 16-bit, unsigned integer

If you select the wrong data type, an error message will appear or the value will be truncated or converted to the required type.

- In the Identifier box, type a unique code number to be associated with this DHCP option. This must be a number between 0 and 255.
- In the Comment box, type a description of the DHCP option, and then choose the OK button.
- In the DHCP Options: Default Values dialog box, select the option, choose the Edit button, and type the value to be configured by default for this DHCP option.
- Choose the OK button.

You can delete custom DHCP options, but you cannot delete any predefined DHCP options.

► **To delete a custom DHCP option**

- From the DHCP Options menu, choose Defaults.
- In the DHCP Options: Default Values dialog box, select the related class in the Option Class list.
- In the Option Name list, select the option you want to delete, and then choose the Delete button.

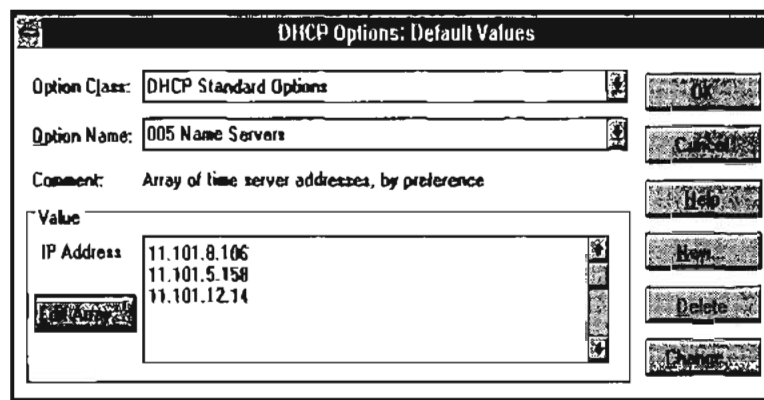
## Changing DHCP Option Values

You can change the values for the predefined and custom DHCP options for configuring clients. For example, you could change the default values for these built-in options:

- 3 = Router, to specify the IP addresses for the routers on the subnet
- 6 = DNS Servers, to specify the IP addresses of the DNS name servers used at your site
- 15 = Domain Name, to specify the DNS domain names to be used for host name resolution

► **To change a DHCP option value**

1. From the DHCP Options menu, choose Defaults.



2. In the Option Class list in the DHCP Options: Default Values dialog box, select the option class for which you want to change values.
3. If you want to change the default value for an option, select the option you want to change in the Option Name list, choose the Edit button, and then type a new value in the Value box.

Choosing the Edit button displays a special dialog box for editing strings, arrays of IP address, or binary values. For information about using the special editing dialog boxes, see the online Help for DHCP Manager.

4. If you want to change basic elements of a custom option, select it in the Option Name list, and then choose the Change button.

You can change the name, data type, identifier, and comment for a DHCP option, following the procedures described earlier in "Creating New DHCP Options."

5. When you complete all the changes you want to make, choose the OK button.

## Defining Options for Reservations

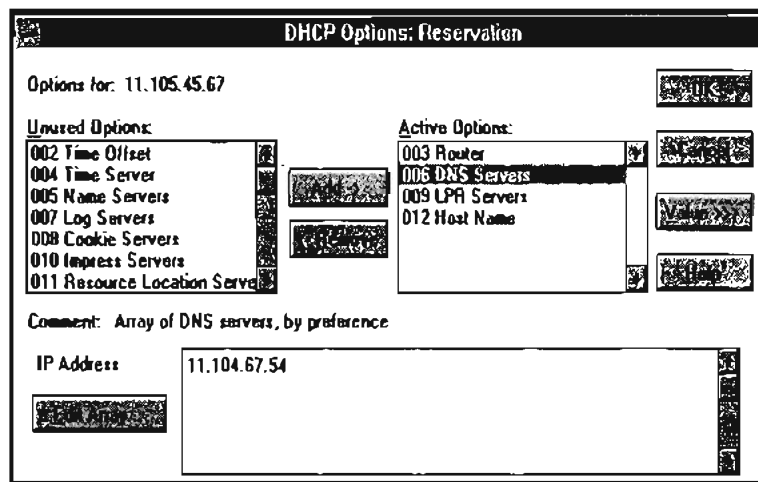
You can assign DHCP options and specify custom values for DHCP clients that use reserved IP addresses.

For information about how to reserve IP configuration information for DHCP clients, see “Managing Client Reservations” later in this chapter.

► **To change DHCP options for reservations**

1. From the Scope menu, choose Active Leases.
2. In the IP Address list of the Active Leases dialog box, select the reserved address whose options you want to change, and then choose the Options button.

The Options button is only available for reserved addresses; it is not available for DHCP clients with dynamic addresses.



3. In the DHCP Options: Reservation dialog box, select an option name in the Unused Options list, and then choose the Add button to move the name to the Active Options list.

If you want to remove a DHCP option that has been assigned to the scope, select its name in the Active Options box, and then choose the Remove button.

4. To change a value for an option selected in the Active Options list, choose the Value button. Then choose the Edit button and enter a new value in the Current Value box.

## Predefined DHCP Client Configuration Options

The tables in this section describe the predefined options available for configuration of DHCP clients. These options are defined in RFC 1533.

### Basic Options

Code	Option name	Meaning
0	Pad	Causes subsequent fields to align on word boundaries.
255	End	Indicates end of options in the DHCP packet.
2	Time offset	Specifies the Universal Coordinated Time (UCT) offset in seconds.
3	Router	Specifies a list of IP addresses for routers on the client's subnet. <sup>1</sup>
4	Time server	Specifies a list of IP addresses for time servers available to the client. <sup>1</sup>
5	Name servers	Specifies a list of IP addresses for name servers available to the client. <sup>1</sup>
6	DNS servers	Specifies a list of IP addresses for DNS name servers available to the client. <sup>1</sup>
7	Log servers	Specifies a list of IP addresses for MIT_LCS User Datagram Protocol (UDP) log servers available to the client. <sup>1</sup>
8	Cookie servers	Specifies a list of IP addresses for RFC 865 cookie servers available to the client. <sup>1</sup>
9	LPR servers	Specifies a list of IP addresses for RFC 1179 line-printer servers available to the client. <sup>1</sup>
10	Impress servers	Specifies a list of IP addresses for Imagen Impress servers available to the client. <sup>1</sup>
11	Resource location servers	Specifies a list of RFC 887 Resource Location servers available to the client. <sup>1</sup>
12	Host name	Specifies the host name of up to 63 characters for the client. The name must start with a letter, end with a letter or digit, and have as interior characters only letters, numbers, and hyphens. The name can be qualified with the local DNS domain name.
13	Boot file size	Specifies the size of the default boot image file for the client, in 512-octet blocks.

<sup>1</sup> List is specified in order of preference.

**Basic Options (continued)**

Code	Option name	Meaning
14	Merit dump file	Specifies the ASCII path name of a file where the client's core image is dumped if a crash occurs.
15	Domain name	Specifies the DNS domain name the client should use for DNS host name resolution.
16	Swap server	Specifies the IP address of the client's swap server.
17	Root path	Specifies the ASCII path name for the client's root disk.
18	Extensions path	Specifies a file retrievable via TFTP containing information interpreted the same as the vendor-extension field in the BOOTP response, except the file length is unconstrained and references to Tag 18 in the file are ignored.

† List is specified in order of preference.

The following table lists IP layer parameters on a per-host basis.

**IP Layer Parameters per Host**

Code	Option name	Meaning
19	IP layer forwarding	Enables or disables forwarding of IP packet for this client. 1 enables forwarding; 0 disables it.
20	Nonlocal source routing	Enables or disables forwarding of datagrams with non-local source routes. 1 enables forwarding; 0 disables it.
21	Policy filter masks	Specifies policy filters that consist of a list of pairs of IP addresses and masks specifying destination/mask pairs for filtering nonlocal source routes. Any source routed datagram whose next-hop address does not match a filter will be discarded by the client.
22	Max DG reassembly size	Specifies the maximum size datagram that the client can reassemble. The minimum value is 576.
23	Default time-to-live	Specifies the default time-to-live (TTL) that the client uses on outgoing datagrams. The value for the octet is a number between 1 and 255.
24	Path MTU aging timeout	Specifies the timeout in seconds for aging Path Maximum Transmission Unit (MTU) values (discovered by the mechanism defined in RFC 1191).
25	Path MTU plateau table	Specifies a table of MTU sizes to use when performing Path MTU Discovered as defined in RFC 1191. The table is sorted by size from smallest to largest. The minimum MTU value is 68.

The following table lists IP parameters on a per-interface basis. These options affect the operation of the IP layer on a per-interface basis. A client can issue multiple requests, one per interface, to configure interfaces with their specific parameters.

#### IP Parameters per Interface

Code	Option name	Meaning
26	MTU option	Specifies the MTU discovery size for this interface. The minimum MTU value is 68.
27	All subnets are local	Specifies whether the client assumes that all subnets of the client's internetwork use the same MTU as the local subnet where the client is connected. 1 indicates that all subnets share the same MTU; 0 indicates that the client should assume some subnets may have smaller MTUs.
28	Broadcast address	Specifies the broadcast address used on the client's subnet.
29	Perform mask discovery	Specifies whether the client should use Internet Control Message Protocol (ICMP) for subnet mask discovery. 1 indicates the client should perform mask discovery; 0 indicates the client should not.
30	Mask supplier	Specifies whether the client should respond to subnet mask requests using ICMP. 1 indicates the client should respond; 0 indicates the client should not respond.
31	Perform router discovery	Specifies whether the client should solicit routers using the router discovery method in RFC 1256. 1 indicates that the client should perform router discovery; 0 indicates that the client should not use it.
32	Router solicitation address	Specifies the IP address to which the client submits router solicitation requests.
33	Static route	Specifies a list of IP address pairs that indicate the static routes the client should install in its routing cache. Any multiple routes to the same destination are listed in descending order of priority. The routes are destination/router address pairs. (The default route of 0.0.0.0 is an illegal destination for a static route.)



The following table lists link layer parameters per interface. These options affect the operation of the data link layer on a per-interface basis.

#### Link Layer Parameters per Interface

Code	Option name	Meaning
34	Trailer encapsulation	Specifies whether the client should negotiate use of trailers (RFC 983) when using the ARP protocol. 1 indicates the client should attempt to use trailer; 0 indicates the client should not use trailers.
35	ARP cache timeout	Specifies the timeout in seconds for ARP cache entries.
36	Ethernet encapsulation	Specifies whether the client should use Ethernet v. 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation if the interface is Ethernet. 1 indicates that the client should use RFC 1042 encapsulation; 0 indicates the client should use RFC 894 encapsulation.

The following table shows TCP parameters. These options affect the operation of the TCP layer on a per-interface basis.

#### TCP Parameters

Code	Option name	Meanlog
37	Default time-to-live	Specifies the default TTL the client should use when sending TCP segments. The minimum value of the octet is 1.
38	Keepalive interval	Specifies the interval in seconds the client TCP should wait before sending a keepalive message on a TCP connection. A value of 0 indicates that the client should not send keepalive messages on connections unless specifically requested by an application.
39	Keepalive garbage	Specifies whether the client should send TCP keepalive messages with an octet of garbage data for compatibility with older implementations. 1 indicates that a garbage octet should be sent; 0 indicates that it should not be sent.

The following table shows application layer parameters. These miscellaneous options are used to configure applications and services.

#### Application Layer Parameters per

Code	Option name	Meaning
40	NIS domain name	Specifies the name of the Network Information Service (NIS) domain as an ASCII string.
41	NIS servers	Specifies a list of IP addresses for NIS servers available to the client. <sup>1</sup>
42	NTP servers	Specifies a list of IP addresses for Network Time Protocol (NTP) servers available to the client. <sup>1</sup>

<sup>1</sup> List is specified in order of preference.

The following options are for vendor-specific information.

#### Vendor-Specific Information

Code	Option name	Meaning
43	Vendor specific info	Binary information used by clients and servers to exchange vendor-specific information. Servers not equipped to interpret the information ignore it. Clients that don't receive the information attempt to operate without it.

#### NetBIOS over TCP/IP

Code	Option name	Meaning
44	WINS/NBNS servers	Specifies a list of IP addresses for NetBIOS name servers (NBNS). <sup>1</sup>
45	NetBIOS over TCP/IP NBDD	Specifies a list of IP addresses for NetBIOS datagram distribution servers (NBDD). <sup>1</sup>
46	WINS/NBT node type	Allows configurable NetBIOS over TCP/IP clients to be configured as described in RFC 1001/1002, where 1=b-node, 2=p-node, 4=m-node, and 8=h-node.

---

**NetBIOS over TCP/IP (continued)**

Code	Option name	Meaning
47	NetBIOS scope ID	Specifies as a string that is the NetBIOS over TCP/IP Scope ID for the client, as specified in RFC 1001/1002.
48	X Window system font	Specifies a list of IP addresses for X Window font servers available to the client. <sup>†</sup>
49	X Window system display	Specifies a list of IP addresses for X Window System Display Manager servers available to the client. <sup>†</sup>

<sup>†</sup> List is specified in order of preference.

**DHCP Extensions**

Code	Option name	Meaning
58	Renewal (T1) time value	Specifies the time in seconds from address assignment until the client enters the renewing state.
59	Rebinding (T2) time value	Specifies the time in seconds from address assignment until the client enters the rebinding state.

## Administering DHCP Clients

After you have established the scope and defined the range of available and excluded IP addresses, DHCP-enabled clients can begin using the service for automatic TCP/IP configuration.

You can use DHCP Manager to manage individual client leases, including creating and managing reservations for clients.

---

**Tip** You can use the `ipconfig` utility to troubleshoot the IP configuration on computers that use DHCP, as described in Chapter 11, “Utilities Reference.” You can also use `ipconfig` on TCP/IP-32 clients on Windows for Workgroups 3.11 computers and on computers running Microsoft Network Client version 2.0 for MS-DOS.

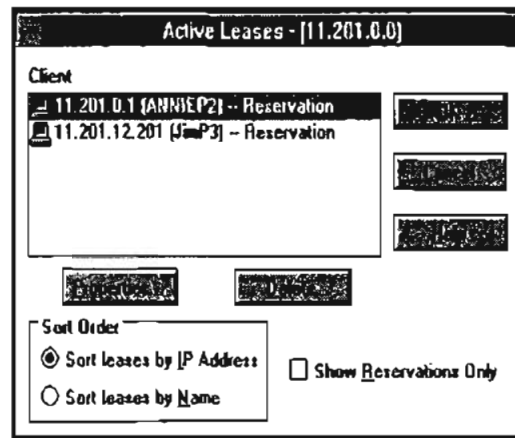
---

## Managing Client Leases

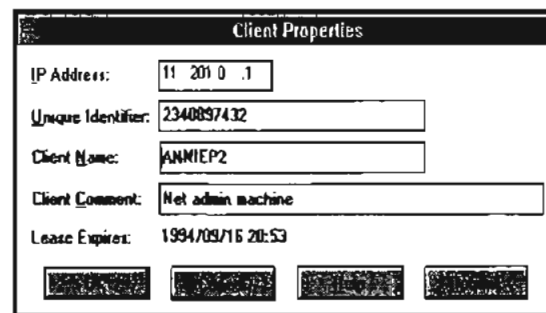
The lease for the IP address assigned by a DHCP server has an expiration date, which the client must renew if it is going to continue to use that address. You can view the lease duration and other information for specific DHCP clients, and you can add options and change settings for reserved DHCP clients.

► **To view client lease information**

1. In the DHCP Servers list in the DHCP Manager window, select the scope for which you want to view or change client information.
2. From the Scope menu, choose Active Leases.



3. In the Active Leases dialog box, select the computer whose lease you want to view in the IP Address list, and then choose the Properties button.  
If you want to view only clients that use reserved IP addresses, check the Show Reservations Only box.
4. In the Client Properties dialog box, you can view the unique identifier and other client information, including the lease expiration date.



**Note** You can only edit the name, unique ID, and comment, or choose the Options button in the Client Properties dialog box for clients with reserved IP addresses.

For information about the Options button in this dialog box, see “Defining Options for Reservations” earlier in this chapter.

You can cancel the DHCP configuration information for a DHCP client that is no longer using an IP address or for all clients in the scope. This has the same effect as if the client’s lease expired—the next time that client computer starts, it must enter the rebinding state and obtain new TCP/IP configuration information from a DHCP server.

---

**Important** Delete only entries for clients that are no longer using the assigned DHCP configuration. Deleting an active client could result in duplicate IP addresses on the network, because deleted addresses will be assigned to new active clients.

You can use `ipconfig /release` at the command prompt for a DHCP client computer to delete an active client entry and safely free its IP address for reuse.

---

- ▶ **To cancel a client’s DHCP configuration**
  1. Make sure the client is not using the assigned IP address.
  2. In the IP Client list of the Active Leases dialog box, select the client you want to cancel, and then choose the Delete button.

## Managing Client Reservations

You can reserve a specific IP address for a client. Typically, you will need to reserve addresses in the following cases:

- For domain controllers if the network also uses LMHOSTS files that define IP addresses for domain controllers
- For clients that use IP addresses assigned using another method for TCP/IP configuration
- For assignment by RAS servers to non-DHCP clients
- For DNS servers

If multiple DHCP servers are distributing addresses in the same scope, the client reservations on each DHCP server should be identical. Otherwise, the DHCP reserved client will receive different IP addresses, depending on the responding server.

---

**Important** The IP address and static name specified in WINS take precedence over the IP address assigned by the DHCP server. For such clients, create client reservations with the IP address that is defined in the WINS database.

---

► To add a reservation for a client

1. From the Scope menu, choose Add Reservations.

2. In the Add Reserved Clients dialog box, type information to identify the first reserved client:
  - IP Address specifies an address from the reserved address pool. You can specify any reserved, unused IP address. DHCP Manager checks and warns you if a duplicate or nonreserved address is entered.
  - Unique Identifier usually specifies the media access control (MAC) address for the client computer's network adapter card. You can determine this address by typing `net config wksta` at the command prompt on the client computer.
  - Client Name specifies the computer name for this client. This is used for identification purposes only and does not affect the actual computer name for the client. This is not available for MS-DOS-based clients; in this case, only the Unique Identifier appears.
  - Client Comment is any optional text that you enter to describe this client.
3. Choose the Add button to add the reservation to the DHCP database. You can continue to add reservations without dismissing this dialog box.
4. When you have added all reservations, choose the Close button.

After the IP address is reserved in DHCP Manager, the client computer must be restarted to be configured with the new IP address.

If you want to change a reserved IP address for a client, you have to remove the old reserved address and add a new reservation. You can change any other information about a reserved client while keeping the reserved IP address.

- ▶ **To change the reserved IP address**
  1. Make sure the reserved client is not using the old IP address. To do this, shut down the client computer immediately after issuing the **ip config/release** command on that client computer.
  2. In the Active Leases dialog box, select the reserved IP address in the Client list, and choose the Delete button. Then choose the OK button.
  3. From the Scope menu, choose Add Reservations, and then enter information for a new reservation as described earlier in this section.
  
- ▶ **To change basic information for a reserved client**
  1. From the Scope menu, choose Active Leases.
  2. In the Client list of the Active Leases dialog box, select the address of the reserved client that you want to change, and then choose the Properties button.
  3. In the Client Properties dialog box, change the unique identifier, client name, or comment, and then choose the OK button.

---

**Note** You can only change values in the Client Properties dialog box for reserved clients.

---

You can also view and change the options types that define configuration parameters for selected reserved clients by choosing the Options button in the Client Properties dialog box. Changing options for a reserved client follows the same procedure as use to originally define options, as described in “Defining Options for Reservations” earlier in this chapter.

## Managing the DHCP Database Files

The following files are stored in the `\systemroot\SYSTEM32\DHCP` directory that is created when you set up a DHCP server:

- DHCP.MDB is the DHCP database file.
- DHCP.TMP is a temporary file that DHCP creates for temporary database information.

- JET.LOG and the JET\*.LOG files contain logs of all transactions done with the database. These files are used by DHCP to recover data if necessary.
- SYSTEM.MDB is used by DHCP for holding information about the structure of its database.

---

**Caution** The DHCP.TMP, DHCP.MDB, JET.LOG, and SYSTEM.MDB files should not be removed or tampered with.

---

The DHCP database and related Registry entries are backed up automatically at a specific interval (15 minutes by default), based on the value of Registry parameters (as described later in this chapter).

## Troubleshooting DHCP

The following error conditions can appear to indicate potential problems with the DHCP server:

- The administrator can't connect for a DHCP server using DHCP Manager. The message that appears might be, "The RPC server is unavailable."
- DHCP clients cannot renew the leases for their IP addresses. The message that appears on the client computer is, "The DHCP client could not renew the IP address lease."
- The DHCP Client service or Microsoft DHCP Server service may be down and cannot be restarted.

The first task is to make sure the DHCP services are running.

► **To ensure the DHCP services are running**

1. Use the Services option in Control Panel to verify that the DHCP services are running.

In the Services dialog box for the client computer, Started should appear in the Status column for the DHCP Client service. For the DHCP server itself, the Started should appear in the Status column for the Microsoft DHCP Server service.

2. If a necessary service is not started on either computer, start the service.

In rare circumstances, the DHCP server may not boot or a STOP error may occur. If the DHCP server is down, follow these steps to restart.



- ▶ **To restart a DHCP server that is down**
  1. Turn off the power to the server and wait one minute.
  2. Turn on the power, start Windows NT Server, and log on under an account with Administrator rights.
  3. At the command prompt, type `net start dhcpserver` and press ENTER.

---

**Note** Use Event Viewer to find the possible source of problems with DHCP services.

---

## Restoring the DHCP Database

If you ascertain that the DHCP services are running on both the client and server computers but the error conditions described earlier persist, then the DHCP database is not available or has become corrupted. If a DHCP server fails for any reason, you can restore the database from the automatic backup files.

- ▶ **To restore a DHCP database**
  - Restart the DHCP server. If the DHCP database has become corrupted, it is automatically restored from the DHCP backup directory specified in the Registry, as described later in this chapter.
- ▶ **To force the restoration of a DHCP database**
  - Set the value of **RestoreFlag** in the Registry to 1, and then restart the computer. For information about this parameter, see “Registry Parameters for DHCP Servers” later in this chapter.
- ▶ **To manually restore a DHCP database**
  - If the two restore methods described earlier do not work, manually copy all DHCP database files from the backup directory to the \DHCP working directory. Then restart the Microsoft DHCP Server service.

## Backing up the DHCP Database onto Another Computer

You may also find a situation where you need to backup a DHCP database to another computer. To do this, follow these steps.

- ▶ **To move a DHCP database**
  - Use the Replicator service to copy the contents of the DHCP backup directory to the new computer.

## Advanced Configuration Parameters for DHCP

This section presents configuration parameters that affect the behavior of DHCP servers and clients, and that can be modified only through Registry Editor. For the changes to take effect after you modify any of these value entries, you must restart the Microsoft DHCP Server service for server parameters or the DHCP Client service for client parameters.

---

---

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

---

---

► **To make changes to the DHCP server or client configuration using Registry Editor**

1. Run REGEDT32.EXE from File Manager or Program Manager, or at a command prompt, type **start regedt32** and press ENTER.

When the Registry Editor window appears, you can press F1 to get Help on how to make changes in Registry Editor.

2. In Registry Editor, click the window titled HKEY\_LOCAL\_MACHINE on Local Machine, and then click the icons for the SYSTEM subtree until you reach the subkey for the specific parameter, as described in the following sections.

The following sections describe the value entries for parameters for DHCP servers and clients that can be set only by adding an entry or changing their values in Registry Editor.

## Registry Parameters DHCP Servers

When you change any of these parameters except **RestoreFlag**, you must restart the computer for the changes to take effect. For the **RestoreFlag** parameter, you must restart the Microsoft DHCP Server service.

The Registry parameters for DHCP servers are specified under the following key:

```
..SYSTEM\current\currentcontrolset\services\DHCPserver\Parameters
```

### APIProtocolSupport

Data type = REG\_DWORD

Range = 0x1, 0x2, 0x4, 0x5, 0x7

Default = 0x1

Specifies the supported protocols for the DHCP server. You can change this value to ensure that different computers running different protocols can access the DHCP server. The values for this parameter can be the following:

- 0x1 For RPC over TCP/IP protocols
- 0x2 For RPC over named pipes protocols
- 0x4 For RPC over local procedure call (LPC) protocols
- 0x5 For RPC over TCP/IP and RPC over LPC
- 0x7 For RPC over all three protocols (TCP/IP, named pipes, and LPC)

### BackupDatabasePath

Data type = REG\_EXPAND\_SZ

Range = *filename*

Default = %SystemRoot%\system32\dhcp\backup

Specifies the location of the backup database file where the database is backed up periodically. The best location for the backup file is on another hard drive, so that the database can be recovered in case of a system drive crash. Do not specify a network drive, because DHCP Manager cannot access a network drive for database backup and recovery.

**BackupInterval**

Data type = REG\_DWORD

Range = no limit

Default = 15 minutes

Specifies the interval for backing up the database.

**DatabaseCleanupInterval**

Data type = REG\_DWORD

Range = No limit

Default = 0x15180 (864,000 minutes — 24 hours)

Specifies the interval for cleaning up expired client records from the DHCP database, freeing up those IP addresses for reuse.

**DatabaseLoggingFlag**

Data type = REG\_DWORD

Range = 0 or 1

Default = 1 (true—that is, database logging is enabled)

Specifies whether to record the database changes in the JET.LOG file. This log file is used after a system crash to recover changes that have not been made to the database file defined by **DatabaseName**. Database logging affects system performance, so **DatabaseLogging** can be turned off if you believe the system is highly stable and if logging is adversely affecting system performance.

**DatabaseName**

Data type = REG\_SZ

Range = *filename*

Default = dhcp.mdb

Specifies the name of the database file to be used for the DHCP client information database.

**DatabasePath**

Data type = REG\_EXPAND\_SZ

Range = *pathname*

Default = %SystemRoot%\System32\dhcp

Specifies the location of the database files that have been created and opened.

**RestoreFlag**

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (false—that is, do not restore)

Specifies whether to restore the database from the backup directory. This flag is reset automatically after the successful restoration of the database.

## Registry Parameters for DHCP Clients

The Registry parameters for DHCP clients are specified under the following key:

```
..SYSTEM\current\currentcontrolset\services\DHCP\Parameter\<option#>
```

The *Option#* keys are a list of DHCP options that the client can request from the DHCP server. For each of the default options, the following values are defined:

### RegLocation

Data type = REG\_SZ

Default = Depends on the Registry location for the specific option

Specifies the location in the Registry where the option value is written when it is obtained from the DHCP server. The “?” character expands to the adapter name for which this option value is obtained.

### KeyType

Data type = REG\_DWORD

Default = 0x7

Specifies the type of Registry key for the option.

## Guidelines for Setting Local Policies

This section provides some suggestions for setting lease options, dividing the free address pool among DHCP servers, and avoiding DNS naming problems.

## Guidelines for Managing DHCP Addressing Policy

Allocation of IP addresses for distribution by DHCP servers can be done dynamically or manually. These methods use the same DHCP client-server protocol, but the network administrator manages them differently at the DHCP server.

### Dynamic Allocation of IP Addresses

Dynamic allocation allows a client to be assigned an IP address from the free address pool. The lease for the address has a lease duration (expiration date), before which the client must renew the lease to continue using that address. Depending on the local lease policies defined by the administrator, dynamically allocated addresses can be returned to the free address pool if the client computer is not being used, if it is moved to another subnet, or if its lease expires. Any IP addresses that are returned to the free address pool can be reused by the DHCP server when allocating an IP address to a new client. Usually the local policy ensures that the same IP address is assigned to a client each time that system starts and that addresses returned to the pool are reassigned.

After the renewal time of the lease time has passed, the DHCP client enters the *renewing* state (as described in Chapter 3, "Networking Concepts for TCP/IP"). The client sends a request message to the DHCP server that provided its configuration information. If the request for a lease extension fits the local lease policy, the DHCP server sends an acknowledgment that contains the new lease and configuration parameters. The client then updates its configuration values and returns to the bound state.

When the DHCP client is in the *renewing* state, it must release its address immediately in the rare event that the DHCP server sends a negative acknowledgment. The DHCP server sends this message to inform a client that it has incorrect configuration information, forcing it to release its current address and acquire new information.

If the DHCP client cannot successfully renew its lease, the client enters a *rebinding* state. At this stage, the client sends a request message to all DHCP servers in its range, attempting to renew its lease. Any server that can extend the lease sends an acknowledgment containing the extended lease and updated configuration information. If the lease expires or if a DHCP server responds with a negative acknowledgment, the client must release its current configuration and return to the initializing state. (This happens automatically, for example, for a computer that is moved from one subnet to another.)

If the DHCP client uses more than one network adapter to connect to multiple networks, this protocol is followed for each adapter that the user wants to configure for TCP/IP. Windows NT allows multihomed systems to selectively configure any combination of the system's interfaces. You can use the `ipconfig` utility to view the local IP configuration for a client computer.

When a DHCP-enabled computer is restarted, it sends a message to the DHCP server with its current configuration information. The DHCP server either confirms this configuration or sends a negative reply so that the client must begin the initializing stage again. System startup might therefore result in a new IP address for a client computer, but neither the user nor the network administrator has to take any action in the configuration process.

## Manual Allocation of IP Addresses

Manual allocation follows the policy used in most current TCP/IP implementations. With this method, the network administrator defines the IP address and other configuration options that the DHCP servers will provide for a particular computer. The DHCP servers respond based on the client's unique identifier, which is the network adapter's MAC-layer address. Any IP addresses assigned in this way cannot be allocated by DHCP servers to other clients using either automatic or dynamic allocation. The address has a permanent lease.

For example, for the range of IP addresses to be provided through RAS servers, these addresses should be manually excluded from the range of dynamically allocated addresses.

## Guidelines for Lease Options

To define appropriate values for lease duration, you should consider the frequency of the following events for your network:

- Changes to DHCP options and default values
- Network interface failures
- Computer removals for any purpose
- Subnet changes by users because of office moves, laptop computers docked at different workstations, and so on

All of these types of events cause IP addresses to be released by the client or cause the leases to expire at the DHCP server. Consequently, the IP addresses will be returned to the free address pool to be reused.

If many changes occur on your internetwork, you should assign short lease times, such as two weeks. This way, the addresses assigned to systems that leave the subnet can be reassigned quickly to new DHCP client computers requesting TCP/IP configuration information.

Another important factor is the ratio between connected computers and available IP addresses. For example, the demand for reusing addresses is low in a network where 40 systems share a class C address (with 254 available addresses). A long lease time such as two months would be appropriate in such a situation. However, if 230 computers share the same address pool, demand for available addresses is much greater, so a lease time of a few days or weeks is more appropriate.

Notice, however, that short lease durations require that the DHCP server be available when the client seeks to renew the lease. So backup servers are especially important when short lease durations are specified.

## Guidelines for Partitioning the Address Pool

You will probably decide to install more than one DHCP server, so the failure of any individual server will not prevent DHCP clients from starting. However, DHCP does not provide a way for DHCP servers to cooperate in ensuring that assigned addresses are unique. Therefore, you must divide the available address pool among the DHCP servers to prevent duplicate address assignment.

A typical scenario is a local DHCP server that maintains TCP/IP configuration information for two subnets. For each DHCP server, the network administrator allocates 70 percent of the IP address pool for local clients and 30 percent for clients from the remote subnet, and then configures a relay agent to deliver requests between the subnets.

This scenario allows the local DHCP server to respond to requests from local DHCP clients most of the time. The remote DHCP server will assign addresses to clients on the other subnet only when the local server is not available or is out of addresses. This same method of partitioning among subnets can be used in a multiple subnet scenario to ensure the availability of a responding server when a DHCP client requests configuration information.

## Guidelines for Avoiding DNS Naming Conflicts

DNS can be used to provide names for network resources, as described in Chapter 3, "Networking Concepts for TCP/IP." However, DNS configuration is static. With DHCP, a host can easily have a different IP address if its lease expires or for other reasons, but there is no standard for updating DNS servers dynamically when IP address information changes. Therefore, DNS naming conflicts can occur if you are using DHCP for dynamic allocation of IP addresses.

This problem will primarily affect systems that extend internetworking services to local network users. For example, a server acting as an anonymous FTP server or as an e-mail gateway might require users to contact it using DNS names. In such cases, such clients should have reserved leases with an unlimited duration..

For workstations in environments that do not require the computers to register in the DNS name space, DHCP dynamic allocation can be used without problems.



## Using DHCP with Diskless Workstations

If your network includes diskless workstations or X terminal BOOTP clients that need configuration information to use TCP/IP, you must build profiles. (BOOTP is the internetworking Bootstrap Protocol used to configure systems across internetworks. DHCP is an extension of BOOTP.)

You might decide to continue to manage these workstations using your existing BOOTP servers. If so, you must be sure to exclude these addresses from the free address pool maintained by the DHCP server.

## Planning a Strategy for DHCP

This section describes how to develop strategies for placing DHCP servers on small-scale and large-scale installations. Most network administrators implementing DHCP will also be planning a strategy for implementing WINS servers. The planning tasks described here also apply for WINS servers, and in fact, the administrator will probably want to plan DHCP and WINS implementation in tandem.

The following describes the general planning tasks:

1. Compile a list of a requirements, including:
  - Client support (numbers and kinds of systems to be supported)
  - Interoperability with existing systems, especially requirements for mission-critical accounting, personnel, and similar information systems
  - Hardware support and related software compatibility (including routers, switches, and servers)
  - Network monitoring software, including SNMP requirements and other tools
2. Isolate the areas of the network where processes must continue uninterrupted, and target these areas for the last stages of implementation.
3. Review the geographic and physical structure of the network to determine the best plan for defining logical subnets as segments of the internetwork.
4. Define the components in the new system that require testing, and develop a phase plan for testing and adding components.

For example, the plan could define units of the organization to be phased into using DHCP, and the order for types of computers to be phased in (including Windows NT servers and workstations, Microsoft RAS servers and clients, Windows for Workgroups computers, and MS-DOS clients).

5. Create a pilot project for testing. Be sure that the pilot project addresses all the requirements identified in Task #1.
6. Create a second test phase, including tuning the DHCP (and WINS) server-client configuration for efficiency. This task can include determining strategies for backup servers and for partitioning the address pool at each server to be provided to local versus remote clients.
7. Document all architecture and administration issues for network administrators.
8. Implement a final phase for bringing all organizational units into using DHCP.

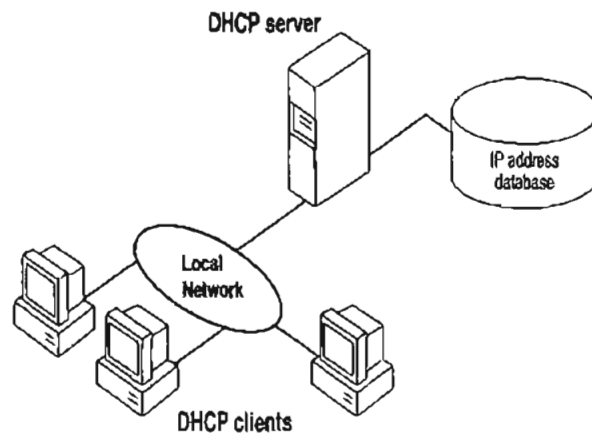
While planning, remember that the actual placement of the servers in the physical network need not be a major planning issue. DHCP servers (and WINS servers) do not participate in the Windows NT Server domain model, so domain membership is not an issue in planning for server placement. Because most routers can forward DHCP configuration requests, DHCP servers are not required on every subnet in the internetwork. Also, because these servers can be administered remotely from any Windows NT Server computer that is DHCP- or WINS-enabled, location is not a major issue in planning for server placement.

## Planning a Small-Scale Strategy for DHCP Servers

For a small LAN that does not include routers and subnetting, the server needs for the network can probably be provided with a single DHCP server.

Planning in this case includes determining the following:

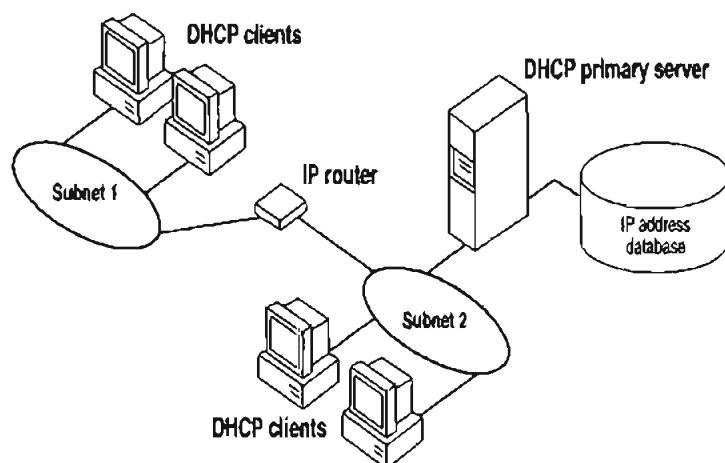
- The hardware and storage requirements for the DHCP server
- Which computers can immediately become DHCP clients for dynamic addressing and which should keep their static addresses
- The DHCP option types and their values to be predefined for the DHCP clients



A Single Local Network Using Automatic TCP/IP Configuration with DHCP

## Planning a Large-Scale Strategy for DHCP Servers

The network administrator can use relay agents implementing RFC 1542 (usually IP routers) so that DHCP servers located on one node of the internetwork can respond to TCP/IP configuration requests from remote nodes. The relay agent forwards requests from local DHCP clients to the DHCP server and subsequently relays responses back to the clients.



### An Internetwork Using Automatic TCP/IP Configuration with DHCP

The additional planning issues for a large enterprise network includes:

- Compatibility of hardware and software routers with DHCP, as described at the beginning of this chapter.
- Planning the physical subnetting of the network and relative placement of DHCP servers. This includes planning for placement of DHCP (and WINS servers) among subnets in a way that reduces b-node broadcasts across routers.
- Specifying the DHCP option types and their values to be predefined per scope for the DHCP clients. This may include planning for scopes based on the needs of particular groups of users. For example, for a marketing group that uses portable computers docked at different stations, or for a unit that frequently moves computers to different locations, shorter lease durations can be defined for the related scopes. This way, frequently changed IP addresses can be freed for reuse.

As one example, the segmenting of the WAN into logical subnets could match the physical structure of the internetwork. Then one IP subnet can serve as the backbone, and off this backbone each physical subnet would maintain a separate IP subnet address.

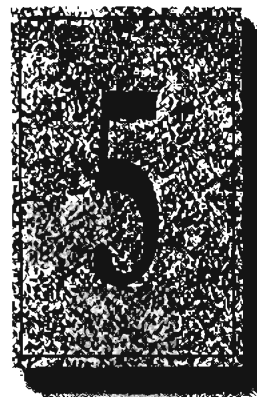
In this case, for each subnet a single computer running Windows NT Server could be configured as both the DHCP and WINS server. Each server would administer a defined number of IP addresses with a specific subnet mask, and would also be defined as the default gateway. Because the server is also acting as the WINS server, it can respond to name resolution requests from all systems on its subnet.

These DHCP and WINS servers can in turn be backup servers for each other. The administrator can partition the address pool for each server to provide addresses to remote clients.

There is no limit to the maximum number of clients that can be served by a single DHCP server. However, your network may have practical constraints based on the IP address class and server configuration issues such as disk capacity and CPU speed.

## CHAPTER 5

# Installing and Configuring WINS Servers



A WINS server is a Windows NT Server computer running Microsoft TCP/IP and the Windows Internet Name Service (WINS) server software. WINS servers maintain a database that maps computer names to IP addresses, allowing users to easily communicate with other computers while gaining all the benefits of TCP/IP.

This chapter describes how to install WINS servers and how to use WINS Manager to manage these servers. The topics include the following:

- WINS benefits
- Installing and administering WINS servers
- Configuring WINS servers and replication partners
- Managing static mappings
- Setting preferences for WINS Manager
- Managing the WINS database
- Troubleshooting WINS
- Advanced configuration parameters for WINS
- Planning a strategy for WINS servers

For an overview of how WINS works, see “Windows Internet Name Service and Broadcast Name Resolution” in Chapter 3, “Networking Concepts for TCP/IP.”

---

**Note** WINS can also be configured and monitored using SNMP. All configuration parameters can be set using SNMP, including configuration parameters that can otherwise only be set by editing the Registry. For a list of WINS MIB object types, see Appendix A, “MIB Object Types for Windows NT.”

You can also use Performance Monitor to track WINS server performance, as described in Chapter 8, “Using Performance Monitor with TCP/IP Services.”

---

## WINS Benefits

Using WINS servers can offer these benefits on your internetwork:

- Dynamic database maintenance to support computer name registration and name resolution. Although WINS provides dynamic name services, it offers a NetBIOS namespace, making it much more flexible than DNS for name resolution.
- Centralized management of the computer name database and the database replication policies, alleviating the need for managing LMHOSTS files.
- Dramatic reduction of IP broadcast traffic in Microsoft internetworks, while allowing client computers to easily locate remote systems across local or wide area networks.
- The ability for clients on a Windows NT Server network (including Windows NT, Windows for Workgroups, and LAN Manager 2.x) to browse domains on the far side of a router without a local domain controller being present on the other side of the router.
- A scalable design, making it a good choice for name resolution for medium to very large internetworks.

---

**Note** WINS client software is part of the Microsoft TCP/IP-32 for Windows for Workgroups and the Microsoft Network Client 2.0 software that is included on the Windows NT Server compact disc. For information about installing these clients, see the *Windows NT Server Installation Guide*.

---

## Installing WINS Servers

You install a WINS server as part of the process of installing Microsoft TCP/IP in Windows NT Server. These instructions assume you have already installed the Windows NT Server operating system on the computer.



You must be logged on as a member of the Administrators group to install a WINS server.

► **To install a WINS server**

1. Choose the Network options in Control Panel. When the Network Settings dialog box appears, choose the Add Software button.
2. In the Network Software list in the Add Network Software dialog box, select TCP/IP Protocol And Related Components, and then choose the Continue button.

3. In the Windows NT TCP/IP Installation Options dialog box, check the appropriate options to install, including at least the following:
  - WINS Server Service
  - SNMP Service (for configuring and monitoring WINS using SNMP or Performance Monitor)
4. Choose the OK button. Windows NT Setup displays a message asking for the full path to the Windows NT Server distribution files. Type the appropriate location, and choose the Continue button.

All necessary files are copied to your hard disk.
5. Complete all the required procedures for manually configuring TCP/IP as described in “Configuring TCP/IP” in Chapter 2. When the Network Settings dialog box reappears after you finish configuring TCP/IP, choose the Close button.

All the appropriate TCP/IP and WINS server software is ready for use after you reboot the computer.

The Windows Internet Name Service is a Windows NT service running on a Windows NT computer. The supporting WINS client software is automatically installed for Windows NT Server and for Windows NT computers when the basic operating system is installed.

► **To start and stop the WINS service on any Windows NT computer**

1. In Control Panel, choose the Services icon.

–Or–

In Server Manager, choose Services from the Computer menu.
2. In the Services dialog box, select the Windows Internet Name Service, and choose the Start or Stop button. Then choose the Close button.

You can start and stop the WINS service at the command prompt using the commands `net start wins` or `net stop wins`.

## Administering WINS Servers

When you install a WINS server, an icon for WINS Manager is added to the Network Administration group in Program Manager. You can use this tool to view and change parameters for any WINS server on the internetwork. To administer a WINS server remotely, you can run WINS Manager on a Windows NT Server computer that is not a WINS server.



You must be logged on as a member of the Administrators group for a WINS server to configure that server.

► To start WINS Manager



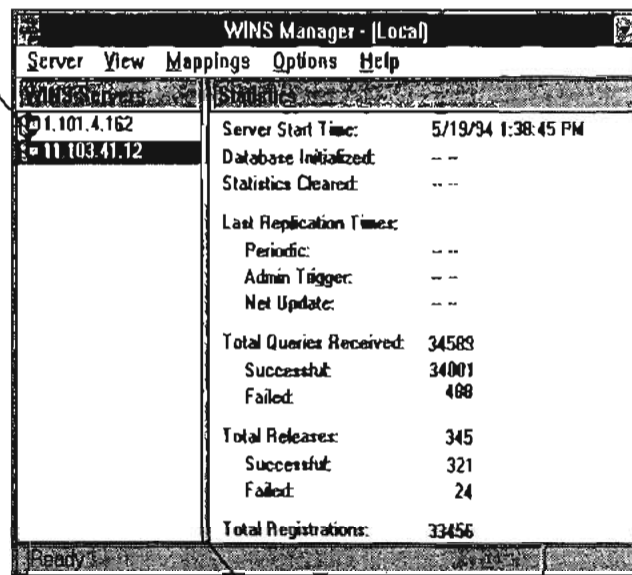
1. Double-click the WINS Manager icon in Program Manager.

–Or–

At the command prompt, type **start winsadm** and press ENTER. You can include a WINS server name or IP address with the command, for example, **start winsadm 11.103.41.12** or **start winsadm myserver**.

2. If the Windows Internet Name Service is running on the local computer, that WINS server is opened automatically for administration. If the Windows Internet Name Service is not running when you start WINS, the Add WINS Server dialog box appears, as described in the following procedure.

Settings in the Preferences dialog box determine whether the IP address or computer name appears first in the list.



— Drag the split bar to size the panes.

**Note** If you specify an IP address when connecting to a WINS server, the connection is made using TCP/IP. If you specify a computer name, the connection is made over NetBIOS. The list that appears in the WINS Server window shows the IP address first if you connected using TCP/IP, or the computer name first, if the connection was made over NetBIOS.

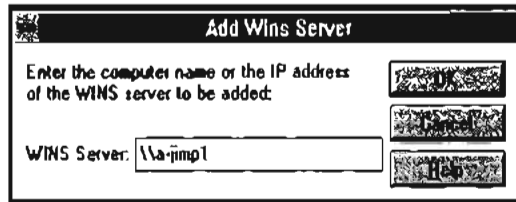


► **To connect to a WINS server for administration**

- In the WINS Manager window, select a server in the WINS Servers list. This list contains all WINS servers that you previously connected to or that have been reported by partners of this WINS server.

–Or–

1. If you want to select another server that you have not previously connected to, choose the Add WINS Server command from the Server menu.



2. In the WINS Server box of the Add WINS Server dialog box, type the IP address or computer name of the WINS server you want to work with, and then choose the OK button. (You do not have to include double backslashes before the name. WINS Manager will add these for you.)

The title bar in the WINS Manager window shows the IP address or computer name for the currently selected server, depending on whether you used the address or name to connect to the server. WINS Manager also shows some basic statistics for the selected server, as described in the following table. Additional statistics can be displayed by choosing the Detailed Information command from the Server menu.

**Statistics in WINS Manager**

Statistic	Meaning
Database Initialized	The time when this WINS database was initialized.
Statistics Cleared	The time when statistics for the WINS server were last cleared with the Clear Statistics command from the View menu.
Last Replication Times	The times at which the WINS database was last replicated.
Periodic	The last time the WINS database was replicated based on the replication interval specified in the Preferences dialog box.
Admin Trigger	The last time the WINS database was replicated because the administrator chose the Replicate Now button in the Replication Partners dialog box.

---

**Statistics in WINS Manager** (*continued*)

<b>Statistic</b>	<b>Meaning</b>
Net Update	The last time the WINS database was replicated as a result of a network request, which is a push notification message that requests propagation.
Total Queries Received	The number of <i>name query request</i> messages received by this WINS server. Successful indicates how many names were successfully matched in the database, and Failed indicates how many names this WINS server could not resolve.
Total Releases	The number of messages received that indicate a NetBIOS application has shut itself down. Successful indicates how many names were successfully released, and Failed indicates how many names this WINS server could not release.
Total Registrations	The number of messages received that indicate name registrations for clients.

---

**► To refresh the statistical display in WINS Manager**

- From the View menu, choose the Refresh Statistics command, or press F5.

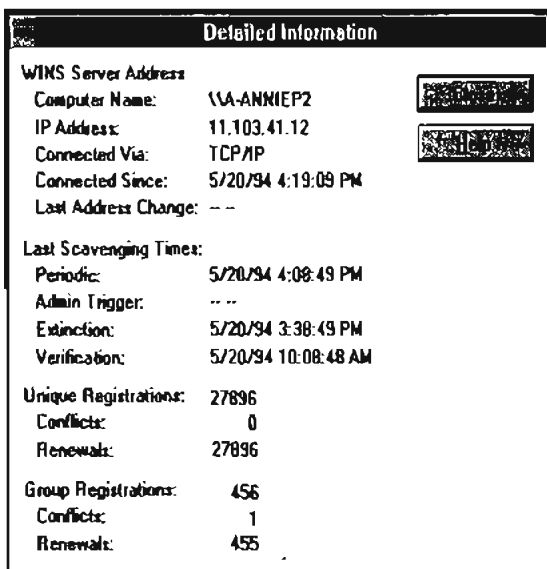
–Or–

From the View menu, choose the Clear Statistics command to reset all statistical counters.

–Or–

Use automatic screen refreshing, based on the interval you specify in the Preferences dialog box, as described in “Setting Preferences for WINS Manager” later in this chapter.

- To see information about the current WINS server
1. From the Server menu, choose the Detailed Information command.



The Detailed Information dialog box shows information about the selected WINS server, as described in the table below.

2. To dismiss the Detail Information dialog box, choose the Close button.

#### Detailed Information Statistics for WINS Manager

Statistic	Meaning
Last Address Change	Indicates the time at which the last WINS database change was replicated.
Last Scavenging Times	The last times that the database was cleaned for specific types of entries. (For information about database scavenging, see "Managing the WINS Database" later in this chapter.
Periodic	Indicates when the database was cleaned based on the renewal interval specified in the WINS Server Configuration dialog box.
Admin Trigger	Indicates when the database was last cleaned because the administrator chose the Initiate Scavenging command.

**Detailed Information Statistics for WINS Manager** *(continued)*

<b>Statistic</b>	<b>Meaning</b>
Extinction	Indicates when the database was last cleaned based on the Extinction interval specified in the WINS Server Configuration dialog box.
Verification	Indicates when the database was last cleaned based on the Verify interval specified in the WINS Server Configuration dialog box.
Unique Registrations	The number of <i>name registration requests</i> that have been accepted by this WINS server.
Unique Conflicts	The number of conflicts encountered during registration of unique names owned by this WINS server.
Unique Renewals	The number of renewals received for unique names.
Group Registrations	The number of registration requests for groups that have been accepted by this WINS server. For information about groups, see “Managing Special Names” later in this chapter.
Group Conflicts	The number of conflicts encountered during registration of group names.
Group Renewals	The number of renewals received for group names.

For descriptions of the related intervals, see “Configuring WINS Servers” later in this chapter.

## Configuring WINS Servers and Replication Partners

You will want to configure multiple WINS servers to increase the availability and balance the load among servers. Each WINS server must be configured with at least one other WINS server as its replication partner.

Configuring a WINS server includes specifying information about when database entries are replicated between partners. A *pull partner* is a WINS server that pulls in replicas of database entries from its partner by requesting and then accepting replicas. A *push partner* is a WINS server that sends update notification messages to its partner when its WINS database has changed. When its partner responds to the notification with a replication request, the push partner sends a copy of its current WINS database to the partner.

For information about configuring preferences, see “Setting Preferences for WINS Manager” later in this chapter.

## Configuring WINS Servers

For each WINS server, you must configure threshold intervals for triggering database replication, based on a specific time, a time period, or a certain number of new records. If you designate a specific time for replication, this occurs one time only. If a time period is specified, replication is repeated at that interval.

### ► To configure a WINS server

1. From the Server menu, choose the Configuration command.

This command is available only if you are logged on as a member of the Administrators group for the WINS server you want to configure.

2. To view all the options in this dialog box, choose the Advanced button.

**WINS Server Configuration - \\RONALDM2**

**WINS Server Configuration**

Renewal Interval (h:m:s): 0 : 40 : 00

Exinction Interval (h:m:s): 8 : 00 : 00

Exinction Timeout (h:m:s): 8 : 00 : 00

Verify Interval (h:m:s): 160 : 00 : 00

**Pull Parameters**

Initial Replication

Retry Count: 3

**Push Parameters**

Initial Replication

Replicate on Address Change

**Advanced WINS Server Configuration**

Logging Enabled

Starting Version Count (hex): 0

Log Detailed Events

Database Backup Path: D:\users\test

Replicate Only With Partners

Backup On Termination

Migrate On/Diff

3. For the configuration options in the WINS Server Configuration dialog box, specify time intervals using the spin buttons, as described in the following list.

Configuration option	Meaning
Renewal Interval	Specifies how often a client reregisters its name. The default is five hours.
Extinction Interval	Specifies the interval between when an entry is marked as <i>released</i> and when it is marked as <i>extinct</i> . The default is four times the renewal interval.
Extinction Timeout	Specifies the interval between when an entry is marked <i>extinct</i> and when the entry is finally scavenged from the database. The default is the same as the renewal interval.
Verify Interval	Specifies the interval after which the WINS server must verify that old names it does not own are still active. The default is 20 times the extinction interval.

The replication interval for this WINS server's pull partner is defined in the Preferences dialog box, as described in "Setting Preferences for WINS Manager" later in this chapter.

4. If you want this WINS server to pull replicas of new WINS database entries from its partners when the system is initialized or when a replication-related parameter changes, check Initial Replication in the Pull Parameters options, and then type a value for Retry Count.

The retry count is the number of times the server should attempt to connect (in case of failure) with a partner for pulling replicas. Retries are attempted at the replication interval specified in the Preferences dialog box. If all retries are unsuccessful, WINS waits for a period before starting replication again. For information about setting the start time and replication interval for pull and push partners, see "Setting Preferences for WINS Manager" later in this chapter.

5. To inform partners of the database status when the system is initialized, check Initial Replication in the Push Parameters group. To inform partners of the database status when an address changes in a mapping record, check Replicate On Address Change.
6. Set any Advanced WINS Server Configuration options, as described in the following table.

7. When you have completed all changes in the WINS Server Configuration dialog box, choose the OK button.

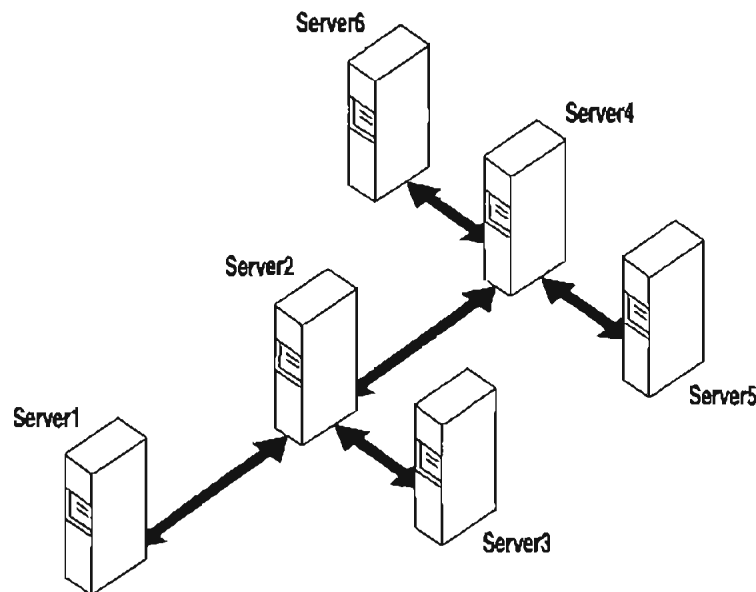
#### Advanced WINS Server Configuration Options

Configuration option	Meaning
Logging Enabled	Specifies whether logging of database changes to JET.LOG should be turned on.
Log Detailed Events	Specifies whether logging events is verbose. (This requires considerable system resources and should be turned off if you are tuning for performance.)
Replicate Only With Partners	Specifies that replication will be done only with WINS pull or push partners. If this option is not checked, an administrator can ask a WINS server to pull or push from or to a non-listed WINS server partner. By default, this option is checked.
Backup On Termination	Specifies that the database will be backed up automatically when WINS Manager is closed.
Migrate On/Off	Specifies that static unique and multihomed records in the database are treated as dynamic when they conflict with a new registration or replica. This means that if they are no longer valid, they will be overwritten by the new registration or replica. Check this option if you are upgrading non-Windows NT systems to Windows NT. By default, this option is not checked.
Starting Version Count	Specifies the highest version ID number for the database. Usually, you will not need to change this value unless the database becomes corrupted and needs to start fresh. In such a case, set this value to a number higher than appears as the version number counter for this WINS server on all the remote partners that earlier replicated the local WINS server's records. This value can be seen in the View Database dialog box in WINS Manager.
Database Backup Path	Specifies the directory where the WINS database backups will be stored. WINS uses this directory to perform an automatic restoration of the database in the event that the database is found to be corrupted when WINS is started. Do not specify a network directory.

## Configuring Replication Partners

WINS servers communicate among themselves to fully replicate their databases, ensuring that a name registered with one WINS server is eventually replicated to all other WINS servers within the internetwork. All mapping changes converge within the *replication period* for the entire WINS system, which is the maximum time for propagating changes to all WINS servers. All released names are propagated to all WINS servers after they become extinct, based on the interval specified in WINS Manager.

Replication is carried out among replication partners, rather than each server replicating to all other servers. In the following illustration, Server1 has only Server2 as a partner, but Server2 has three partners. So, for example, Server1 gets all replicated information from Server2, but Server2 gets information from Server1, Server3, and Server4.



**Replication Configuration Example for WINS Servers**

Ultimately, all replications are pulled from the other WINS servers on an internetwork, but triggers are sent by WINS servers to indicate when a replication should be pulled. To achieve replication, each WINS server is a push partner or pull partner with at least one other WINS server. A pull partner is a WINS server that pulls in database replicas from its push partner by requesting and then accepting replicas of new database entries in order to synchronize its own database. A push partner is a WINS server that sends notification of changes and then sends replicas to its pull partner upon receiving a request. When the server's pull partner replicates the information, it pulls replicas by asking for all records with a higher version number than the last record stored from the last replication for that server.



Choosing whether to configure another WINS server as a push partner or pull partner depends on several considerations, including the specific configuration of servers at your site, whether the partner is across a wide area network (WAN), and how important it is to propagate the changes.

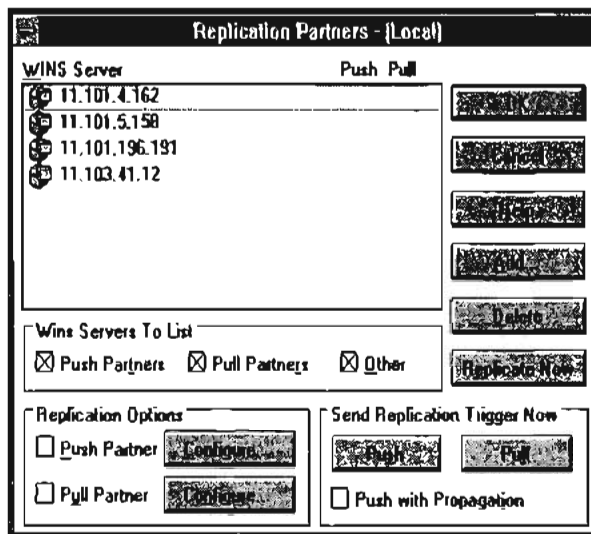
- If Server2, for example, needs to perform pull replications with ServerB, make sure it is a push partner of Server3.
- If Server2 needs to push replications to Server3, it should be a pull partner of WINS ServerB.

Replication is triggered when a WINS server polls another server to get a replica. This can begin at system startup and can also be at a specific time, and it can then repeat at the time interval specified for periodic replication. Replication is also triggered when a WINS server reaches a threshold set by the administrator, which is an *update count* for registrations and changes. In this case, the server notifies its pull partners that it has reached this threshold, and the other servers may then decide to pull replicas.

► **To add a replication partner for a WINS server**

1. From the Server menu, choose the Replication Partners command.

This command is available only if you are logged on as a member of the Administrators group for the local server.



2. In the Replication Partners dialog box, choose the Add button.
3. In the Add WINS Server dialog box, type the name or IP address of the WINS server that you want to add to the list, and then choose the OK button. If WINS Manager can find this server, it will add it to the WINS Server list in the Replication Partners dialog box.

4. From the WINS Server list in the Replication Partners dialog box, select the server you want to configure, and then complete the actions described in “Configuring Replication Partner Properties” later in this chapter.
5. If you want to limit which WINS servers are displayed in the Replication Partners dialog box, check or clear the options as follows:
  - Check Push Partners to display push partners for the current WINS server.
  - Check Pull Partners to display pull partners for the current WINS server.
  - Check Other to display the WINS servers that are neither push partners nor pull partners for the current WINS server.
6. To specify replication triggers for the partners you add, follow the procedures described in “Triggering Replication Between Partners” later in this chapter.
7. When you finish adding replication partners, choose the OK button.

► **To delete replication partners**

1. From the Server menu, choose the Replication Partners command.
2. In the Replication Partners dialog box, select one or more servers in the WINS Server list, and then choose the Delete button, or press DEL.

WINS Manager asks you to confirm the deletion if you checked the related confirmation option in the Preference dialog box, as described in “Setting Preferences for WINS Manager” later in this chapter.

## Configuring Replication Partner Properties

When you designate replication partners, you need to specify parameters for when replication will begin.

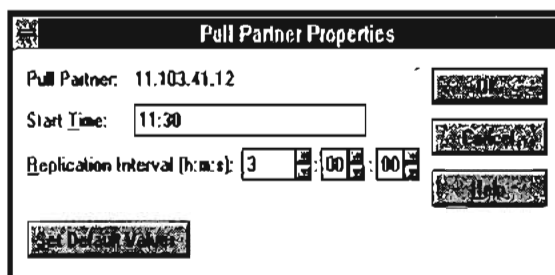
► **To configure replication partners for a WINS server**

1. In the WINS Server list of the Replication Partners dialog box, select the server you want to configure.
2. Check either Push Partner or Pull Partner or both to indicate the replication partnership you want, and then choose the related Configure button.
3. Complete the entries in the appropriate Properties dialog box, as described in the following procedures.

► **To define pull partner properties**

1. In the Start Time box of the Pull Partner Properties dialog box, type a time to indicate when replication should begin.

You can use any separator for hours, minutes, and seconds. You can type AM or PM, for example, only if these designators are part of your time setting, as defined using the International option in Control Panel.



2. In the Replication Interval box, type a time in hours, minutes, and seconds to indicate how often replications will occur, or use the spin buttons to set the time you want.

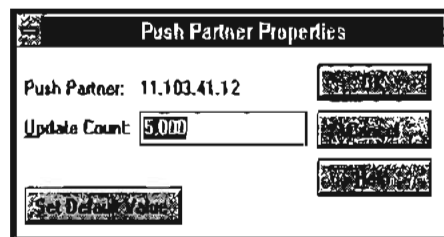
If you want to return to the values specified in the Preferences dialog box, choose the Set Default Values button.

3. Choose the OK button to return to the Replication Partners dialog box.

► **To define push partner properties**

1. In the Update Count box of the Push Partner Properties dialog box, type a number for how many additions and updates made to records in the database will result in changes that need replication. (Replications that have been pulled in from partners do not count as insertions or updates in this context.)

The minimum value for Update Count is 5.



If you want to return to the value specified in the Preferences dialog box, choose the Set Default Values button.

2. Choose the OK button to return to the Replication Partners dialog box.

## Triggering Replication Between Partners

You can also replicate the database between the partners immediately, rather than waiting for the start time or replication interval specified in the Preference dialog box, as described in “Setting Preferences for WINS Manager” later in this chapter.

You will probably want to begin replication immediately after you make a series of changes such as entering a range of static address mappings.

### ► To send a replication trigger

- In the Replication Partners dialog box, select the WINS servers to which you want to send a replication trigger, and then choose the Push or Pull button, depending on whether you want to send the trigger to push partners or pull partners.

Optionally, you can check the Push With Propagation box if you want the selected WINS server to propagate the trigger to all its pull partners.

- If Push With Propagation is not checked, the selected WINS server will not propagate the trigger to its other partners.
- If Push With Propagation is checked, the selected WINS server sends a propagate push trigger to its pull partners after it has pulled in the latest information from the source WINS server. If it does not need to pull in any replicas because it has the same or more up-to-date replicas than the source WINS server, it does not propagate the trigger to its pull partners.

### ► To start replication immediately

- In the Replication Partners dialog box, choose the Replicate Now button.

## Managing Static Mappings

Static mappings are permanent lists of computer name-to-IP address mappings that cannot be challenged or removed, except when the administrator removes the specific mapping. You use the Static Mappings command in WINS Manager to add, edit, import, or delete static mappings for clients on the network that are not WINS enabled.

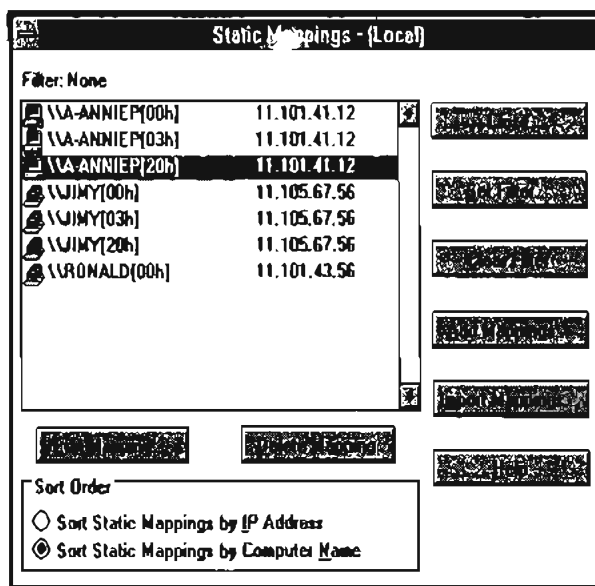
---

**Important** If DHCP is also used on the network, a reserved (or static) IP address will override any WINS server settings. Static mappings should not be assigned to WINS-enabled computers.

---

► To view static mappings

1. From the Mappings menu, choose the Static Mappings command.




---

**Caution** You cannot cancel changes made to the WINS database while working in the Static Mappings dialog box. You must manually delete any entries that are added in error or manually add back any entries that you mistakenly delete. This is because all changes to the WINS database made in this dialog box take effect immediately.

---

2. In the Static Mappings dialog box, select a Sort Order option, either by IP address or by computer name. This selection determines the order in which entries appear in the list of static mappings.
3. To edit or add a mapping, follow the procedures described in “Adding Static Mappings” and “Editing Static Mappings” later in this chapter.
4. To remove existing static mappings, select the mappings you want to delete from the list, and then choose the Delete Mapping button.
5. To limit the range of mappings displayed in the list of static mappings, choose the Set Filter button and follow the procedure in “Filtering the Range of Mappings” later in this chapter. To turn off filtering, choose the Clear Filter button.
6. When you finish viewing or changing the static mappings, choose the Close button.

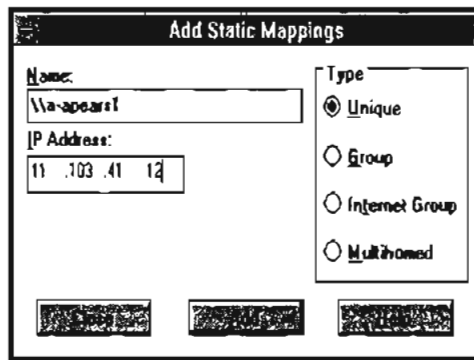
## Adding Static Mappings

You can add static mappings to the WINS database for specific IP addresses using two methods:

- Type static mappings in a dialog box
- Import files that contain static mappings

► **To add static mappings to the WINS database by typing entries**

1. In the Static Mappings dialog box, choose the Add Mappings button.



2. In the Name box of the Add Static Mappings dialog box, type the computer name of the system for which you are adding a static mapping. (If you want, you do not need to type two backslashes, because WINS Manager will add these for you.)
3. In the IP Address box, type the address for the computer.

If Internet Group or Multihomed is selected as the Type option, the dialog box shows additional controls for adding multiple addresses. Use the down-arrow button to move the address you type into the list of addresses for the group. Use the up-arrow button to change the order of a selected address in the list.

4. Select a Type option to indicate whether this entry is a unique name or a kind of group with a special name, as described in the following list.

Type option	Meaning
Unique	Unique name in the database, with one address per name.
Group	Normal group, where addresses of individual members are not stored. The client broadcasts name packets to normal groups.

---

Type option	Meaning
Internet group	Groups with NetBIOS names that have 0x1C as the 16th byte. An internet group stores up to 25 addresses for members. The maximum number of addresses is 25. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.
Multihomed	Unique name that can have more than one address (multihomed computers). The maximum number of addresses is 25. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.

---

**Important** For internet group names defined in this dialog box (that is, added statically), make sure that the primary domain controller (PDC) for that domain is defined in the group if the PDC is running Windows NT Advanced Server version 3.1.

---

For more information, see “Managing Special Names” later in this chapter.

5. Choose the Add button.

The mapping is immediately added to the database for that entry, and then the boxes are cleared so that you can add another entry.

6. Repeat this process for each static mapping you want to add to the database, and then choose the Close button.

---

**Important** Because each static mapping is added to the database when you choose the Add button, you cannot cancel work in this dialog box. If you make a mistake in entering a name or address for a mapping, you must return to the Static Mappings dialog box and delete the mapping there.

---

You can also import entries for static mappings for unique and special group names from any file that has the same format as the LMHOSTS file (as described in Chapter 6, “Setting Up LMHOSTS”). Scope names and keywords other than #DOM are ignored. However, normal group and multihomed names can be added only by typing entries in the Add Static Mappings dialog box.

► **To import a file containing static mapping entries**

1. In the Static Mappings dialog box, choose the Import Mappings button.
2. In the Select Static Mapping File dialog box, which is similar to the standard Windows NT Open dialog box, specify a filename for a static mappings file by typing its name in the box, or select one or more filenames in the list, and then choose the OK button to import the file.

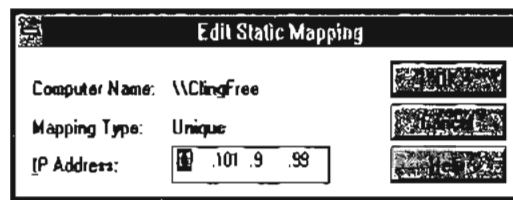
The specified file is read, and a static mapping is created for each computer name and address. If the #DOM keyword is included for any record, an internet group is created (if it is not already present), and the address is added to that group.

## Editing Static Mappings

You can change the IP addresses in static mappings owned by the WINS server you are currently administering.

► **To edit a static mapping entry**

1. In the Static Mappings dialog box, select the mapping you want to change and choose the Edit Mapping button, or double-click the mapping entry in the list.



You can view, but not edit, the Computer Name and Mapping Type option for the mapping in the Edit Static Mappings dialog box.

2. In the IP Address box, type a new address for the computer, and then choose the OK button.

The change is made in the WINS database immediately.

---

**Note** If you want to change the computer name or group type related to a specific IP address, you must delete the entry and redefine it in the Add Static Mappings dialog box.

---



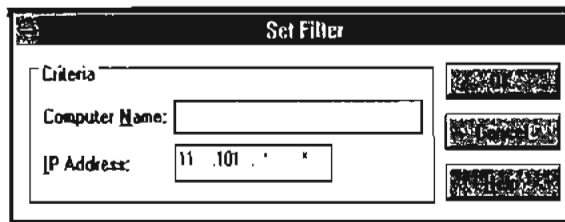
## Filtering the Range of Mappings

You may want to limit the range of IP addresses or computer names displayed in the Static Mappings or Show Database dialog boxes.

You can specify a portion of the computer name or IP address or both when filtering the list of mappings.

### ► To filter mappings by address or name

1. In the dialog box for Static Mappings or Show Database, choose the Set Filter button.



2. In the Set Filter dialog box, type portions of the computer name, address, or both in the Computer Name or IP Address boxes.

You can use the asterisk (\*) wildcard for portions of the name or address or both. For example, you could type `\\acct*` to filter all computers with names that begin with `acct`. However, for the address, a wildcard can be used only for a complete octet. That is, you can type `11.101.*.*`, but you cannot enter `11.1*.1.1` in these boxes.

3. Choose the OK button.

The selected range is displayed in the Static Mappings or Show Database dialog box. The filtered range will remain until you clear the filter.

A message will tell you if no mappings are found to match the range you specified, and the list of mappings will be empty.

If a filter is in effect for the range of mappings, the Clear Filter button is available for restoring the entire list.

### ► To clear the filtered range of mappings

- In the Static Mappings or Show Database dialog box, choose the Clear Filter button.

The list now shows all mappings found in the database.

## Managing Special Names

WINS recognizes special names for several types of groups, including a normal group, multihomed, and internet group. This section describes these groups and presents some background details to help you understand how WINS manages these groups.

### Normal Group Names

A group name does not have an address associated with it. It can be valid on any subnet and can be registered with more than one WINS server. A group's timestamp shows the last time for any change received for the group. If the WINS server receives a query for the group name, it returns FFFFFFFF (the limited broadcast address). The client then broadcasts on the subnet. The group name is renewed when any member of the group renews the group name.

### Multihomed Names

A multihomed name is a single, unique name storing multiple addresses. A multihomed device is a computer with multiple network cards and/or multiple IP addresses bound to NetBIOS over TCP/IP. A multihomed device with multiple IP addresses can register one or more addresses by sending one address at a time in a special name registration packet. A multihomed name in a WINS database can have one or more addresses. The timestamp for the record reflects any changes made for any members of the name.

Each multihomed group name can contain a maximum of 25 IP addresses.

When you configure TCP/IP manually on a Windows NT computer, you use the Advanced Microsoft TCP/IP dialog box to specify the IP address and other information for each adapter on a multihomed computer.

### Internet Group Names

The internet group name is read as configuration data. When dynamic name registrations for internet groups are received, the actual address (rather than the subnet broadcast address) is stored in the group with a timestamp and the owner ID, which indicates the WINS server registering that address.

The internet group name (which has a 16th byte ending in 0x1C reserved for domain names, as described in the following section) can contain a maximum of 25 IP addresses for primary and backup domain controllers in a domain. Dynamically registered names are added if the list is not static and has fewer than 25 members. If the list has 25 members, WINS removes a replica member (that is, a member registered by another WINS server) and adds the new member. If all members are owned by this WINS server, the oldest member is replaced by the new one.

WINS gives precedence over remote members to members in an internet group name that registered with it. This preference means that the group name always contains the geographically closest Windows NT Server computers. To establish the preference of members of internet groups registered with other WINS servers under the \Partners\Pull key in the Registry, a precedence is assigned for each WINS partner as a value of the **MemberPrec** Registry parameter. Preference should be given to WINS servers near the WINS server you are configuring. For more information about the value of this parameter, see its entry in “Advanced Configuration Parameters for WINS” later in this chapter.

The internet group name is handled specially by WINS, which returns the 24 closest Windows NT Server computers in the domain, plus the domain controller. The name ending in 1C is also used to discover a Windows NT Server computer in a domain when a computer running Windows NT Workstation or Windows NT Server needs a server for pass-through authentication.

If your network still has domain controllers running Windows NT Advanced Server version 3.1 to be included in the internet group name, you must add these to the group manually using WINS Manager. When you manually add such a computer to the internet group name, the list becomes static and no longer accepts dynamic updates from WINS-enabled computers.

For information about related issues in LMHOSTS for #DOM entries, see “Designating Domain Controllers Using #DOM” in Chapter 6, “Setting Up LMHOSTS.”

## How WINS Handles Special Names

Special names are indicated by a 16th byte appended to the computer name or domain name. The following table shows some special names that can be defined for static entries in the Add Static Mappings dialog box.

**Special Names for Static Mappings**

Name ending	Usage	How WINS handles queries
0x1E	A normal group. Browsers broadcast to this name and listen on it to elect a master browser. The broadcast is done on the local subnet and should not cross routers.	WINS always returns the limited broadcast address (FFFFFFF).
0x1D	Clients resolve this name to access the master browser for server lists. There is one master browser on a subnet.	WINS always returns a negative response. If the node is h-node or m-node, the client broadcasts a name query to resolve the name. For registrations, WINS returns a positive response even though the names are not put into the database.

**Special Names for Static Mappings** (*continued*)

<b>Name ending</b>	<b>Usage</b>	<b>How WINS handles queries</b>
0x1C	The internet group name, which contains a list of the specific addresses of systems that have registered the name. The domain controller registers this name.	<p>WINS treats this as an internet group, where each member of the group must renew its name individually or be released. The internet group is limited to 25 names. (Note, however, that there is no limit for #DOM entries in LMHOSTS.)</p> <p>WINS returns a positive response for a dynamic registration of a static 1C name, but the address is not added to the list. When a static 1C name is replicated that clashes with a dynamic 1C name on another WINS server, a union of the members is added, and the record is marked as static.</p>

The following illustrates a sample NetBIOS name table for a Windows NT Server domain controller, such as the list that appears if you type **nbtstat -n** at the command prompt. This table shows the 16th byte for special names, plus the type (unique or group).

NetBIOS Local Name Table			
Name	NetBIOS	Type	Status
<0C29870B>		Unique	Registered
ANNIEP5	<20>	UNIQUE	Registered
ANNIEP5	<00>	UNIQUE	Registered
ANNIEPDOM	<00>	GROUP	Registered
ANNIEPDOM	<1C>	GROUP	Registered
ANNIEPDOM	<1B>	UNIQUE	Registered
ANNIEP5	<03>	UNIQUE	Registered
ANNIEP5	<1E>	GROUP	Registered
ANNIEP5	<1D>	UNIQUE	Registered
.._MSBROWSE_.	<01>	GROUP	Registered

**Example NetBIOS Name Table for a Windows NT Domain Controller**

As shown in this example, several special names are identified for both the computer and the domain. These special names include the following:

- 0x0 (shown as <00> in the example), the redirector name, which is used with **net view**.
- 0x3, the Messenger service name for sending messages.
- MSBROWSE\_, the name master browsers broadcast to on the local subnet to announce their domains to other master browsers. WINS handles this name by returning the broadcast address FFFFFFFF.
- 0x1B, the domain master browser name, which clients and browsers use to contact the domain master browser. A domain master browser gets the names of all domain master browsers. When WINS is queried for the domain master browser name, it handles the query like any other name query and returns its address.

WINS assumes that the computer that registers a domain name with the 1B character is the domain controller. This name is registered by the browser running on the domain controller. This ensures that the domain controller is in the internet group name list that is returned when a 1C name is queried, for which WINS always returns the address of the 1B name along with the members of a 1C name.

## Setting Preferences for WINS Manager

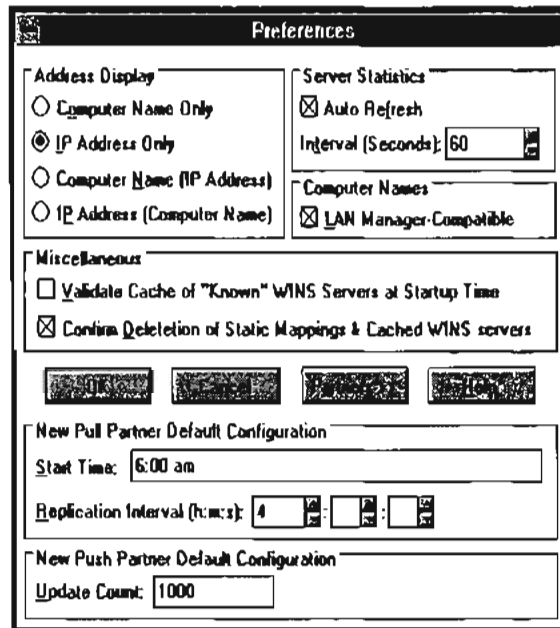
You can configure several options for administration of WINS servers. The commands for controlling preferences are on the Options menu.

► **To display the status bar for help on commands**

- From the Options menu, choose the Status Bar command.

When this command is active, its name is checked on the menu, and the status bar at the bottom of the WINS Manager window displays descriptions of commands as they are highlighted in the menu bar.

- ▶ To set preferences for WINS Manager
  1. From the Options menu, choose the Preferences command.
  2. To see all the available preferences, choose the Partners button in the Preferences dialog box.



3. Select an Address Display option to indicate how you want address information to be displayed throughout WINS Manager—as computer name, IP address, or an ordered combination of both.

---

**Note** Remember that the kind of address display affects how a connection is made to the WINS server — for IP addresses, the connection is made via TCP/IP; for computer names, the connection is made via named pipes.

---

4. Check Auto Refresh if you want the statistics in the WINS Manager window to be refreshed automatically. Then enter a number in the Interval box to specify the number of seconds between refresh actions.

WINS Manager also refreshes the statistical display automatically each time an action is initiated while you are working in WINS Manager.

5. Check the LAN Manager-Compatible check box if you want computer names to adhere to the LAN Manager naming convention.

LAN Manager computer names are limited to 15 characters, as opposed to 16-character NetBIOS names used by some other sources, such as Lotus Notes®. In LAN Manager names, the 16th byte is used to indicate whether the device is a server, workstation, messenger, and so on. When this option is checked, WINS adds and imports static mappings with 0, 0x03, and 0x20 as the 16th byte.

All Windows networking, including Windows NT, follows the LAN Manager convention. So this box should be checked unless your network accepts NetBIOS name from other sources.

6. Check Validate Cache Of Known WINS Servers At Startup Time if you want the system to query the list of servers each time the system starts to find out if each server is available.
7. If you want a warning message to appear each time you delete a static mapping or the cached name of a WINS server, check the Confirm Deletion Of Static Mappings And Cached WINS Servers option.
8. In the Start Time box, type a time to specify the default for replication start time for new pull partners. Then specify values for the Replication Interval to indicate how often data replicas will be exchanged between the partners.  
The minimum value for the Replication Interval is 40 minutes.
9. In the Update Count box, type a number to specify a default for how many registrations and changes can occur locally before a replication trigger is sent by this server when it is a push partner. The minimum value is 5.
10. When all options are set for your preferences, choose the OK button.

## Managing the WINS Database

The following files are stored in the `\systemroot\SYSTEM32\WINS` directory that is created when you set up a WINS server:

- JET.LOG is a log of all transactions done with the database. This file is used by WINS to recover data if necessary.
- SYSTEM.MDB is used by WINS for holding information about the structure of its database.
- WINS.MDB is the WINS database file.
- WINSTMP.MDB is a temporary file that WINS creates. This file may remain in the `\WINS` directory after a crash.

You should back up these files when you back up other files on the WINS server.

---

**Caution** The JET.LOG, SYSTEM.MDB, WINS.MDB, and WINSTMP.MDB files should not be removed or tampered with in any manner.

---

Like any database, the WINS database of address mappings needs to be cleaned and backed up periodically. WINS Manager provides the tools you need for maintaining the database. This section describes how to scavenge (clean), view, and back up the database. For information on restoring and moving the WINS database, see “Troubleshooting WINS” later in this chapter.

## Scavenging the Database

The local WINS database should periodically be cleared of released entries and old entries that were registered at another WINS server but did not get removed from this WINS database for some reason. This process, called scavenging, is done automatically over intervals defined by the relationship between the Renewal and Extinct intervals defined in the Configuration dialog box. You can also clean the database manually.

For example, if you want to verify old replicas immediately instead of waiting the time interval specified for verification, you can manually scavenge the database.



► **To scavenge the WINS database**

- From the Mappings menu, choose the Initiate Scavenging command.

The database is cleaned, with the results as shown in the following table.

State before scavenging	State after scavenging
Owned active names for which the Renewal interval has expired	Marked <i>released</i>
Owned released name for which the Extinct interval has expired	Marked <i>extinct</i>
Owned extinct names for which the Extinct timeout has expired	Deleted
Replicas of extinct names for which the Extinct timeout has expired	Deleted
Replicas of active names for which the Verify interval has expired	Revalidated
Replicas of extinct or deleted names	Deleted

For information about the intervals and timeouts that govern database scavenging, see “Configuring WINS Servers” earlier in this chapter.

After WINS has been running for a while, the database may need to be compacted to improve WINS performance.

► **To compact the WINS database**

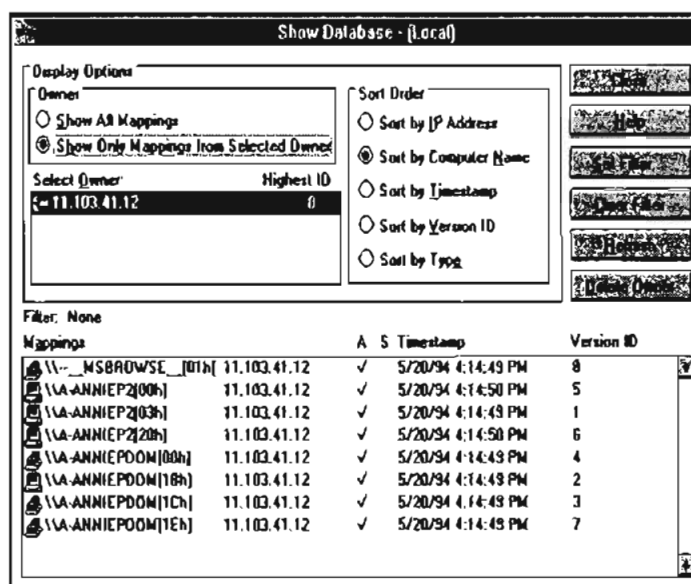
1. At the WINS server, stop the Windows Internet Name Service using the Control Panel Services option or by typing `net stop wins` at the command prompt.
2. Run COMPACT.EXE (which is found in the `\systemroot\SYSTEM32` directory).
3. Restart the Windows Internet Name Service on the WINS server.

## Viewing the WINS Database

You can view the actual active and static mappings stored in the WINS database, based on the WINS server that owns the entries.

► To view the WINS database

1. From the Mappings menu, choose the Show Database command.





2. In the Show Database dialog box, to view the mappings in the database for a specific WINS server, select Show Only Mappings From Specific Owner, and then from the Select Owner list, select the WINS server whose database you want to view.

By default, the Show Database dialog box shows all mappings for the WINS database on the currently selected WINS server.

3. Select a Sort Order option to sort by IP address, computer name, timestamp for the mapping, version ID, or type. (For information about types, see "Adding Static Mappings" earlier in this chapter.)

4. If you want to view only a range of mappings, choose the Set Filter button and follow the procedures described in “Filtering the Range of Mappings” earlier in this chapter. To turn off filtering, choose the Clear Filter button.
5. Use the scroll bars in the Mappings box to view entries in the database. Then choose the Close button when you are finished viewing.

As shown in the Mappings list, each registration record in the WINS database includes these elements:

Item	Meaning
	Unique
	Group, internet group, or multihomed
Computer name	The NetBIOS computer name.
IP address	The assigned Internet Protocol address.
A or S	Whether the mapping is active (dynamic) or static.
Timestamp	Shows when the record was registered or updated. When a replica is stored in the database, its timestamp is set to the current time on the receiving WINS server.
Version ID	A unique hexadecimal number assigned by the WINS server during name registration, which is used by the server's pull partner during replication to find new records.

You can also use the Show Database dialog box to remove all references to a specific WINS server in the database, including all database entries owned by the WINS server.

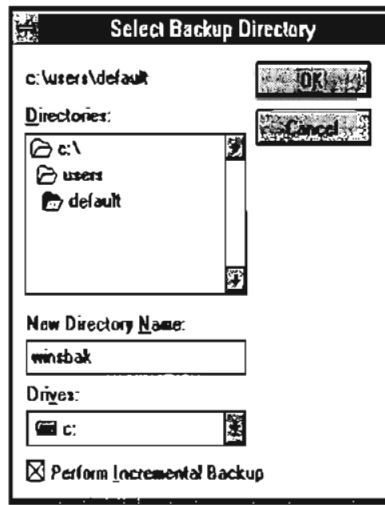
- ▶ **To delete a specific WINS server's entries in the database**
  - In the Show Database dialog box, select a WINS server in the Select Owner list, and then choose the Delete Owner button.

## Backing Up the Database

WINS Manager provides backup tools so that you can back up the WINS database. After you specify a backup directory for the database, WINS performs complete database backups every 24 hours, using the specified directory.

► **To back up a WINS database**

1. From the Mappings menu, choose the Backup Database command.



2. In the Select Backup Directory dialog box, specify the location for saving the backup files.

Windows NT proposes a subdirectory of the \WINS directory. You can accept this proposed directory. The most secure location is to back up the database on another hard disk. Do not back up to a network drive, because WINS Manager cannot restore from a network source.

3. If you want to back up only the newest version numbers in the database (that is, changes that have occurred since the last backup), check Perform Incremental Backup.

---

**Note** You must have performed a complete backup before this option can be used successfully.

---

4. Choose the OK button.

You should also periodically back up the Registry entries for the WINS server.

► **To back up the WINS Registry entries**

1. Run REGEDT32.EXE.
2. In Registry Editor, select the HKEY\_LOCAL\_MACHINE window, and then select this key:  
`..SYSTEM\CurrentControlSet\Services\WINS`
3. From the Registry menu, choose Save Key.
4. In the Save Key dialog box, specify the path where you store backup versions of the WINS database files.

For information about restoring the WINS database, see the following section, “Troubleshooting WINS.”

## Troubleshooting WINS

This section describes some basic troubleshooting steps for common problems and also describes how to restore or rebuild the WINS database.

### Basic WINS Troubleshooting

These error conditions can indicate potential problems with the WINS server:

- The administrator can't connect to a WINS server using WINS Manager. The message that appears might be, “The RPC server is unavailable.”
- The WINS Client service or Windows Internet Name Service may be down and cannot be restarted.

The first troubleshooting task is to make sure the appropriate services are running.

► **To ensure the WINS services are running**

1. Use the Services option in Control Panel to verify that the WINS services are running.  
In the Services dialog box for the client computer, Started should appear in the Status column for the WINS Client service. For the WINS server itself, Started should appear in the Status column for the Windows Internet Name Service.
2. If a necessary service is not started on either computer, start the service.

The following describes solutions to common WINS problems.

- ▶ **To locate the source of “duplicate name” error messages**
  - Check the WINS database for the name. If there is a static record, remove it from the database of the primary WINS server.  
–Or–  
Set the value of **MigrateOn** in the Registry to 1, so the static records in the database can be updated by dynamic registrations (after WINS successfully challenges the old address).
  
- ▶ **To locate the source of “network path not found” error messages on a WINS client**
  - Check the WINS database for the name. If the name is not present in the database, check whether the computer uses b-node name resolution. If so, add a static mapping for it in the WINS database.  
  
If the computer is configured as a p-node, m-node, or h-node and if its IP address is different from the one in the WINS database, then it may be that its address changed recently and the new address has not yet replicated to the local WINS server. To get the latest records, ask the WINS server that registered the address to perform a push replication with propagation to the local WINS server.
  
- ▶ **To discover why a WINS server cannot pull or push replications to another WINS server**
  1. Confirm that the router is working.
  2. Ensure that each server is correctly configured as either a pull or push partner:
    - If ServerA needs to perform pull replications with ServerB, make sure it is a push partner of ServerB.
    - If ServerA needs to push replications to ServerB, it should be a pull partner of WINS ServerB.  
To determine the configuration of a replication partner, check the values under the **\Pull** and **\Push** keys in the Registry, as described in “Advanced Configuration Parameters for WINS” later in this chapter.
  
- ▶ **To determine why WINS backup is failing consistently**
  - Make sure the path for the WINS backup directory is on a local disk on the WINS server.  
  
WINS cannot back up its database files to a remote drive.

## Restoring or Moving the WINS Database

This section describes how to restore, rebuild, or move the WINS database.

### Restoring a WINS Database

If you have determined that the Windows Internet Name Service is running on the WINS server, but you cannot connect to the server using WINS Manager, then the WINS database is not available or has become corrupted. If a WINS server fails for any reason, you can restore the database from a backup copy.

You can use the menu commands to restore the WINS database or restore it manually.

- ▶ **To restore a WINS database using menu commands**
  1. From the Mappings menu, choose the Restore Database command.
  2. In the Select Directory To Restore From dialog box, select the location where the backup files are stored, and then choose the OK button.
  
- ▶ **To restore a WINS database manually**
  1. In the `\systemroot\SYSTEM32\WINS` directory, delete the JET.LOG, JET\*.LOG, WINS.TMP, and SYSTEM.MDB files.
  2. From the Windows NT Server installation source, copy SYSTEM.MDB on the WINS server. The installation source can be the Windows NT Server compact disc, the installation floppy disks, or a network directory that contains the master files for Windows NT Server.
  3. Copy an uncorrupted backup version of WINS.MDB to the `\systemroot\SYSTEM32\WINS` directory.
  4. Restart the Windows Internet Name Service on the WINS server.

### Restarting and Rebuilding a Down WINS Server

In rare circumstances, the WINS server may not boot or a STOP error may occur. If the WINS server is down, follow these steps to restart.

- ▶ **To restart a WINS server that is down**
  1. Turn off the power to the server and wait one minute.
  2. Turn on the power, start Windows NT Server, and logon under an account with Administrator rights.
  3. At the command prompt, type `net start wins` and press ENTER.

If the hardware for the WINS server is malfunctioning or other problems prevent you from running Windows NT, you will have to rebuild the WINS database on another computer.

► **To rebuild a WINS server**

1. If you can start the original WINS server using MS-DOS, use MS-DOS to make backup copies of the files in the `\systemroot\SYSTEM32\WINS` directory. If you cannot start the computer with MS-DOS, you will have to use the last backup version of the WINS database files.
2. Install Windows NT Server and Microsoft TCP/IP to create a new WINS server using the same hard drive location and `\systemroot` directory. That is, if the original server stored the WINS files on `C:\WINNT35\SYSTEM32\WINS`, then the new WINS server should use this same path to the WINS files.
3. Make sure the WINS services on the new server are stopped, and then use Registry Editor to restore the WINS keys from backup files.
4. Copy the WINS backup files to the `\systemroot\SYSTEM32\WINS` directory.
5. Restart the new, rebuilt WINS server.

## Moving the WINS Database

You may find a situation where you need to move a WINS database to another computer. To do this, follow these steps.

► **To move a WINS database**

1. Stop the Windows Internet Name Service on the current computer.
2. Copy the `\SYSTEM32\WINS` directory to the new computer that has been configured as a WINS server.  

Make sure the new directory is under exactly the same drive letter and path as on the old computer.

If you must copy the files to a different directory, copy `WINS.MDB`, but not `SYSTEM.MDB`. Use the version of `SYSTEM.MDB` created for that new computer.
3. Start the Windows Internet Name Service on the new computer. WINS will automatically use the `.MDB` and `.LOG` files copied from the old computer.



## Advanced Configuration Parameters for WINS

This section presents configuration parameters that affect the behavior of WINS and that can be modified only through Registry Editor. For some parameters, WINS can detect Registry changes immediately. For other parameters, you must restart the Windows Internet Name Service for the changes to take effect.

---

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

---

► **To make changes to WINS configuration using Registry Editor**

1. Run REGEDT32.EXE from File Manager or Program Manager, or at a command prompt, type **start regedt32** and press ENTER.

When the Registry Editor window appears, you can press F1 to get Help on how to make changes in Registry Editor.

2. In Registry Editor, click the window titled HKEY\_LOCAL\_MACHINE On Local Machine, and then click the icons for the SYSTEM subtree until you reach the appropriate subkey, as described later in this section.

The following describes the value entries for WINS parameters that can only be set by adding an entry or changing values in Registry Editor.

## Registry Parameters for WINS Servers

The Registry parameters for WINS servers are specified under the following key:

```
.. \SYSTEM\CurrentControlSet\Services\Wins\Parameters
```

This subkey lists all the nonreplication-related parameters needed to configure a WINS server. It also contains a \Datafiles subkey, which lists all the files that should be read by WINS to initialize or reinitialize its local database.

### DbFileNm

Data type = REG\_EXPAND\_SZ

Range = *path name*

Default = %SystemRoot%\system32\wins\wins.mdb

Specifies the full path name for the WINS database file.

### DoStaticDataInit

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (false—that is, the WINS server does not initialize its database)

If this parameter is set to a non-zero value, the WINS server will initialize its database with records listed in one or more files listed under the \Datafiles subkey. The initialization is done at process invocation and whenever a change is made to one or more values of the \Parameters or \Datafiles keys (unless the change is to change the value of **DoStaticDataInit** to 0).

The following parameters in this subkey can be set using the options available in the WINS Server Configuration dialog box:

### LogDetailedEvents

### LogFilePath

### LoggingOn

### RefreshInterval

### RptOnlyWCnfPnrs

### TombstoneInterval (extinction interval)

### TombstoneTimeout (extinction timeout)

### VerifyInterval

Also, the `\Wins\Parameters\Datafiles` key lists one or more files that the WINS server should read to initialize or reinitialize its local database with static records. If the full path of the file is not listed, the directory of execution for the WINS server is assumed to contain the data file. The parameters can have any names (for example, DF1 or DF2). Their data types must be `REG_SZ` or `REG_EXPAND_SZ`.

---

**Important** The `\Wins\Performance` key contains values used for WINS performance counters that can be viewed in Performance Monitor. These values should be maintained by the system, so do not change these values.

---

## Registry Parameters for Replication Partners

The `\Wins\Partners` key has two subkeys, `\Pull` and `\Push`, under which are subkeys for the IP addresses of all push and pull partners, respectively, of the WINS server.

### Parameters for Push Partners

A push partner, listed under the `\Partners\Pull` key, is one from which a WINS server pulls replicas and from which it can expect update notification messages. The following parameter appears under the IP address for a specific push partner. This parameter can be set only by changing the value in Registry Editor:

#### MemberPrec

Data type = `REG_DWORD`

Range = 0 or 1

Default = None

Specifies the order of precedence for this WINS partner. 0 indicates low precedence, and 1 indicates high precedence. Notice that dynamically registered names are always high precedence. When a 1C name is pulled from this WINS partner, the addresses contained in it are given this precedence level. The value can be 0 (low) or 1 (high). Set this value to 1 if this WINS server is serving a geographic location that is nearby.

The following parameters appear under this subkey and can be set in the WINS Server Configuration dialog box:

```
.. \SYSTEM\CurrentControlSet\Services\Wins\Partners\Pull
```

#### **InitTimeReplication**

#### **CommRetryCount**

The following parameters appear under this subkey and can be set using the Preferences dialog box:

```
.. \SYSTEM\CurrentControlSet\Services\Wins\Partners\Pull\<Ip Address>
```

**SpTime** (Start Time for pull partner default configuration)

**TimeInterval** (Replication Interval)

For **SpTime**, WINS replicates at the set time if it is in the future for that day. After that, it replicates every number of seconds specified by **TimeInterval**. If **SpTime** is in the past for that day, WINS replicates every number of seconds specified by **TimeInterval**, starting from the current time (if **InitTimeReplication** is set to 1).

## **Parameters for Pull Partners**

A pull partner of a WINS server, listed under the **\Partners\Push** key, is one from which it can expect pull requests to pull replicas and to which it sends update notification messages. The following parameters appear under this subkey and can be set using the options available in the WINS Server Configuration dialog box:

```
.. \SYSTEM\CurrentControlSet\Services\Wins\Partners\Push
```

#### **InitTimeReplication**

#### **RplOnAddressChg**

The following parameter appears under this subkey and can be set using the options available in the Preferences dialog box:

```
.. \SYSTEM\CurrentControlSet\Services\Wins\Partners\Push\<Ip Address>
```

#### **UpdateCount**

## Planning a Strategy for WINS Servers

The planning issues for implementing WINS servers are similar to those for implementing DHCP servers, as described in Chapter 4, "Installing and Configuring DHCP Servers." Most network administrators will be installing both kinds of servers, so the planning and implementation tasks will be undertaken jointly for DHCP and WINS servers.

This section provides some additional planning issues for WINS servers.

### Planning for Server Performance

A WINS server can typically service 1500 name registrations per minute and about 760 queries per minute. There is no built-in limit to the number of records that a WINS server can replicate or store.

Based on these numbers, and planning for large-scale power outage where many computers will come on line simultaneously, the conservative recommendation is that you plan to include one WINS server and a backup server for every 10,000 computers on the network.

Two factors can particularly enhance WINS server performance. WINS performance increases almost 25 percent on a computer with two processors. Also, using NTFS as the file system also improves performance.

After you establish WINS servers in the internetwork, you can adjust the Renewal interval. Setting this interval to reduce the numbers of registrations can help tune server response time. (The Renewal interval is specified in the WINS Server Configuration dialog box.)

### Planning Replication Partners and Proxies

In one possible configuration, one WINS server can be designated as the central server, and all other WINS servers can be configured as both push partner and pull partner of this central server. Such a configuration ensures that the WINS database on each server contains addresses for every node on the WAN.

Another option is to set up a chain of WINS servers, where each server is both the push partner and pull partner with a nearby WINS server. In such a configuration, the two servers at the ends of the chain would also be push and pull partners with each other. Other replication partner configurations can be established for your site's needs.

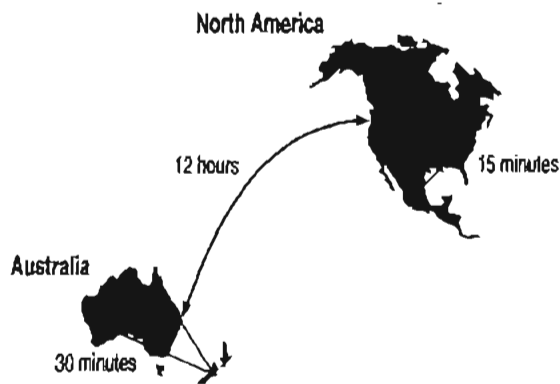
Only a limited number of WINS proxies should be designated on each domain, so that a limited number of computers are using resources to respond to broadcast name requests.

## Planning Replication Frequency Between Hubs

A major tuning issue for WINS servers is replication frequency. You want replication to occur frequently enough that any server being down will not interfere with the reliability of name query responses. However, for longer wide area network (WAN) lengths, you do not want replication to interfere with network throughput.

For multiple network hubs interconnected by WAN links, replication frequency can be configured to be low compared to the replication frequency of multiple WINS servers at a single hub. For long WAN links, infrequent replication ensures that the links are available to carry client traffic without WINS affecting throughput.

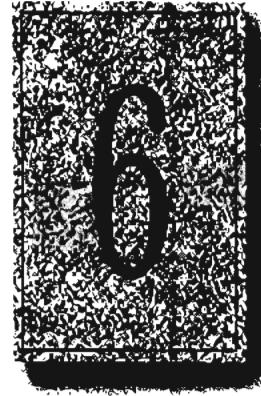
For example, the WAN servers at a central site might be configured to replicate every 15 minutes. Replication between WAN hubs of a greater distance might be scheduled for every 30 minutes. Replication between servers on different continents might replicate twice a day.



**Example of an Enterprise-Wide Configuration for WINS Replication**

## CHAPTER 6

# Setting Up LMHOSTS



The LMHOSTS file is commonly used on Microsoft networks to locate remote computers for network file, print, and remote procedure services and for domain services such as logons, browsing, replication, and so on.

You will want to use LMHOSTS for smaller networks or to find hosts on remote networks that are not part of the WINS database (since name query requests are not broadcast beyond the local subnet). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution, since WINS is the preferred method for name resolution. With WINS servers in place, therefore, LMHOSTS may not be necessary.

This chapter presents the following topics:

- Editing the LMHOSTS file
- Using LMHOSTS with dynamic name resolution

## Editing the LMHOSTS File

The LMHOSTS file used by Windows NT contains mappings of IP addresses to Windows NT computer names (which are NetBIOS names). This file is compatible with Microsoft LAN Manager 2.x TCP/IP LMHOSTS files.

You can use Notepad or any other text editor to edit the sample LMHOSTS file that is automatically installed in the `\systemroot\SYSTEM32\DRIVERS\ETC` directory.

This section provides some basic rules and guidelines for LMHOSTS.

## Rules for LMHOSTS

The following rules apply for entries in LMHOSTS:

- Each entry should be placed on a separate line.
- The IP address should begin in the first column, followed by the corresponding computer name.
- The address and the computer name should be separated by at least one space or tab.
- NetBIOS names can contain uppercase and lowercase characters and special characters. If a name is placed between double quotation marks, it will be used exactly as entered. For example, "AccountingPDC" is a mixed-case name, and "HumanRscSr \0x03" generates a name with a special character.

---

**Note** In Microsoft networks, a NetBIOS computer name in quotes that is less than 16 characters is padded with spaces. If you do not want this behavior, make sure the quoted string is 16 characters long.

---

- The # character is usually used to mark the start of a comment. However, it can also designate special keywords, as described in this section.



The keywords listed in the following table can be used in LMHOSTS under Windows NT. (LAN Manager 2.x, which also uses LMHOSTS for NetBIOS over TCP/IP name resolution, treats these keywords as comments.)

#### LMHOSTS Keywords

Keyword	Meaning
#PRE	Added after an entry to cause that entry to be preloaded into the name cache. By default, entries are not preloaded into the name cache but are parsed only after WINS and name query broadcasts fail to resolve a name. #PRE must be appended for entries that also appear in #INCLUDE statements; otherwise, the entry in #INCLUDE is ignored.
#DOM:<domain>	Added after an entry to associate that entry with the domain specified by <domain>. This keyword affects how the Browser and Logon services behave in routed TCP/IP environments. To preload a #DOM entry, you must also add the #PRE keyword to the line.
#INCLUDE <filename>	Forces the system to seek the specified <filename> and parse it as if it were local. Specifying a Uniform Naming Convention (UNC) <filename> allows you to use a centralized LMHOSTS file on a server. If the server is located outside of the local broadcast area, you must add a mapping for the server before its entry in the #INCLUDE section and also append #PRE to ensure that it preloaded.
#BEGIN_ALTERNATE	Used to group multiple #INCLUDE statements. Any single successful #INCLUDE causes the group to succeed.
#END_ALTERNATE	Used to mark the end of an #INCLUDE grouping.
\0xnn	Support for nonprinting characters in NetBIOS names. Enclose the NetBIOS name in double quotation marks and use \0xnn notation to specify a hexadecimal value for the character. This allows custom applications that use special names to function properly in routed topologies. However, LAN Manager TCP/IP does not recognize the hexadecimal format, so you surrender backward compatibility if you use this feature.  Note that the hexadecimal notation applies only to one character in the name. The name should be padded with blanks so the special character is last in the string (character 16).

The following example shows how all of these keywords are used:

```
102.54.94.98    localsrv    #PRE
102.54.94.97    trey        #PRE    #DOM:networking    #net group's PDC
102.54.94.102  "appname    \0x14"    #special app server
102.54.94.123  popular    #PRE        #source server

#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\lmhosts    #adds LMHOSTS from this server
#INCLUDE \\trey\public\lmhosts        #adds LMHOSTS from this server
#END_ALTERNATE
```

In the above example:

- The servers named **localsrv** and **trey** are specified so they can be used later in an **#INCLUDE** statement in a centrally maintained LMHOSTS file.
- The server named **"appname \0x14"** contains a special character after the 15 characters in its name (including the blanks), so its name is enclosed in double quotation marks.
- The server named **popular** is preloaded, based on the **#PRE** keyword.

## Guidelines for LMHOSTS

When you use a host table file, be sure to keep it up to date and organized. Follow these guidelines:

- Update the LMHOSTS file whenever a computer is changed or removed from the network.
- Because LMHOSTS files are searched one line at a time from the beginning, list remote computers in priority order, with the ones used most often at the top of the file, followed by remote systems listed in **#INCLUDE** statements. Finally, the **#PRE** entries should be left for the end of the file, because these are preloaded into the cache at system startup time and are not accessed later. This increases the speed of searches for the entries used most often. Also, any comment lines add to the parsing time, because each line is processed individually.
- Use **#PRE** statements to preload popular entries and servers listed in **#INCLUDE** statements into the local computer's name cache.

## Using LMHOSTS with Dynamic Name Resolution

On networks that do not use WINS, the broadcast name resolution method used by Windows NT computers provides a simple, dynamic mechanism for locating resources by name on a TCP/IP network.

Because broadcast name resolution relies on IP-level broadcasts to locate resources, unwanted effects can occur in routed IP topologies. In particular, resources located on remote subnets do not receive name query requests, because routers do not pass IP-level broadcasts. For this reason, Windows NT allows you to manually provide computer name and IP address mappings for remote resources via LMHOSTS.

This section describes how the LMHOSTS file can be used to enhance Windows NT in routed environments. This section includes the following topics:

- Specifying remote servers in LMHOSTS
- Designating primary domain controllers using #DOM
- Using centralized LMHOSTS files

### Specifying Remote Servers in LMHOSTS

Computer names can be resolved outside the local broadcast area if computer name and IP address mappings are specified in the LMHOSTS file. For example, suppose the computer named ClientA wants to connect to the computer named ServerB, which is outside of its IP broadcast area. Both Windows NT computers are configured with Microsoft TCP/IP.

Under a strict b-node broadcast protocol, as defined in RFCs 1001 and 1002, ClientA's name query request for ServerB would fail (by timing out), because ServerB is located on a remote subnet and does not respond to ClientA's broadcast requests. So an alternate method is provided for name resolution. Windows NT maintains a limited cache of computer name and IP address mappings, which is initialized at system startup. When a workstation needs to resolve a name, the cache is examined first and, if there is no match in the cache, Windows NT uses b-node broadcast name resolution. If this fails, the LMHOSTS file is used. If this last method fails, the name is unresolved, and an error message appears.

This strategy allows the LMHOSTS file to contain a large number of mappings without requiring a large chunk of static memory to maintain an infrequently used cache. At system startup, the name cache is preloaded only with entries from LMHOSTS tagged with the #PRE keyword. For example, the LMHOSTS file could contain the following:

```
102.54.94.91    accounting      #accounting server
102.54.94.94    payroll        #payroll server
102.54.94.97    stockquote     #PRE #stock quote server
102.54.94.102  printqueue     #print server in Bldg 10
```

In this example, the server named **stockquote** is preloaded into the name cache, because it is tagged with the #PRE keyword. Entries in the LMHOSTS file can represent Windows NT Workstation computers, Windows NT Server computers, LAN Manager servers, or Windows for Workgroups 3.11 computers running Microsoft TCP/IP. There is no need to distinguish between different platforms in LMHOSTS.

---

**Note** The Windows NT tag #PRE allows backward compatibility with LAN Manager 2.x LMHOSTS files and offers added flexibility in Windows NT. Under LAN Manager, the # character identifies a comment, so all characters thereafter are ignored. But #PRE is a valid tag for Windows NT.

---

In the above example, the servers named **accounting**, **payroll**, and **printqueue** would be resolved only after the cache entries failed to match and after broadcast queries failed to locate them. After nonpreloaded entries are resolved, their mappings are cached for a period of time for reuse.

Windows NT limits the preload name cache to 100 entries by default. This limit only affects entries marked with #PRE. If you specify more than 100 entries, only the first 100 #PRE entries will be preloaded. Any additional #PRE entries will be ignored at startup but will be resolved when the system parses the LMHOSTS file after dynamic resolution fails.

Finally, you can reprime the name cache by using the **nbtstat -R** command to purge and reload the name cache, reread the LMHOSTS file, and insert entries tagged with the #PRE keyword. Use **nbtstat** to remove or correct preloaded entries that may have been mistyped or any names cached by successful broadcast resolution.

## Designating Domain Controllers Using #DOM

The most common use of LMHOSTS is for locating remote servers for file and print services. But for Windows NT, LMHOSTS can also be used to find domain controllers running TCP/IP in routed environments. Windows NT primary domain controllers (PDCs) and backup domain controllers (BDCs) maintain the user account security database and manage other network-related services. Because large Windows NT domains can span multiple IP subnets, it is possible that routers could separate the domain controllers from one another or separate other computers in the domain from domain controllers.

The #DOM keyword can be used in LMHOSTS files to distinguish a Windows NT domain controller from a Windows NT Workstation computer, a LAN Manager server, or a Windows for Workgroups computer. To use the #DOM tag, follow the name and IP address mapping in LMHOSTS with the #DOM keyword, a colon, and the domain in which the domain controller participates. For example:

```
102.54.94.97   treydc #DOM:treycorp #The treycorp PDC
```

Using the #DOM keyword to designate domain controllers adds entries to a special *internet group name cache* that is used to limit internetwork distribution of requests intended for the local domain controller. When domain controller activity such as a logon request occurs, the request is sent on the special internet group name. In the local IP-broadcast area, the request is sent only once and picked up by any local domain controllers. However, if you use #DOM to specify domain controllers in the LMHOSTS file, Microsoft TCP/IP uses datagrams to also forward the request to domain controllers located on remote subnets.

Examples of such domain controller activities include domain controller pulses (used for account database synchronization), logon authentication, password changes, master browser list synchronization, and other domain management activities.

For domains that span subnets, LMHOSTS files can be used to map important members of the domain using #DOM. The following lists some guidelines for doing this.

- For each local LMHOSTS file on a Windows NT computer that is a member in a domain, there should be #DOM entries for all domain controllers in the domain that are located on remote subnets. This ensures that logon authentication, password changes, browsing, and so on all work properly for the local domain. These are the minimum entries necessary to allow a Windows NT system to participate in a Windows networking internetwork.
- For local LMHOSTS files on all servers that can be backup domain controllers, there should be mappings for the primary domain controller's name and IP address, plus mappings for all other backup domain controllers. This ensures that promoting a backup to primary domain controller status does not affect the ability to offer all services to members of the domain.
- If trust relationships exist between domains, all domain controllers for all trusted domains should also be listed in the local LMHOSTS file.
- For domains that you want to browse from your local domain, the local LMHOSTS files should contain at least the name and IP address mapping for the primary domain controller in the remote domain. Again, backup domain controllers should also be included so that promotion to primary domain controller does not impair the ability to browse remote domains.

For small to medium sized networks with fewer than 20 domains, a single common LMHOSTS file usually satisfies all workstations and servers on the internetwork. To achieve this, systems should use the Windows NT replicator service to maintain synchronized local copies of the global LMHOSTS or use centralized LMHOSTS files, as described in the following section.

Names that appear with #DOM in LMHOSTS are placed in a special domain name list in NetBIOS over TCP/IP. When a datagram is sent to this domain using the DOMAIN<IC> name, the name is resolved first via WINS or broadcast. The datagram is then sent to all the addresses on the list from LMHOSTS, and there is also a broadcast on the local subnet.

---

**Important** To browse across domains, for Windows NT Advanced Server 3.1 and Windows NT 3.1, each computer must have an entry in its LMHOSTS file for the primary domain controller in each domain. This remains true for Windows NT version 3.5 clients, unless the Windows NT Server computer is also version 3.5 and, optionally, offers WINS name registration.

However, you cannot add an LMHOSTS entry for a Windows NT Server that is a DHCP client, because the IP address changes dynamically. To avoid problems, any domain controllers whose names are entered in LMHOSTS files should have their IP addresses reserved as static addresses in the DHCP database rather than running as DHCP clients.

Also, all Windows NT Advanced Server 3.1 computers in a domain and its trusted domains should be upgraded to version 3.5, so that browsing across domains is possible without LMHOSTS.

---

## Using Centralized LMHOSTS Files

With Microsoft TCP/IP, you can include other LMHOSTS files from local and remote computers. The primary LMHOSTS file is always located in the `\systemroot\SYSTEM32\DRIVERS\ETC` directory on the local computers. Most networks will also have an LMHOSTS file maintained by the network administrator, so administrators should maintain one or more global LMHOSTS files that users can rely on. This is done using #INCLUDE statements rather than copying the global file locally. Then use the replicator service to distribute multiple copies of the global file(s) to multiple servers for reliable access.

To provide a redundant list of servers maintaining copies of the same LMHOSTS file, use the `#BEGIN_ALTERNATE` and `#END_ALTERNATE` keywords. This is known as a *block inclusion*, which allows multiple servers to be searched for a valid copy of a specific file. The following example shows the use of the `#INCLUDE` and `#_ALTERNATE` keywords to include a local LMHOSTS file (in the C:\PRIVATE directory):

```
102.54.94.97   treydc     #PRE #DOM:treycorp   #primary DC
102.54.94.99   treydc     #PRE #DOM:treycorp   #backup DC in domain
102.54.94.98   localsvr  #PRE #DOM:treycorp

#INCLUDE      c:\private\lmhosts      #include a local lmhosts

#BEGIN_ALTERNATE
#INCLUDE      \\treydc\public\lmhosts  #source for global file
#INCLUDE      \\treydc\public\lmhosts  #backup source
#INCLUDE      \\localsvr\public\lmhosts #backup source
#END_ALTERNATE
```

---

**Important** This feature should never be used to include a remote file from a redirected drive, because the LMHOSTS file is shared between local users who have different profiles and different logon scripts, and even on single-user systems, redirected drive mappings can change between logon sessions.

---

In the above example, the servers **treydc** and **treydc** are located on remote subnets from the computer that owns the file. The local user has decided to include a list of preferred servers in a local LMHOSTS file located in the C:\PRIVATE directory. During name resolution, the Windows NT system first includes this private file, then gets the global LMHOSTS file from one of three locations: **treydc**, **treydc**, or **localsvr**. All names of servers in the `#INCLUDE` statements must have their addresses preloaded using the `#PRE` keyword; otherwise, the `#INCLUDE` statement will be ignored.

The block inclusion is satisfied if one of the three sources for the global LMHOSTS is available and none of the other servers are used. If no server is available, or for some reason the LMHOSTS file or path is incorrect, an event is added to the event log to indicate that the block inclusion failed.



## CHAPTER 7

# Using the Microsoft FTP Server Service



The Microsoft FTP Server service allows other computers using the FTP utility to connect to this computer and transfer files. The FTP Server service supports all Windows NT **ftp** client commands. Non-Microsoft versions of FTP clients may contain commands that are not supported. The FTP Server service is implemented as a multithreaded Win32 service that complies with the requirements defined in Requests for Comments (RFCs) 959 and 1123.

The FTP Server service is integrated with the Windows NT security model. Users connecting to the FTP Server service are authenticated based on their Windows NT user accounts and receive access based on their user profiles. For this reason, it is recommended that the FTP Server service be installed on an NTFS partition so that the files and directories made available via FTP can be secured.

---

**Caution** The FTP Server protocol relies on the ability to pass user passwords over the network without data encryption. A user with physical access to the network could examine user passwords during the FTP validation process.

---

The following topics are included in this chapter:

- Installing the FTP Server service
- Configuring the FTP Server service
- Administering the FTP Server service
- Advanced configuration parameters for FTP Server service

For information about using performance counters to monitor FTP Server traffic, see Chapter 8, “Using Performance Monitor with TCP/IP Services.”

## Installing the FTP Server Service

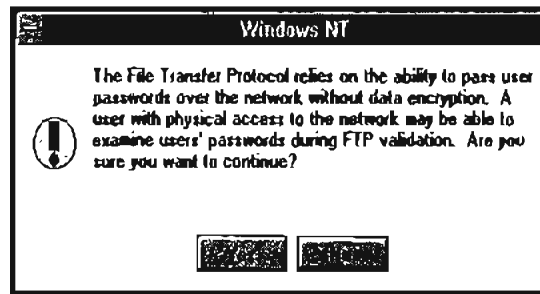
These procedures assume that you have installed any necessary devices and device drivers.



You must be logged on as a member of the Administrators group for the local computer to install and configure the FTP Server service.

### ► To install the FTP Server service

1. Choose the Network option in Control Panel.
2. In the Network Settings dialog box, choose the Add Software button to display the Add Network Software dialog box.
3. In the Network Software box, select TCP/IP Protocol And Related Components, and then choose the Continue button. When the Windows NT TCP/IP Installation Options dialog box appears, check the FTP Server Service option, and then choose the OK button.
4. When the message prompts you to confirm that you are familiar with FTP security, choose the Yes button to continue with FTP Server service installation.



5. When prompted for the full path to the Windows NT distribution files, provide the appropriate location, and then choose the Continue button.
6. After the necessary files are copied to your computer, the FTP Service dialog box appears so that you can continue with the configuration procedure as described in the next section. The FTP Server service must be configured in order to operate.

---

**Note** For disk partitions that do not use the Windows NT file system (NTFS), you can apply simple read/write security by using the FTP Server tool in the Control Panel as described in the following section.

---

## Configuring the FTP Server Service

After the FTP Server service software is installed on your computer, you must configure it to operate. When you configure the FTP Server service, your settings result in one of the following:

- No anonymous FTP connection allowed. In this case, each user must provide a valid Windows NT username and password. To configure the FTP Server service for this, make sure the Allow Anonymous Connection box is cleared in the FTP Service dialog box.
- Allow both anonymous and Windows NT users to connect. In this case, a user can choose to use either an anonymous connection or a Windows NT username and password. To configure the FTP Server service for this, make sure only the Allow Anonymous Connection box is checked in the FTP Service dialog box.
- Allow only anonymous FTP connections. In this case, a user cannot connect using a Windows NT username and password. To configure the FTP Server service for this, make sure both the Allow Anonymous Connections and the Allow Anonymous Connections Only boxes are checked in the FTP Service dialog box.

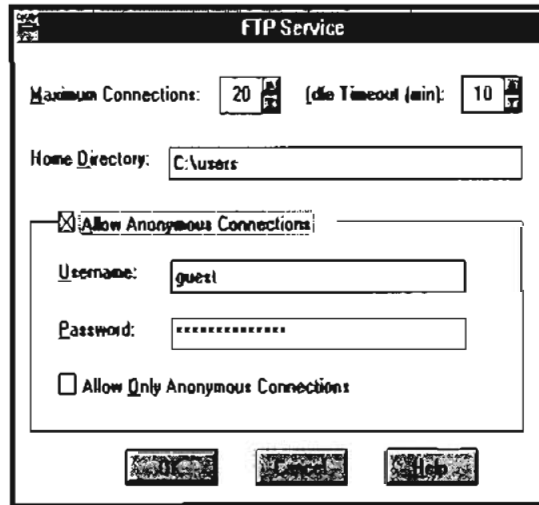
If anonymous connections are allowed, you must supply the Windows NT username and password to be used for anonymous FTP. When an anonymous FTP transfer takes place, Windows NT will check the username assigned in this dialog box to determine whether access is allowed to the files.

► To configure or reconfigure the FTP Server service

1. The FTP Service dialog box appears automatically after the FTP Server service software is installed on your computer.

–Or–

If you are reconfiguring the FTP Server service, choose the Network option in Control Panel. In the Installed Network Software box, select FTP Server, and then choose the Configure button.



The FTP Service dialog box displays the following options:

Item	Description
Maximum Connections	Specifies the maximum number of FTP users who can connect to the system simultaneously. The default value is 20; the maximum is 50. A value of 0 means no maximum, that is, an unlimited number of simultaneous users.  When the specified number of concurrent users are logged onto the FTP server, any subsequent attempts to connect will receive messages defined by the administrator. For information about defining custom messages, see “Advanced Configuration Parameters for FTP Server Service” later in this chapter.
Idle Timeout	Specifies how many minutes an inactive user can remain connected to the FTP Server service. The default value is 10 minutes; the maximum is 60 minutes. If the value is 0, users are never automatically disconnected.

Item	Description
Home Directory	Specifies the initial directory for users.
Allow Anonymous Connections	Enables users to connect to the FTP Server using the user name <b>anonymous</b> (or <b>ftp</b> , which is a synonym for <b>anonymous</b> ). A password is not necessary, but the user will be prompted to supply a mail address as the password. By default, anonymous connections are not allowed. Notice that you cannot use a Windows NT user account with the name <b>anonymous</b> with the FTP Server. The <b>anonymous</b> user name is reserved in the FTP Server for the anonymous logon function. Users logging on with the username <b>anonymous</b> receive permissions based on the FTP Server configuration for anonymous logons.
Username	Specifies which local user account to use for FTP Server users who log on under <b>anonymous</b> . Access permissions for the anonymous FTP user will be the same as the specified local user account. The default is the standard Guest system account. If you change this, you must also change the password.
Password	Specifies the password for the user account specified in the Username box.
Allow Only Anonymous Connections	Allows only the user name <b>anonymous</b> to be accepted. This option is useful if you do not want users to log on using their own user names and passwords because FTP passwords are unencrypted. However, all users will have the same access privilege, defined by the anonymous account. By default, this option is not enabled.

- Default values are provided for Maximum Connections, Idle Timeout, and Home Directory. Accept the default values, or change values for each field as necessary.
- Choose the OK button to close the FTP Service dialog box and return to the Network Settings dialog box.
- To complete initial FTP Server service installation and configuration, choose the OK button.

A message reminds you that you must restart the computer so that the changes you made will take effect.

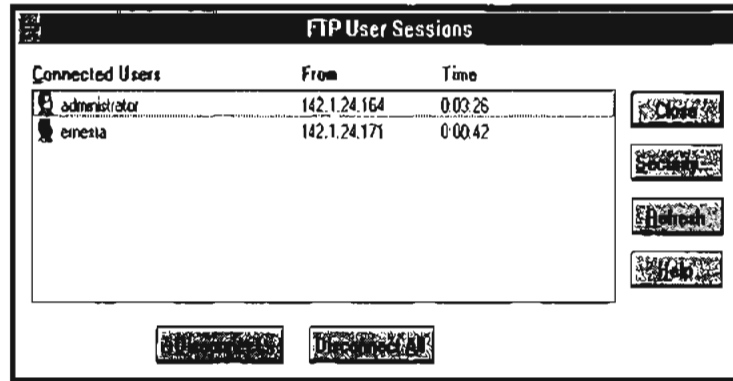
---

**Note** When you first install the FTP Server service, you must also complete the security configuration as described in the following procedure for users to access volumes on your computer.

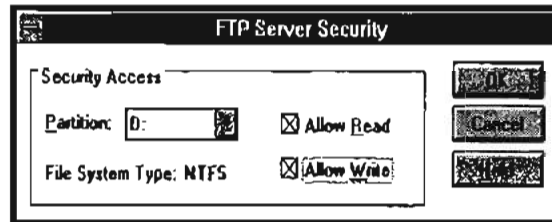
---

► To configure FTP Server security

1. After the FTP Server has been installed and you have restarted Control Panel, start the FTP Server option in Control Panel. Windows NT Server users can also use the FTP menu in Server Manager.



2. In the FTP User Sessions dialog box, choose the Security button.



3. In the Partition box of the FTP Server Security dialog box, select the drive letter you want to set security on, and then check the Allow Read or Allow Write check box, or both check boxes, depending on the security you want for the selected partition.

Repeat this step for each partition.

Setting these permissions will affect all files across the entire partition on file allocation table (FAT) and high-performance file system (HPFS) partitions. On NTFS partitions, this feature can be used to remove read or write access (or both) on the entire partition.

Any restrictions set in this dialog box are enforced in addition to any security that might be part of the file system. That is, an administrator can use this dialog box to remove permissions on specific volumes but cannot use it to grant permissions beyond those maintained by the file system. For example, if a partition is marked as read-only, no one can write to the partition via FTP regardless of any permissions set in this dialog box.

4. Choose the OK button when you are finished setting security access on partitions.

The changes take effect immediately. The FTP Server service is now ready to operate.

## Administering the FTP Server Service



After initial installation is complete, the FTP Server service is automatically started in the background each time the computer is started. Remote computers can initiate an FTP session while the FTP Server service is running on your Windows NT computer. Both computers must be running the TCP/IP protocol.



You must be logged on as a member of the Administrators group to administer the FTP Server.

Remote users can connect to the FTP Server using their account on the FTP Server, an account on the FTP Server's domain or trusted domains (Windows NT Server only), or using the **anonymous** account if the FTP Server service is configured to allow anonymous logons.

When making any configuration changes to the FTP Server (with the exception of security configuration), you must restart the FTP Server by either restarting the computer or manually stopping and restarting the server, using the **net** command or Services icon in Control Panel.

► To start or stop the FTP Server service

- Use the Services option in Control Panel, or at the command prompt use the commands `net stop ftpsvc` followed by `net start ftpsvc`.

Restarting the service in this way disconnects any users presently connected to the FTP Server without warning—so use the FTP Server option in Control Panel to determine if any users are connected. Pausing the FTP Server (by using the Services option in Control Panel or the `net pause` command) prevents any more users from connecting to the FTP Server but does not disconnect the currently logged on users. This feature is useful when the administrator wants to restart the server without disconnecting the current users. After the users disconnect on their own, the administrator can safely shut down the server without worrying that users will lose work. When attempting to connect to a Windows NT FTP Server that has been paused, clients receive the message “421 - Service not available, closing control connection.”

## Using FTP Commands at the Command Prompt

When you install the FTP service, a set of `ftp` commands are automatically installed that you can use at the command prompt. For a summary list of these commands, see the `ftp` entry in Chapter 11, “Utilities Reference.”

► To get help on `ftp` commands

1. Double-click the Windows NT Help icon in the Program Manager group.
2. In the Windows NT help window, click the Command Reference Help button.
3. Click the `ftp` commands name in the Commands window.
4. Click an `ftp` command name in the Command Reference window to see a description of the command, plus its syntax and parameter definitions.

## Managing Users

Use the FTP Server option in Control Panel to manage users connected to the FTP Server and to set security for each volume on the FTP Server. For convenience on Windows NT Server computers, the same dialog box can be reached from Server Manager by choosing the FTP menu command.

In the FTP User Sessions dialog box, the Connected Users box displays the names of connected users, their system’s IP addresses, and how long they have been connected. For users who logged on using the `anonymous` user name, the display shows the passwords used when they logged on as their user names. If the user name contained a mail host name (for example, `ernesta@trey-research.com`) only the username (`ernesta`) appears. Anonymous users also have a question mark (?) over their user icons. Users who have been authenticated by Windows NT security have no question mark.



The FTP Server allows you to disconnect one or all users with the disconnect buttons. Users are not warned if you disconnect them.

The FTP Server displays users' names as they connect but does not update the display when users disconnect or when their connect time elapses. The Refresh button allows you to update the display to show only users who are currently connected.

Choosing the Security button displays the FTP Service Security dialog box, where you can set Read and Write permissions for each partition on the FTP Server, as described earlier in this chapter. You must set the permissions for each partition you want FTP users to have access to. If you do not set partition parameters, no users will be able to access files. If the partition uses a secure file system, such as NTFS, file system restrictions are also in effect.

In addition to FTP Server partition security, if a user logs on using a Windows NT account, access permissions for that account are in effect.

## Controlling the FTP Server and User Access

A network administrator can control several of the FTP Server configuration variables. One such variable, Maximum Connections, can be set by using the Network option in Control Panel to define a value between 0 and 50. Any value from 1 to 50 restricts concurrent FTP sessions to the value specified. A value of 0 allows unlimited connections to be established to the FTP Server until the system exhausts the available memory.

You can specify a custom message to be displayed when the maximum number of concurrent connections is reached. To do this, enter a new value for **MaxClientsMessage** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter.

## Annotating Directories

You can add directory descriptions to inform FTP users of the contents of a particular directory on the server by creating a file called `~FTPSVC~.CKM` in the directory that you want to annotate. Usually you want to make this a hidden file so directory listings do not display this file. To do this, use File Manager or type the command `attrib +h ~ftpsvc~.ckm` at the command prompt.

Directory annotation can be toggled by FTP users on a user-by-user basis with a built-in, site-specific command called `ckm`. On most FTP client implementations (including the Windows NT FTP client), users type a command at the command prompt similar to `quote site ckm` to get this effect.

You can set the default behavior for directory annotation by setting a value for **AnnotateDirectories** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter.

## Changing Directory Listing Format

Some FTP client software makes assumptions based on the formatting of directory list information. The Windows NT FTP Server provides some flexibility for client software that requires directory listing similar to UNIX systems. Users can use the command **dirstyle** to toggle directory listing format between MS-DOS-style (the default) and UNIX-style listings. On most FTP client implementations (including the Windows NT FTP client), users type a command at the command prompt similar to `quote site dirstyle` to get this effect.

You can set the default style for directory listing format by setting a value for **MsDosDirOutput** in the Registry, as described in “Advanced Configuration Parameters for FTP Server Service” later in this chapter.

## Customizing Greeting and Exit Messages

You can create customized greeting and exit messages by setting values for **GreetingMessage** and **ExitMessage** in the Registry, as described in “Advanced Configuration Parameters for FTP Server Service” later in this chapter. By default, these value entries are not in the Registry, so you must add them to customize the message text.

Greeting and exit messages are sent to users when they connect or disconnect from the FTP Server. When you create custom messages, you can add multiline messages of your choice.

## Logging FTP Connections

You can log incoming FTP connections in the System event log by setting values for **LogAnonymous** and **LogNonAnonymous** in the Registry, as described in “Advanced Configuration Parameters for FTP Server Service” later in this chapter. By default, these value entries are not in the Registry, so you must add them to log incoming connections.

You can specify whether event log entries are made for both anonymous and nonanonymous users connecting to the FTP Server. You can view such entries in the System event log by using Event Viewer.

## Advanced Configuration Parameters for FTP Server Service

This section presents configuration parameters that affect the behavior of the FTP Server service and that can be modified only through Registry Editor. After you modify any of these value entries, you must restart the FTP Server service for the changes to take effect.

---

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

---

► **To make changes to the FTP Server service configuration using Registry Editor**

1. Run REGEDT32.EXE from File Manager or Program Manager, or at a command prompt, type `start regedt32` and press ENTER.

When the Registry Editor window appears, you can press F1 to get Help on how to make changes in Registry Editor.

2. In Registry Editor, click the window titled HKEY\_LOCAL\_MACHINE On Local Machine, and then click the icons for the SYSTEM subtree until you reach this subkey:

```
.. \SYSTEM\CurrentControlSet\Services\ftpsvc\Parameters
```

All of the parameters described here are located under this Registry subkey.

The following describes the value entries for FTP Server service parameters that can only be set by adding an entry or changing their values in Registry Editor. These value entries do not appear by default in the Registry, so you must add an entry if you want to change its default value.

**AnnotateDirectories**

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (false—that is, directory annotation is off)

This value entry defines the default behavior of directory annotation for newly connected users. Directory descriptions are used to inform FTP users of the contents of a directory on the server. The directory description is saved in a file named ~FTPSVC-.CKM, which is usually a hidden file. When this value is 1, directory annotation is on.

**ExitMessage**

Data type = REG\_SZ

Range = String

Default = "Goodbye."

This value entry defines a signoff message that will be sent to FTP clients upon receipt of a **quit** command.

**GreetingMessage**

Data type = REG\_MULTI\_SZ

Range = String

Default = None (no special greeting message)

This value entry defines the message to be sent to new clients after their accounts have been validated. In accordance with Internet behavior, if the client logs on as anonymous and specifies an identity that starts with a minus sign (-), this greeting message is not sent.

**LogAnonymous**

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (false—that is, do not log successful anonymous logons)

This value entry enables or disables logging of anonymous logons in the System event log.

**LogNonAnonymous**

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (false—that is, do not log successful nonanonymous logons)

This value entry enables or disables logging of nonanonymous logons in the System event log.

### LogFileAccess

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (do not log file accesses to FTPSVC.LOG)

If this value is non-zero, all file accesses are logged to the file FTPSVC.LOG in the service's current directory (typically `\systemroot\SYSTEM32`). For each file opened by the FTP Server, FTPSVC.LOG will contain a single line entry in the following format:

*IPAddress username action path date\_time*

- *ip\_address* is the client computer's IP address
- *username* is the user's name (or *password* for anonymous logons)
- *action* is either "opened," "created," or "appended"
- *path* is the fully qualified path of the file acted upon
- *date\_time* is the date and time the action took place

Entries are also written to the log whenever the FTP Server starts or stops. For example:

```
***** FTP SERVER SERVICE STARTING Fri Apr 29 10:28:49 1994
11.101.199.173 daveo opened d:\tmp\tst.bat Fri Apr 29 10:29:42 1994
11.101.199.173 daveo created d:\tmp\new.txt Fri Apr 29 10:30:25 1994
11.101.199.173 daveo appended d:\tmp\new.txt Fri Apr 29 10:33:04 1994
***** FTP SERVER SERVICE STOPPING Fri Apr 29 10:33:08 1994
```

### LowercaseFiles

Data type = REG\_DWORD

Range = 0 or 1

Default = 0 (do not map filenames to lowercase)

If this value is nonzero, all filenames returned by the `list` and `nlst` commands will be mapped to lowercase for noncase-preserving file systems. This mapping only occurs when a directory listing is requested on a noncase-preserving file system. If this value is 0, case in all filenames will be unaltered. Currently, FAT is the only noncase-preserving file system supported under Windows NT, so this flag has no effect when retrieving listings on HPFS or NTFS partitions.

### MaxClientsMessage

Data type = REG\_SZ

Range = String

Default = "Maximum clients reached, service unavailable."

This value entry specifies the message to be sent to an FTP client if the maximum number of clients has been reached or exceeded. This message indicates that the server is refusing additional clients because it is currently servicing the maximum number of connections (as specified in the FTP Service dialog box or the `MaxConnections` value in the Registry).

**MsdosDirOutput**

Data type = REG\_DWORD

Range = 0 or 1

Default = 1 (true—that is, directory listings will look like MS-DOS)

This value entry specifies the default behavior for whether the output of the **list** command will look like the output of the MS-DOS **dir** command or the output of the UNIX **ls** command. This value also controls the direction of slashes in paths sent by the **pwd** command.

When this value is 1, directory listings will look like MS-DOS listings, and the path will contain backward slashes (\). If this value is 0, listings will look like UNIX listings, and the path will contain forward slashes (/).

The following Registry parameters can be set using the options available when configuring the FTP Server service in the Network Settings dialog box:

**AllowAnonymous**

**AnonymousOnly**

**AnonymousUsername**

**ConnectionTimeout**

**HomeDirectory**

**MaxConnections**

The following Registry parameters can be set using the options available when you select the FTP Server icon in Control Panel and then choose the Security button:

**ReadAccessMask**

**WriteAccessMask**

The ranges of values that can be entered for these parameters in Registry Editor are the same as those described in the related dialog boxes earlier in this chapter. You should use only the FTP Server service dialog boxes to set these values.

## CHAPTER 8

# Using Performance Monitor with TCP/IP Services



This chapter describes the performance counters that can be charted in Performance Monitor so you can track performance of the IP protocols, FTP Server service traffic, and WINS servers.

The performance counters are described in the following topics in this chapter:

- Using Performance Monitor with TCP/IP
- Monitoring TCP/IP performance
- Monitoring FTP Server service traffic
- Monitoring WINS server performance

---

**Important** To use the TCP/IP performance counters in Performance Monitor, you must install the SNMP service, as described in Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."

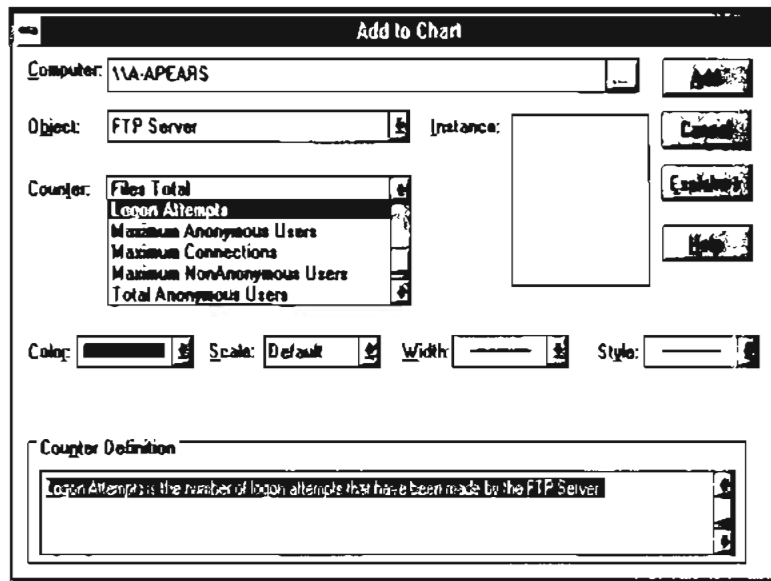
---

## Using Performance Monitor with TCP/IP

After elements of Microsoft TCP/IP are installed, you can use Performance Monitor to track performance.

### ► To use Performance Monitor with TCP/IP

1. In the Administrative Tools group in Program Manager, double-click Performance Monitor.
2. From the Edit menu, choose Add To Chart.



3. In the Computer list in the Add To Chart dialog box, select the computer you want to monitor.
4. In the Object list, select the TCP/IP-related process you want to monitor: FTP Server, ICMP, IP, Network Interface, TCP, UDP, or WINS Server.
5. In the Counter list, select the counters you want to monitor for each process, and then choose the Add button.

For information about each counter, choose the Explain button, or see the definition tables later in this chapter.

6. When you have selected all the counters you want for a particular chart, choose the Done button.

For more information about using Performance Monitor, see Chapter 19, "Performance Monitor," in the *Windows NT Server System Guide*.



## Monitoring TCP/IP Performance

Each of the different elements that make up the TCP/IP protocol suite can be monitored separately in Performance Monitor if SNMP services are installed on the computer.

- ▶ To view counters specific to TCP/IP processes
  - In the Add To Chart dialog box in Performance Monitor, select ICMP, IP, Network Interface, TCP, or UDP in the Object list.

The counters for each of these object types are described in the following sections.

### ICMP Performance Counters

The ICMP Object Type includes those counters that describe the rates that Internet Control Message Protocol (ICMP) messages are received and sent by a certain entity using the ICMP protocol. It also describes various error counts for the ICMP protocol.

ICMP performance counter	Meaning
Messages Outbound Errors	The number of ICMP messages that this entity did not send because of problems discovered within ICMP, such as lack of buffers. This value should not include errors discovered outside the ICMP layer, such as the inability of IP to route the resultant datagram. In some implementations, there may be no types of error that contribute to this counter's value.
Messages Received Errors	The number of ICMP messages that the entity received, but determined as having errors (bad ICMP checksums, bad length, and so on).
Messages Received/Second	The rate at which ICMP messages are received by the entity. The rate includes those messages received in error.
Messages Sent/Second	The rate at which ICMP messages are attempted to be sent by the entity. The rate includes those messages sent in error.
Messages/Second	The total rate at which ICMP messages are received and sent by the entity. The rate includes those messages received or sent in error.
Received Address Mask	The number of ICMP Address Mask Request messages received.

ICMP performance counter	Meaning
Received Address Mask Reply	The number of ICMP Address Mask Reply messages received.
Received Destination Unreachable	The number of ICMP Destination Unreachable messages received.
Received Echo Reply/Second	The rate of ICMP Echo Reply messages received.
Received Echo/Second	The rate of ICMP Echo messages received.
Received Parameter Problem	The number of ICMP Parameter Problem messages received.
Received Redirect/Second	The rate of ICMP Redirect messages received.
Received Source Quench	The number of ICMP Source Quench messages received.
Received Time Exceeded	The number of ICMP Time Exceeded messages received.
Received Timestamp Reply/Second	The rate of ICMP Timestamp Reply messages received.
Received Timestamp/Second	The rate of ICMP Timestamp (request) messages received.
Sent Address Mask	The number of ICMP Address Mask Request messages sent.
Sent Address Mask Reply	The number of ICMP Address Mask Reply messages sent.
Sent Destination Unreachable	The number of ICMP Destination Unreachable messages sent.
Sent Echo Reply/Second	The rate of ICMP Echo Reply messages sent.
Sent Echo/Second	The rate of ICMP Echo messages sent.
Sent Parameter Problem	The number of ICMP Parameter Problem messages sent.
Sent Redirect/Second	The rate of ICMP Redirect messages sent.
Sent Source Quench	The number of ICMP Source Quench messages sent.
Sent Time Exceeded	The number of ICMP Time Exceeded messages sent.
Sent Timestamp Reply/Second	The rate of ICMP Timestamp Reply messages sent.
Sent Timestamp/Second	The rate of ICMP Timestamp (request) messages sent.

## IP Performance Counters

The IP Object Type includes those counters that describe the rates that Internet Protocol (IP) datagrams are received and sent by a certain computer using the IP protocol. It also describes various error counts for the IP protocol.

IP performance counter	Meaning
Datagrams Forwarded/Second	The rate of input datagrams for which this entity was not their final IP destination that resulted in an attempt to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this rate will include only those packets that were Source-Routed via this entity, when the Source-Route option processing was successful.
Datagrams Outbound Discarded	The number of output IP datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space.) This counter would include datagrams counted in Datagrams Forwarded if any such packets met this (discretionary) discard criterion.
Datagrams Outbound No Route	The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in Datagrams Forwarded that meet this "no route" criterion.
Datagrams Received Address Errors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Datagrams Received Delivered/Second	The rate at which input datagrams are successfully delivered to IP user protocols (including ICMP).
Datagrams Received Discarded	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
Datagrams Received Header Errors	The number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.

<b>IP performance counter</b>	<b>Meaning</b>
Datagrams Received Unknown Protocol	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Datagrams Received/Second	The rate at which IP datagrams are received from the interfaces, including those in error.
Datagrams Sent/Second	The rate at which IP datagrams are supplied to IP for transmission by local IP user protocols (including ICMP). This counter does not include any datagrams counted in Datagrams Forwarded.
Datagrams/Second	The rate at which IP datagrams are received from or sent to the interfaces, including those in error. Any forwarded datagrams are not included in this rate.
Fragment Re-assembly Failures	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments, because some algorithms (notably RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmentation Failures	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their "Don't Fragment" flag was set.
Fragmented Datagrams/Second	The rate at which datagrams are successfully fragmented at this entity.
Fragments Created/Second	The rate at which IP datagram fragments have been generated as a result of fragmentation at this entity.
Fragments Re-assembled/Second	The rate at which IP fragments are successfully reassembled.
Fragments Received/Second	The rate at which IP fragments that need to be reassembled at this entity are received.

## Network Interface Performance Counters for TCP/IP

The Network Interface Object Type includes those counters that describe the rates at which bytes and packets are received and sent over a network TCP/IP connection. It also describes various error counts for the same connection.

Network Interface counter	Meaning
Bytes Received/Second	The rate at which bytes are received on the interface, including framing characters.
Bytes Sent/Second	The rate at which bytes are sent on the interface, including framing characters.
Bytes Total/Second	The rate at which bytes are sent and received on the interface, including framing characters.
Current Bandwidth	An estimate of the interface's current bandwidth in bits per second (bps). For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.
Output Queue Length	The length of the output packet queue (in packets.) If this is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible. Since the requests are queued by NDIS in this implementation, this will always be 0.
Packets Outbound Discarded	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Packets Outbound Errors	The number of outbound packets that could not be transmitted because of errors.
Packets Received Discarded	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Network Interface counter	Meaning
Packets Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Received Non-Unicast/Second	The rate at which non-unicast (that is, subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.
Packets Received Unicast/Second	The rate at which (subnet) unicast packets are delivered to a higher-layer protocol.
Packets Received Unknown	The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.
Packets Received/Second	The rate at which packets are received on the network interface.
Packets Sent Non-Unicast/Second	The rate at which packets are requested to be transmitted to non-unicast (that is, subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets Sent Unicast/Second	The rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets Sent/Second	The rate at which packets are sent on the network interface.
Packets/Second	The rate at which packets are sent and received on the network interface.

## TCP Performance Counters

The TCP Object Type includes those counters that describe the rates that Transmission Control Protocol (TCP) segments are received and sent by a certain entity using the TCP protocol. In addition, it describes the number of TCP connections that are in each of the possible TCP connection states.

TCP performance counter	Meaning
Connection Failures	The number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Connections Active	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Connections Established	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Connections Passive	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Connections Reset	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Segments Received/Second	The rate at which segments are received, including those received in error. This count includes segments received on currently established connections.
Segments Retransmitted/Second	The rate at which segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes.
Segments Sent/Second	The rate at which segments are sent, including those on current connections, but excluding those containing only retransmitted bytes.
Segments/Second	The rate at which TCP segments are sent or received using the TCP protocol.

## UDP Performance Counters

The UDP Object Type includes those counters that describe the rates that User Datagram Protocol (UDP) datagrams are received and sent by a certain entity using the UDP protocol. It also describes various error counts for the UDP protocol.

UDP performance counter	Meaning
Datagrams No Port/Second	The rate of received UDP datagrams for which there was no application at the destination port.
Datagrams Received Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Datagrams Received/Second	The rate at which UDP datagrams are delivered to UDP users.
Datagrams Sent/Second	The rate at which UDP datagrams are sent from the entity.
Datagrams/Second	The rate at which UDP datagrams are sent or received by the entity.

## Monitoring FTP Server Traffic

When you install the FTP Server services, the necessary software is also installed so that you can monitor and graph various FTP Server statistics using Performance Monitor. Using Performance Monitor to view activity on remote Windows NT systems makes FTP Server administration more convenient when you are administering multiple Windows NT FTP Servers.



► **To view counters specific to the FTP Server service**

- In the Performance Monitor window, select FTP Server in the Object list.

The FTP Server performance counters are cleared each time you start and stop the FTP Server service.

FTP performance counter	Meaning
Bytes Received/Second	The rate at which data bytes are received by the FTP Server.
Bytes Sent/Second	The rate at which data bytes are sent by the FTP Server.
Bytes Total/Second	The sum of Bytes Sent/Second and Bytes Received/Second. This is the total rate of bytes transferred by the FTP Server.
Connection Attempts	The number of connection attempts that have been made to the FTP Server.
Current Anonymous Users	The number of anonymous users currently connected to the FTP Server.
Current Connections	The current number of connections to the FTP Server.
Current NonAnonymous Users	The number of nonanonymous users currently connected to the FTP Server.
Files Received	The total number of files received by the FTP Server.
Files Sent	The total number of files sent by the FTP Server.
Files Total	The sum of Files Sent and Files Received. This is the total number of files transferred by the FTP Server.
Logon Attempts	The number of logon attempts that have been made to the FTP Server.
Maximum Anonymous Users	The maximum number of anonymous users simultaneously connected to the FTP Server.
Maximum Connections	The maximum number of simultaneous connections to the FTP Server.
Maximum NonAnonymous Users	The maximum number of nonanonymous users simultaneously connected to the FTP Server.
Total Anonymous Users	The total number of anonymous users that have ever connected to the FTP Server.
Total NonAnonymous Users	The total number of nonanonymous users that have ever connected to the FTP Server.

## Monitoring WINS Server Performance

When you install a WINS server and SNMP services, counters are automatically installed so that you can use Performance Monitor to view WINS Server service performance.

- ▶ **To view counters specific to the WINS Server service**
  - In the Performance Monitor window, select WINS Server in the Object list.

WINS performance counter	Meaning
Failed Queries/Second	The total number of failed queries per second.
Failed Releases/Second	The total number of failed releases per second.
Group Conflicts/Second	The rate at which group registrations received by the WINS server resulted in conflicts with records in the database.
Group Registrations/Second	The rate at which group registrations are received by the WINS server.
Group Renewals/Second	The rate at which group renewals are received by the WINS server.
Queries/Second	The total number of queries per second, which is the rate at which queries are received by the WINS server.
Releases/Second	The total number of releases per second, which is the rate at which releases are received by the WINS server.
Successful Queries/Second	The total number of successful queries per second.
Successful Releases/Second	The total number of successful releases per second.
Total Number of Conflicts/Second	The sum of the Unique and Group conflicts per second, which is the total rate at which conflicts were seen by the WINS server.
Total Number of Registrations/Second	The sum of the Unique and Group registrations per second. This is the total rate at which registrations are received by the WINS server.
Total Number of Renewals/Second	The sum of the Unique and Group registrations per second, which is the total rate at which renewals are received by the WINS server.
Unique Conflicts/Second	The rate at which unique registrations and renewals received by the WINS server resulted in conflicts with records in the database.
Unique Registrations/Second	The rate at which unique registrations are received by the WINS server.
Unique Renewals/Second	The rate at which unique renewals are received by the WINS server.



## CHAPTER 9

# Internetwork Printing with TCP/IP



Users on any Microsoft networking computer can print to direct-connect TCP/IP printers or to printers that are physically attached to UNIX computers if at least one Windows NT computer has Microsoft TCP/IP printing installed.

Microsoft TCP/IP printing conforms with Request for Comment (RFC) 1179.

This chapter describes how to create a TCP/IP printer when TCP/IP is installed on a Windows NT computer and how to print to a Windows NT print server from a UNIX computer.

The topics in this chapter include:

- Overview of TCP/IP printing
- Setting up Windows NT for TCP/IP printing
- Creating a printer for TCP/IP printing
- Printing to Windows NT from UNIX clients

For complete information about working with printers, see Chapter 6, "Print Manager," in the *Windows NT System Guide*.