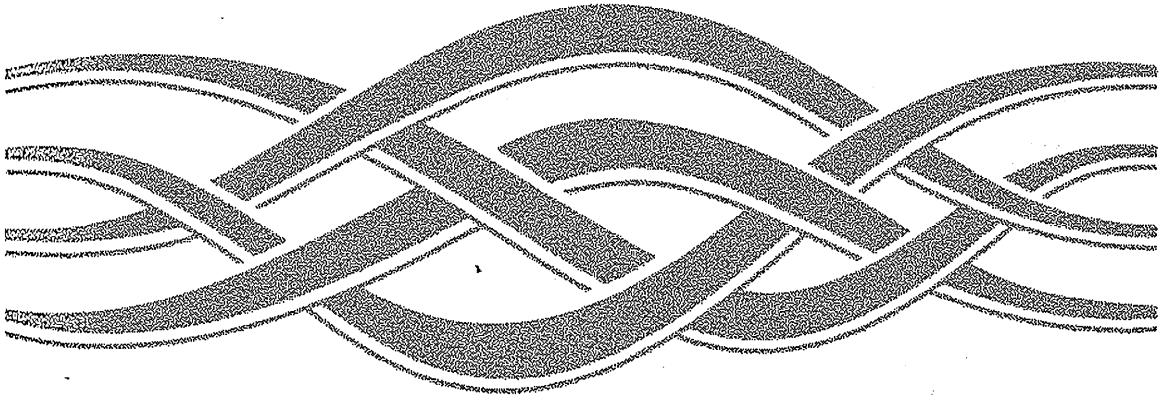
Microsoft®

Networking Supplement



Microsoft®

Windows NT® Server

Networking Supplement

Microsoft® Windows NT® Server

Version 4.0

Microsoft Corporation

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

© 1985-1996 Microsoft Corporation. All rights reserved.

Microsoft, MS, MS-DOS, Windows, Windows NT, and BackOffice are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Microsoft.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Document No. 69941-0696
Printed in the United States of America.

Contents

Welcome

Microsoft® Windows NT® Server provides many built-in networking utilities, protocols, and services. Along with its basic file and print services and excellent client/server application functionality, Windows NT Server includes

- Open network protocols (including TCP/IP)
- Multi-Protocol Routing
- Remote Access Service
- NetWare connectivity
- Macintosh connectivity

These features are described in the five parts of this book:

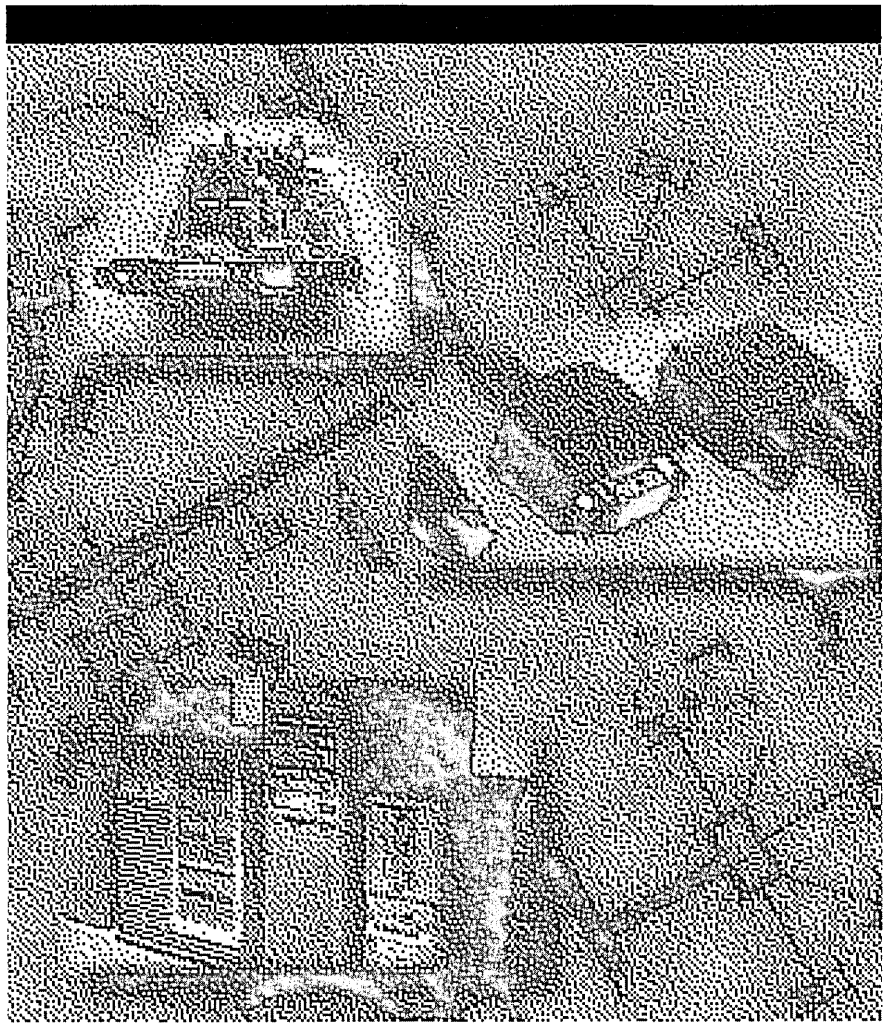
- Part 1, "TCP/IP," describes Microsoft's implementation of the Transmission Control Protocol/Internet Protocol (TCP/IP). This includes diagnostic tools and basic TCP/IP utilities, administrative services and utilities—such as Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS), and Domain Name System (DNS)—and support for network programming interfaces.
- Part 2, "Routing Protocols," describes Multi-Protocol Routing support, which enables routing over IP and Internetwork Packet Exchange (IPX) networks using a computer running Windows NT Server as the router. Routing on AppleTalk networks is also explained.
- Part 3, "Remote Access Service," describes the Windows NT Server Remote Access Service (RAS), which enables remote or mobile users to connect to the network over telephone lines, Integrated Services Digital Network (ISDN) lines, X.25 carriers, or over the Internet using Point-to-Point Tunneling Protocol (PPTP). RAS includes support for a variety of protocols—Point to Point Protocol (PPP), Serial-Line IP (SLIP), and Microsoft RAS—security control, and other standard RAS features.

- Part 4, "Services for NetWare," describes the NetWare interoperability features of Windows NT Server. These include Gateway Service for NetWare (which enables a computer running Windows NT Server to act as a gateway between Microsoft client computers and NetWare servers) and Migration Tool for NetWare (which smoothly transfers users, groups, volumes, and files from NetWare servers to computers running Windows NT Server).
- Part 5, "Services for Macintosh," describes how Windows NT Server provides basic network services to Macintosh clients, enabling PC and Macintosh computers to share files and printers. Features include secured logon, printing to both PostScript and non-PostScript printers, and simple, integrated administration.

For an in-depth discussion of other networking topics, such as advanced TCP/IP configuration or multiple-domain security planning, see the *Networking Guide* in the Windows NT Server Resource Kit.

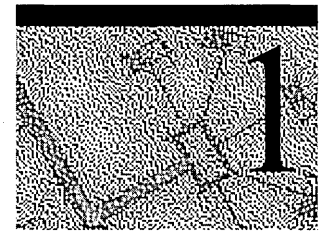
PART 1

TCP/IP



CHAPTER 1

Microsoft TCP/IP and Related Services for Windows NT



The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is a standard set of networking protocols that govern how data passes between networked computers. With TCP/IP you can communicate with Windows NT platforms, with devices that use other Microsoft networking products, and with non-Microsoft systems (such as UNIX systems). TCP/IP is the primary protocol of the Internet and the World Wide Web. It is also the primary protocol for many private *internetworks*, which are networks that connect local area networks (LANs) together.

For procedural information about installing and configuring TCP/IP under Windows NT, see the online Help. For more detailed information about TCP/IP and its integration with Windows NT and other networking products, see the *Microsoft Windows NT Resource Kit Networking Guide.*

Benefits of Using TCP/IP

Microsoft TCP/IP for Windows NT Server and Windows NT Workstation offers the following advantages:

- A standard, routable 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.
- The enabling technology necessary to connect Windows NT to the global Internet. TCP/IP, Point to Point Protocol (PPP), Point to Point Tunneling Protocol (PPTP), and Windows Sockets provide the foundation needed to connect and use Internet services.
- A robust, scalable, cross-platform, client-server framework. Microsoft TCP/IP supports the *Windows Sockets interface*, which is a Windows-based implementation of the widely used Berkeley Sockets interface for network programming.

Core Technology and Third-Party Add-Ons

Microsoft TCP/IP is a full-featured implementation of the protocol suite and related services. It 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 dictates how computers communicate and how networks are interconnected. Support is also provided for Point to Point Protocol (PPP), Point to Point Tunneling Protocol (PPTP), and Serial-Line IP (SLIP), which are protocols used for dial-up access to TCP/IP networks, including the Internet.
- Support for network programming interfaces such as Windows Sockets, remote procedure call (RPC), NetBIOS, and network dynamic data exchange (Network DDE).
- Basic TCP/IP connectivity utilities, including **finger**, **ftp**, **lpr**, **rcp**, **rexec**, **rsh**, **telnet**, and **tftp**. These utilities allow users running Windows NT to interact with and use resources on non-Microsoft hosts (such as those running UNIX).
- TCP/IP diagnostic tools, including **arp**, **hostname**, **ipconfig**, **lpq**, **nbtstat**, **netstat**, **ping**, **route**, and **tracert**. Use these utilities to detect and resolve TCP/IP networking problems.

- Services and related administrative tools, including the Internet Information Server for setting up Internet or Intranet Web sites, Dynamic Host Configuration Protocol (DHCP) service for automatically configuring TCP/IP on computers running Windows NT, Windows Internet Name Service (WINS) for dynamically registering and querying NetBIOS computer names on an internetwork, Domain Name System (DNS) Server service for registering and querying DNS domain names on an internetwork, and TCP/IP printing for accessing printers connected to computers running UNIX or connected directly to the network with a dedicated network adapter.
- Simple Network Management Protocol (SNMP) agent. This component allows a computer running Windows NT to be monitored remotely with management tools such as Sun® Net Manager or HP® Open View. Microsoft TCP/IP also includes SNMP support for DHCP and WINS servers.
- The server software for simple network protocols, including Character Generator, Daytime, Discard, Echo, and Quote of the Day. These protocols allow a computer running Windows NT to respond to requests from other systems that support these protocols.
- Path MTU Discovery, which provides the ability to determine the datagram size for all routers between Windows NT-based computers and any other systems on the WAN. Microsoft TCP/IP also supports the Internet Group Management Protocol (IGMP), which is used by workgroup software products.

Figure 1-1 shows the elements of Microsoft TCP/IP alongside the variety of additional applications and connectivity utilities provided by Microsoft and other third-party vendors.

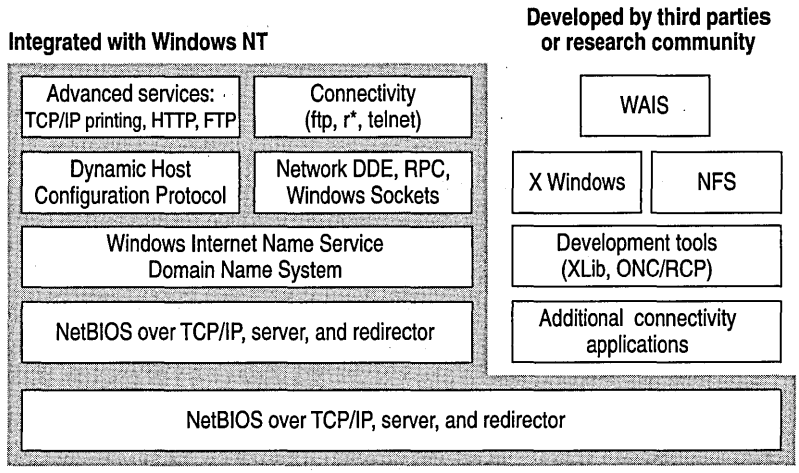


Figure 1-1 Microsoft TCP/IP Core Technology and Third-party Add-ons

Microsoft TCP/IP for Windows NT does not include a complete suite of TCP/IP connectivity utilities or server services (*daemons*). Many such applications and utilities—available in the public domain or from third-party vendors—are compatible with Microsoft TCP/IP.

Note For computers running Windows for Workgroups, you can install Microsoft TCP/IP-32. For computers running MS-DOS, you can install the Microsoft Network Client for MS-DOS. Both are available on the Windows NT Server compact disc. For installation information, see the *Windows NT Server Concepts and Planning Guide*.

Supported Standards

Requests for Comments (RFCs) are an evolving series of reports, proposals for protocols, and protocol standards used by the Internet community. TCP/IP standards are defined in RFCs published by the Internet Engineering Task Force (IETF) and other working groups. Table 1.1 lists the RFCs supported in this version of Microsoft TCP/IP (and Microsoft Remote Access Service).

Table 1.1 Requests for Comments (RFCs) Supported by Microsoft TCP/IP

RFC	Title
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)
816	Fault Isolation and Recovery
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)
950	Internet Standard Subnetting Procedure
959	File Transfer Protocol (FTP)

(continued)

Table 1.2 Requests for Comments (RFCs) Supported by Microsoft TCP/IP

RFC	Title
1001, 1002	NetBIOS Service Protocols
1034, 1035	Domain Name System (DNS)
1042	IP over Token Ring
1055	Transmission of IP over Serial Lines (IP-SLIP)
1112	Internet Group Management 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)
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
1518	An Architecture for IP Address Allocation with CIDR
1519	Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy
1533	DHCP Options and BOOTP Vendor Extensions [1]
1534	Interoperation Between DHCP and BOOTP
1541	Dynamic Host Configuration Protocol (DHCP)
1542	Clarifications and Extensions for the Bootstrap Protocol [2]
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

[1] The Microsoft DHCP server does not support BOOTP. BOOTP requests are silently ignored. However, a DHCP server and a BOOTP server can coexist.

[2] Windows NT Server can be configured to act as a BOOTP relay agent.

Note For details on retrieving RFCs by means of FTP or email, send an email message to "rfc-info@ISI.EDU" with the subject "getting rfcs" and the message body "help: ways_to_get_rfcs".

RFCs can be obtained by means of FTP from NIS.NSF.NET, NISC.JVNC.NET, VENERA.ISI.EDU, WUARCHIVE.WUSTL.EDU, SRC.DOC.IC.AC.UK, FTP.CONCERT.NET, DS.INTERNIC.NET, or NIC.DDN.MIL.

Internetworking

This section summarizes how Microsoft TCP/IP works with Windows NT to provide enterprise internetworking solutions. For a more detailed discussion of these points, see the *Microsoft Windows NT Resource Kit Networking Guide*.

Using TCP/IP for Scalability

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-based 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, with enhancements to support wide area networks (WAN), TCP/IP printing, FTP, Telnet, DHCP, WINS, and DNS client software, Windows Sockets, and extended LMHOSTS file.
- Microsoft Windows NT Server, with the same enhancements as Windows NT Workstation, plus Internet Information Server, DHCP Server, WINS Server, and DNS Server software.
- Microsoft Windows 95, with enhancements to support wide area networks (WAN), DHCP, WINS, and DNS client software, extended LMHOSTS file, and Windows Sockets.
- Microsoft TCP/IP-32 for Windows for Workgroups, 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, WINS and DNS client software.
- Microsoft LAN Manager—including both client and server support for Windows Sockets—and MS-DOS–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.

As shown in Figure 1-2, 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*).

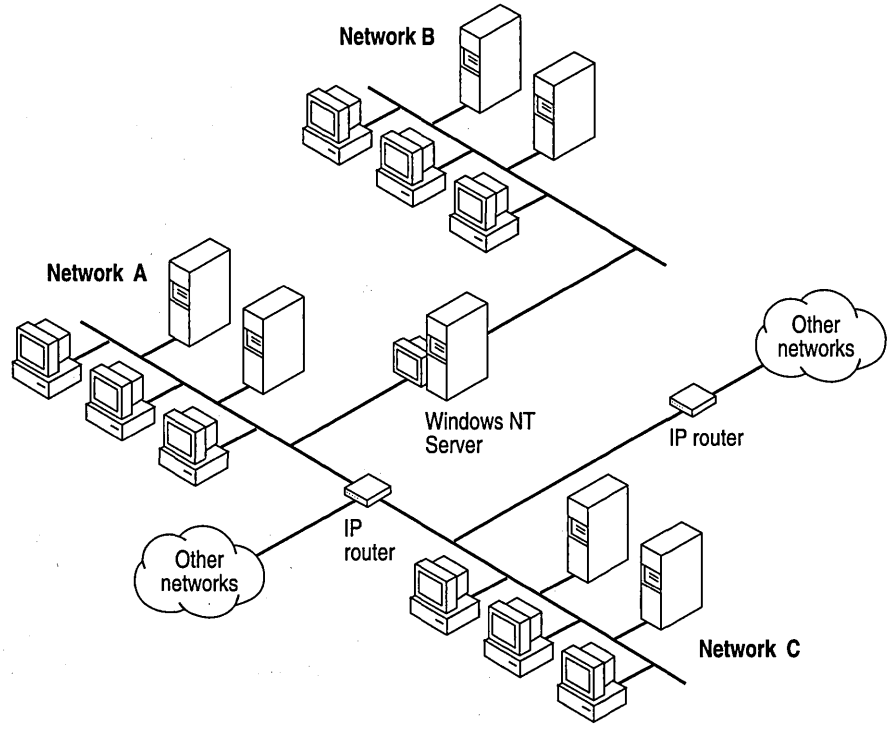


Figure 1-2 TCP/IP for Windows NT Supports IP Routing for Multihomed Systems

Using TCP/IP in Heterogeneous Networks

Because most modern operating systems support TCP/IP protocols, heterogeneous computers on an internetwork can use simple networking applications and utilities to share information. TCP/IP enables Windows NT to 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

As shown in Figure 1-3, 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 the following transport protocols:

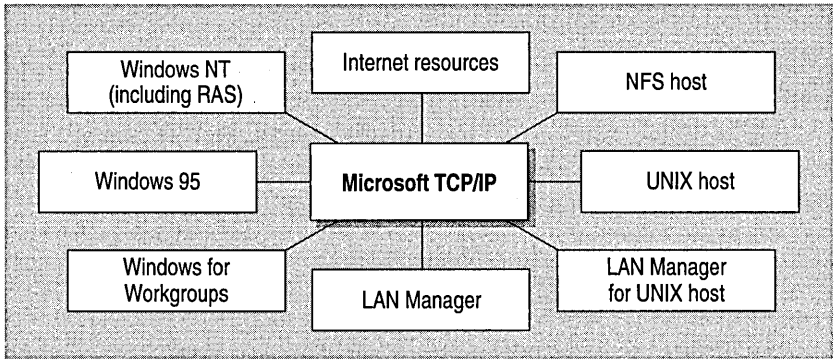


Figure 1-3 Microsoft TCP/IP Connectivity

- 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-based 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 IBM LAN Server networks.
- AppleTalk for connecting to and sharing resources with Macintosh systems.

Note Transport protocols (such as DECnet and OSI) from third-party vendors can also be used by Windows NT networking services.

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.

The Windows Sockets standard defines a networking API that developers use to create applications for the entire family of Microsoft 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 major vendors implementing TCP/IP for Windows systems.

The Windows Sockets standard ensures compatibility with Windows-based TCP/IP utilities developed by many vendors. This includes third-party applications for X Windows, 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 run on Windows NT without modification or recompilation.

For example, third-party applications for X Windows provide strong connectivity solutions by means of X Windows servers, database servers, and terminal emulation. With such applications, a computer running Windows NT can work as an X Windows server while retaining compatibility with applications created for Windows NT, Windows 95, Windows 3.*x*, and MS-DOS on the same system. Other third-party software includes X Windows client libraries for Windows NT, which enable developers to write X Windows client applications on Windows NT that can be run and displayed remotely on X Windows servers.

The TCP/IP utilities for Windows NT 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 TCP/IP implementations. Windows Sockets is designed to:

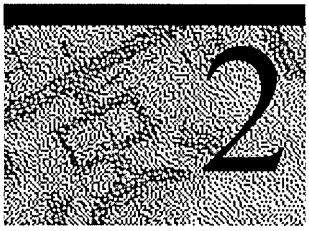
- Provide a familiar networking API to developers using Windows NT, Windows 95, Windows for Workgroups, or UNIX.
- Offer binary compatibility between vendors for heterogeneous Windows-based TCP/IP stacks and utilities.
- Support both connection-oriented and connectionless protocols.

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.

Specifications for Windows Sockets are available on numerous Internet sites such as www.microsoft.com, the Microsoft Network (MSN), and CompuServe.

CHAPTER 2

Microsoft TCP/IP Architecture



TCP/IP protocols map to a four-layered conceptual model: Application, Transport, Internet, and Network Interface. This model is officially known as the *TCP/IP Internet Protocol Suite* but is often referred to as *the TCP/IP protocol family*. As shown in Figure 2-1, each layer in the TCP/IP model corresponds to one or more layers of the International Standards Organization (ISO) seven-layer Open Systems Interconnection (OSI) model.

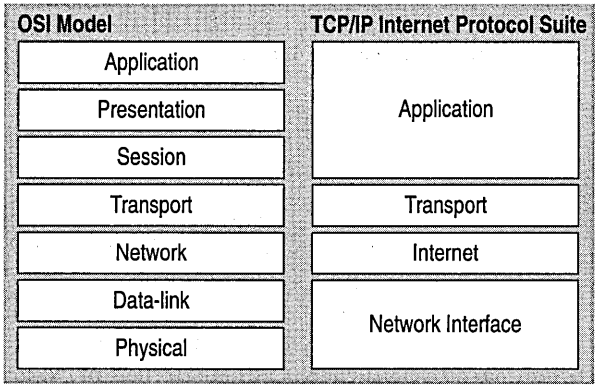


Figure 2-1 TCP/IP and the OSI Model

The TCP/IP Protocol Suite

Defined within the four layers of TCP/IP are protocols that dictate how computers connect and communicate. The most common of these protocols are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Protocol (IP), Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP). The following sections introduce these protocols, explain how they relate to Windows NT networking, and describe where and how TCP/IP configuration parameters are stored on Windows NT.

Transmission Control Protocol

The most common higher-level protocol in the suite is Transmission Control Protocol (TCP). It provides a reliable, connection-oriented packet delivery service on top of (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. If the network either corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty packet. This reliability makes TCP 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 additional bits to provide proper sequencing of information, as well as a mandatory checksum to ensure reliability of both the TCP packet header and the packet data. To guarantee successful data delivery, the protocol also requires that the recipient acknowledge successful receipt of data.

Such acknowledgments (ACKs) generate additional network traffic, diminishing the rate at which data passes in favor of reliability. To reduce the impact on performance, most hosts send an acknowledgment for every other segment or when a specified time interval has passed.

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 might 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 the integrity of both the header and data. ACKs are not enforced by the UDP protocol; this is left to higher-level protocols.

UDP also supports sending data from a single sender to multiple receivers.

Internet Protocol

Internet Protocol (IP) provides packet delivery for all other protocols within the suite. It 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.

Address Resolution Protocol

Not directly related to data transport, but important nonetheless, the Address Resolution Protocol (ARP) is one of the maintenance protocols that supports the TCP/IP suite and is usually invisible to users and applications.

If two systems are to communicate across a TCP/IP network, the system sending the packet must map the IP address of the final destination to the physical address of the final destination. IP acquires this physical address by broadcasting a special inquiry packet (an ARP *request packet*) containing the IP address of the destination system. All ARP-enabled systems on the local IP network detect these broadcast messages, and the system that owns the IP address in question replies by sending its physical address to the requester (in an ARP reply packet). The physical/IP address is then stored in the ARP cache of the requesting system for subsequent use.

Because the ARP reply can also be broadcast to the network, other systems on the network can use this information to update their own ARP caches. (Use the **arp** utility to view the ARP tables.)

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is another of the maintenance protocols. It allows two systems on an IP network to share 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 IP network implementation.)

The **ping** utility uses the ICMP *echo request* and *echo reply* packets to determine whether a particular IP system on a network is functional. For this reason, the **ping** utility is useful for diagnosing IP network or router failures.

TCP/IP and the Windows NT Network Architecture

The architecture of the Microsoft Windows NT operating system with integrated networking is protocol-independent. This architecture, illustrated in Figure 2-2, provides application, file, print, and other services over any network protocol that supports the *transport driver interface* (TDI). The protocols package network requests for applications in their respective formats and send the requests to the appropriate network adapter by means of the *network device interface specification* (NDIS) interface. NDIS allows multiple network protocols to reside over a wide variety of network adapters and media types.

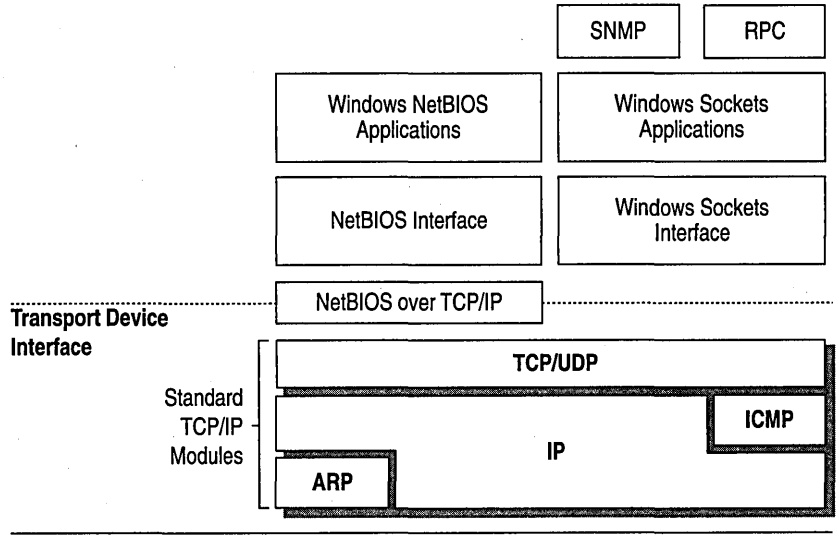


Figure 2-2 Architectural Model of Windows NT with TCP/IP

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

TCP/IP and the Windows NT Configuration Database

TCP/IP configuration information is stored in the Windows NT Registry. The Registry, illustrated in Figure 2-3, is a hierarchical database that provides a central repository for hardware-specific information.

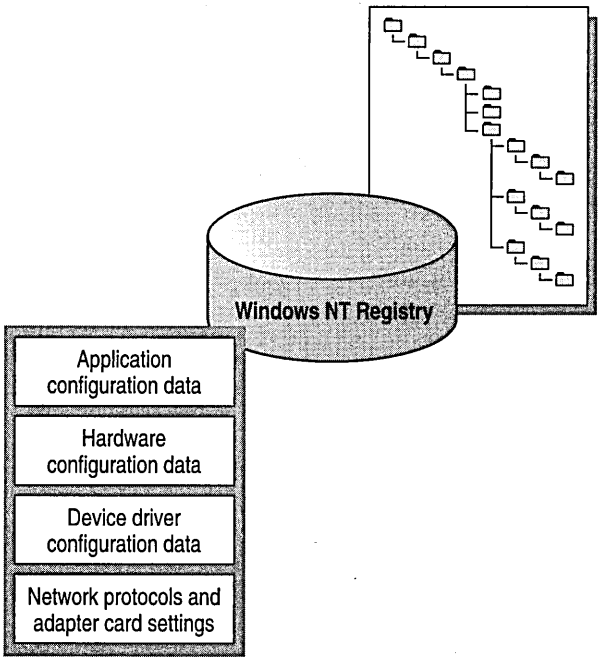


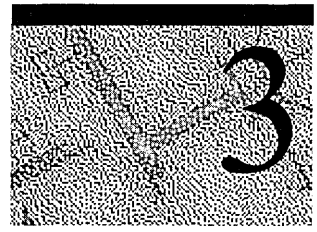
Figure 2-3 Conceptual View of the Windows NT Registry

In general, the TCP/IP-configuration parameters (such as IP address and computer name) are modified by means of the Windows NT Control Panel or the Administrative Tools (Common) folder. However, parameters that are not routinely changed, such as default Time To Live (TTL) and default Type Of Service (TOS), can be modified only by means of the Registry (with the Registry Editor).

Caution Incorrectly adjusting TCP/IP registry parameters may adversely affect system performance. For a description of these parameters, see the REGENTRY.HLP help file on the *Microsoft Windows NT Resource Kit* CD-ROM.

CHAPTER 3

Implementation Considerations



Administration of Microsoft TCP/IP and related services splits roughly into two functional areas:

- *Client Configuration Options.* Every computer on a TCP/IP internetwork must be given a unique computer name and IP address. The IP address identifies both the computer and the subnetwork to which it is attached. When the computer is moved to a different subnetwork, the IP address must be changed to reflect the new subnetwork ID.
- *Name Resolution Services.* People use "friendly" names to connect to computers; programs use IP addresses. TCP/IP internetworks require a *name resolution service* that converts computer names to IP addresses and IP addresses to computer names.

Client Configuration Options

This section begins with a high-level overview of IP addressing, introduces the Dynamic Host Configuration Protocol (DHCP), and concludes with a brief overview of IP-addressing under Windows NT Remote Access Service (RAS). For further information about RAS, see the RAS chapters in this manual.

Understanding IP Addressing

To receive and deliver packets successfully between computers, TCP/IP requires that three values be provided by the network administrator: an IP address, a subnet mask, and a default gateway (router).

Note Users running Windows NT on networks with DHCP servers can take advantage of automatic system configuration and do not need to manually configure these TCP/IP values.

IP Addresses

Every device attached to a TCP/IP network is identified by a unique *IP address*. (If a computer has multiple network adapters, each adapter will have its own IP address.) This address is typically represented in dotted-decimal notation, that is, with the decimal value of each octet (eight bits, or one byte) of the address separated by a period. Here is a sample IP address:

```
138.57.7.27
```

Important Because IP addresses identify devices on a network, each device on the network must be assigned a unique IP address.

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 ID of your computer.

- The *network ID* identifies the systems that are located on the same physical network. All systems on the same physical network must have the same network ID, and the network ID must be unique to the internetwork.
- The *host ID* identifies a workstation, server, router, or other TCP/IP device within a network. The address for each device must be unique to the network ID.

A computer connected to a TCP/IP network 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 computers with the same network ID accept each other's IP-level broadcast messages.)

Note Networks that connect to the public Internet must obtain an official network ID from the *Internet Network Information Center* (InterNIC) to guarantee IP network ID uniqueness. For more information, visit the InterNIC home page on the Internet at: **http://www.internic.net/**

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 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. The address class can be discerned from the first octet of an IP address. Table 3.1 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 example uses w.x.y.z to designate the bytes of the IP address.

Table 3.1 IP Address Classes

Class	w values [1,2]	Network ID	Host ID	Available networks	Available hosts per network
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

1 Inclusive range for the first octet in the IP address.

2 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 (Internet Group Management Protocol multicast and others) and cannot be used as host addresses.

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. Subnet masks are created by assigning 1's to network ID bits and 0's to host ID bits. The 32-bit value is then converted to dotted-decimal notation, as shown in Table 3.2.

Table 3.2 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

For example, when the IP address is 138.57.7.27 and the subnet mask is 255.255.0.0, the network ID is 138.57 and the host ID is 7.27.

Because the class of a host is easily determined, configuring a host with a subnet mask might seem redundant. But subnet masks are also used to further segment an assigned network ID among several local networks. Sometimes only *portions* of an octet need to be segmented using only a few bits to specify subnet IDs.

Important To prevent addressing and routing problems, all computers on a logical network must use the same subnet mask and network ID.

IP Routing

TCP/IP networks are interconnected by *routers*, which are devices that pass IP packets from one network to another.

For each computer on an IP network, you can maintain a table with an entry for every other computer or network with which the local computer communicates. In general, this is not practical, and the default gateway (router) is used instead. (The default gateway is a computer connected to the local subnet and to other networks. It has knowledge of the network IDs for other networks in the internetwork and how to reach them. It 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. It then examines the destination address, compares it to a locally maintained *route table*, and takes appropriate action based on what it finds. There are three possible actions:

- It can pass the packet up to a protocol layer above IP on the local host.
- It can be forwarded through one of the locally attached network adapters.
- It can be discarded.

The search for a match of the destination address in the route table proceeds from the specific to the general in the following order:

- The table is examined for an exact match (host route).
- The host portion is stripped from the destination address, and the table is examined for a match (subnet route).
- The subnet portion is stripped from the destination address, and the table is examined for a match (network route).
- The default gateway is used.
- If a default gateway has not been specified, the packet is discarded.

Because the default gateway contains information about the network IDs of the other networks in the internetwork, it can forward the packet to other routers until the packet is eventually delivered to a router connected to the specified destination. This process is known as *routing* and is illustrated in Figure 3-1.

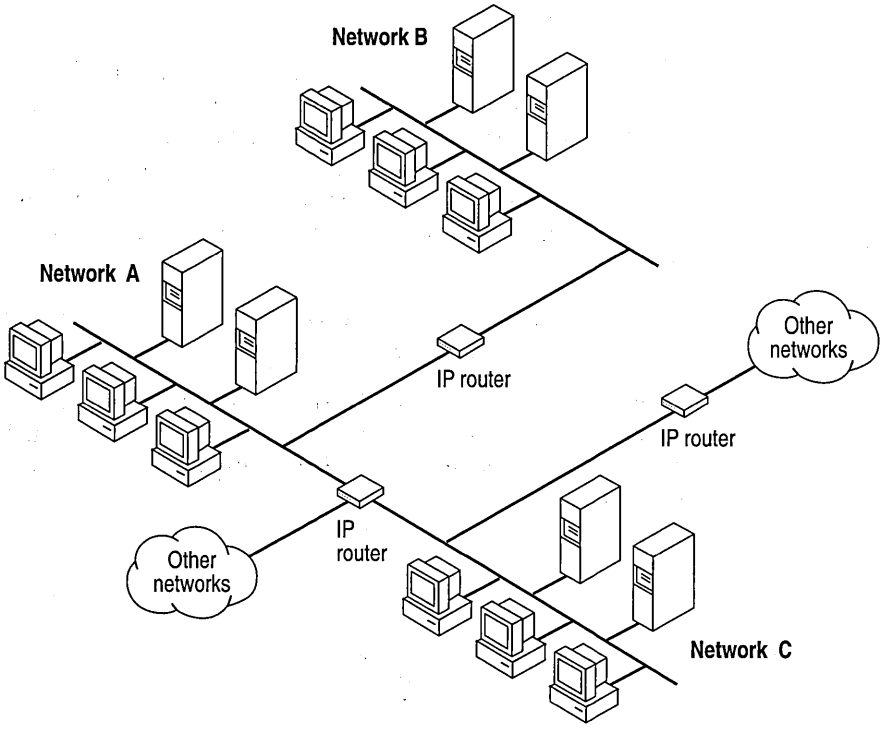


Figure 3-1 Internetwork Routing Through Routers

Note If the default gateway becomes unavailable, communication beyond the local subnet can be impaired. To prevent this, use the Network application in Control Panel to specify multiple default gateways, or use the **route** utility to manually add routes to the route table for heavily used systems or networks.

Dynamic Host Configuration Protocol

Assignment and maintenance of IP-address information can be an administrative burden. To provide a degree of relief, the Dynamic Host Configuration Protocol (DHCP) offers dynamic configuration of IP addresses and related information.

The network administrator controls how IP addresses are assigned by specifying *lease durations* that specify how long a computer can use an assigned IP address before having to renew the lease with the DHCP server. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of IP addresses through centralized management of address allocation.

For example, 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 supply new configuration information. This feature is significant for both mobile computer users with portables that are docked at different computers and for computers that are frequently moved.

The DHCP client and server services for Windows NT are implemented under the following RFCs: 1533, 1534, 1541, 1542.

Figure 3-2 illustrates a DHCP server providing configuration information on two subnets. If, for example, Client C is moved to Subnet 1, the DHCP server automatically supplies new TCP/IP configuration information the next time that Client C is started.

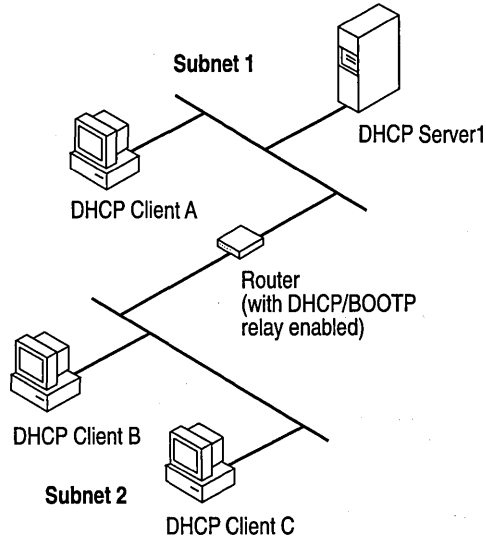


Figure 3-2 DHCP Clients and Servers on a Routed Network

Note You can configure Windows NT Server 4.0 to act as a DHCP relay agent. (A DHCP relay agent relays DHCP and BOOTP broadcast messages between a DHCP/BOOTP server and a client across an IP router.) If it is impractical or impossible to configure the router in the illustration to support DHCP relay, a Windows NT Server computer on Subnet 2 can be configured as the DHCP relay agent to forward DHCP messages to Subnet 1. You could also replace the router in the illustration with a Windows NT Server 4.0 computer that is enabled as a DHCP relay agent and configured to run the multiprotocol routing service. For more information about the multiprotocol routing service, see the Multiprotocol Routing chapters in this manual. For information about configuring either DHCP relay or multiprotocol routing, see Windows NT Help.

How DHCP Clients Get IP Addresses

DHCP uses a client-server model and is based on leases for IP addresses. As illustrated in Figure 3-3, a DHCP client passes through four phases as it acquires a lease from the DHCP server.

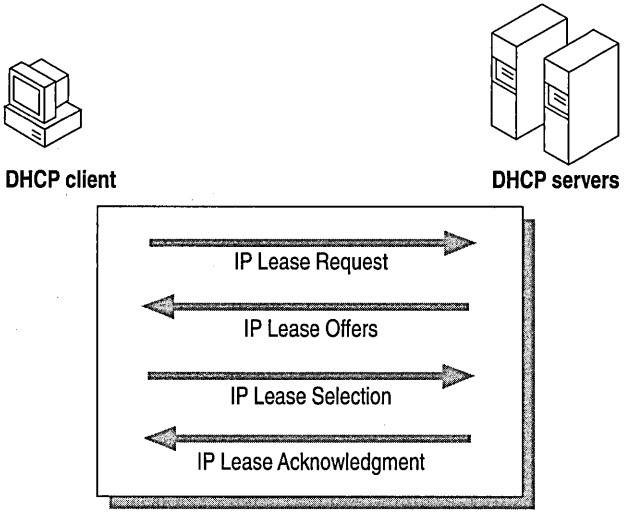


Figure 3-3 DHCP Client and Server Interaction During System Startup

During system startup, a DHCP client computer sends an *IP Lease Request* (as a broadcast message) on the network. Each DHCP server that receives the client's request responds with an *IP Lease Offer* containing an IP address and valid configuration information for the client that sent the request.

After sending the IP Lease Request, the client waits for IP Lease Offers to come back. If the client does not receive an IP Lease Offer from a DHCP server, it will resend the IP Lease Request four times every five minutes until it does.

The client then selects one of the IP Lease Offers—typically the first one received—and responds to the DHCP server with an *IP Lease Selection*, which indicates acceptance of the offered IP Address.

The selected DHCP server sends an *IP Lease Acknowledgment* that contains the address first sent in the IP Lease Offer, plus a valid lease for the address and the TCP/IP network configuration parameters for the client. After the client receives the acknowledgment, it can participate on the TCP/IP network and complete its system startup.

Note When a DHCP client is shut down and restarted (on the same subnet), it will typically obtain a lease for the same IP address it had prior to the shutdown.

As the lease approaches its expiration date, the client tries to renew it:

- When 50% of the lease time has expired, the client tries to renew the lease with the DHCP server that originally assigned it.
- If the client is unable to communicate with the original DHCP server, and 87.5% of the lease time has expired, the client tries to renew the lease by broadcasting a request to any available DHCP server.
- If the lease expires, the client must immediately discontinue using the IP address and begin again with a new *IP Lease Request.*

In Windows NT Server, the network administrator uses DHCP Manager to define local policies for address allocation, leases, and other options. For information about the steps for setting up TCP/IP using DHCP, or for information about the DHCP Manager tool, see Windows NT Help. For further information about planning for DHCP deployment, see the *Microsoft Windows NT Resource Kit Networking Guide.*

IP Addressing for RAS

Remote dial-in access to internetworks is provided by a built-in feature of Windows NT known as *Remote Access Service* (RAS). RAS is based on a client-server architecture in which a remote RAS-based client connects to a local RAS server. After the connection has been made, the client running RAS becomes a full-fledged host on the network, and the remote user can then use the same Windows-based tools as a local user to access resources such as files, printers, electronic mail, and databases.

As shown in Figure 3-4, RAS supports multiple protocols, two of which are TCP/IP over Point-to-Point Protocol (PPP), and Serial Line IP (SLIP). Such protocol support allows a client with a RAS connection to interoperate with the heterogeneous servers typically found on today's internetworks.

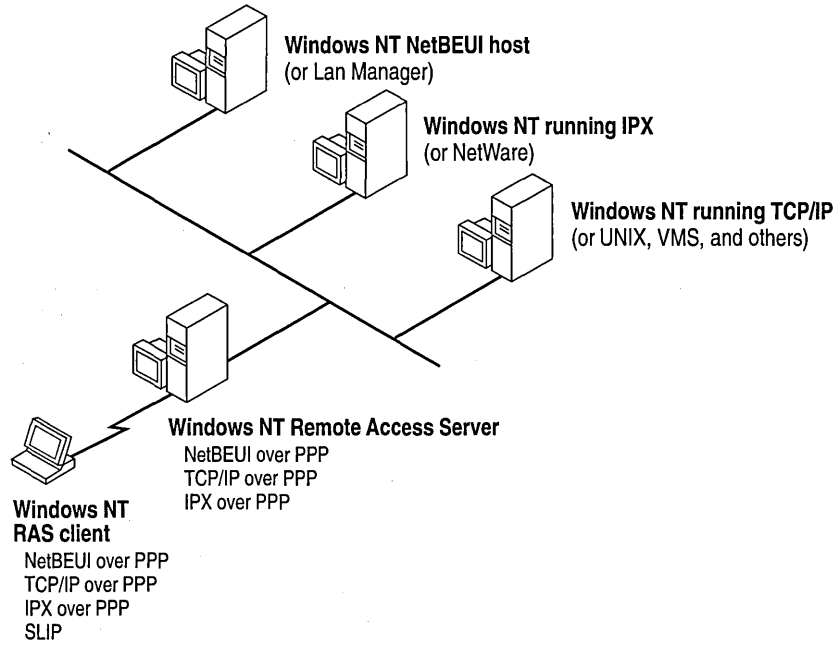


Figure 3-4 Network Access with RAS in Windows NT

Client configuration options are handled directly by the RAS server. The RAS server reserves a pool of IP addresses for static configuration during RAS installation. These addresses are automatically assigned to RAS clients who dial in using PPP. 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 to other computers on the network.)

Clients running RAS can use the same name resolution services as hosts connected directly to the internetwork. For further information about RAS, see the RAS chapters in this manual.

Name Resolution Services

Windows NT with TCP/IP requires a unique IP address and computer name for each computer on the network. A mechanism must be available on a TCP/IP network to match computer names to IP addresses. These are called *name resolution services*.

Background

As networks have grown in complexity, so have these name resolution mechanisms increased in sophistication.

NetBIOS and DNS Computer Names

Windows NT networking components rely on a naming convention known as *NetBIOS*. In general, NetBIOS computer names consist of a single part.

In contrast, TCP/IP components rely on a naming convention know as the *Domain Name System* (DNS). DNS computer names consist of two parts: a *host name* and a *domain name*, which combined form the *fully qualified domain name* (FQDN).

Fortunately, NetBIOS computer names are compatible with DNS host names, making interoperation possible between the two. Windows NT combines the NetBIOS computer name with the DNS domain name to form the FQDN.

Note Under Windows NT, the DNS host name defaults to the same name as the NetBIOS computer name. You can change this if you need separate names.

Flat vs. Hierarchical Name Spaces

The original naming scheme for both NetBIOS and TCP/IP consisted of a *flat name space* where each computer was assigned a single-part name. (A single-part name consists of a short sequence of characters without any additional structure.) Flat name spaces worked well for simple networks with relatively few interconnected computers, but as network complexity increased, they rapidly become inadequate for the following reasons:

- Single-part names are derived from a finite set of identifiers. The potential for conflict increases with the number of computers interconnected.

- Administration of the name space rests with a central authority. Someone must ensure that each computer is assigned a unique name. Because there is no convenient way to segment a flat name space, control of name assignment must be centralized.
- All changes to the network must be approved by the central authority. Before a new computer is added to the network or an existing computer is moved to a different subnet, the change must be coordinated with the central authority. For a large network, this results in a significant administrative burden.

A hierarchical name space implemented as a multi-part naming scheme enables authority to be distributed and administration to be decentralized. A hierarchical name space can be viewed as an inverted tree with the branches and leaves pointing down. A central authority still manages the top of the tree, but below the top level the structure can be distributed into autonomous administrative units. Name uniqueness must still be enforced at the lowest administrative level, but this is a reasonable task for a well-segmented name space. The hierarchical structure of the name space guarantees name uniqueness above these lower levels.

Implementations of hierarchical naming schemes exist for both TCP/IP and NetBIOS: Domain Name System (DNS) for TCP/IP and NetBIOS Scope for NetBIOS.

Name Space Implementations

The first implementations of name spaces—both flat and hierarchical—relied on text files for mapping of computer name to IP address. Each computer on the internetwork had its name and IP address on a line in the file, and a copy of the file existed on each computer. This solution worked well for simple networks having relatively few interconnected computers. As networks grew in size and complexity, this method ran into scaling problems similar to those experienced with a flat name space.

Newer implementations have largely done away with the need for a mapping file on each machine; instead, server-based repositories store the necessary information. Mapping files still exist but are typically used in simple networks or as a safety feature in case the name servers are down.

The mapping files are

- HOSTS for DNS names
- LMHOSTS for NetBIOS names

Note When you install Windows NT, example HOSTS and LMHOSTS files are placed in the *\systemroot*\SYSTEM32\DRIVERS\ETC directory.

NetBIOS over TCP/IP (NetBT) Name Resolution

Name resolution services for Windows NT fall into two general categories. Each provides similar services for clients and can operate independently or in tandem. They are

- *NetBIOS over TCP/IP* (NetBT)
- *Domain Name System* (DNS)

NetBT is the session-layer network service that performs name-to-IP address mapping for name resolution. Under Windows NT, it is implemented through the Windows Internet Name Service (WINS) and broadcast name resolution. The two most important aspects of the related naming activities are *registration* and *resolution*:

- Registration is the process used to register a unique name for each computer (node) 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.

Note RFCs 1001 and 1002 specify how NetBIOS should be implemented over TCP/IP and define the name resolution modes.

Defined within NetBT are modes that specify how network resources are identified and accessed. The most common NetBT modes are

- *b-node*, which uses broadcast messages to resolve names
- *p-node*, which uses point-to-point communications with a name server to resolve names
- *m-node*, which first uses b-node and then—if necessary—p-node to resolve names
- *h-node*, which first uses p-node for name queries and then b-node if the name service is unavailable or if the name is not registered in the database

---

Note The RFCs refer to a NetBIOS Name Server (NBNS). WINS is an enhanced NBNS.

The two most common node types for client computers running Windows NT are h-node and b-node. If the client computer is configured to use WINS, Windows NT defaults to h-node; otherwise, the default node type is b-node.

Important For DHCP clients on a Windows NT network, the node type is assigned by the DHCP server.

When WINS servers are in place on the network, NetBT resolves names on a client computer by communicating with the WINS server. When WINS servers are not in place, NetBT uses b-node broadcast messages to resolve names. NetBT can also use LMHOSTS files and DNS for name resolution, depending on how TCP/IP is configured on a particular computer.

Note In Windows NT, the NETBT.SYS module provides the NetBT functionality that supports name registration and resolution modes.

Windows NT supports all NetBT modes described in the following sections. NetBT is also used with the LAN Manager 2.*x* Server message protocol.

B-Node

The b-node mode uses broadcast messages for name registration and resolution. For example, if a computer named NT_PC1 wants to communicate with a computer named NT_PC2, NT_PC1 sends a broadcast message that it is looking for NT_PC2, and then it waits a specified time for NT_PC2 to respond.

B-node has two major problems:

- In a large environment, it loads the network with broadcast messages.
- Typically, routers do not forward broadcast messages, so computers on opposite sides of a router 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 broadcast messages. All computers register themselves with the WINS server, which is responsible for knowing computer names and addresses and for ensuring that no duplicate names exist on the network.

In this environment, when NT_PC1 wants to communicate with NT_PC2, it queries the WINS server for the address of NT_PC2. Upon receipt of the address, NT_PC1 goes directly to NT_PC2 without broadcasting. Because the name queries go directly to the WINS server, p-node avoids loading the network with broadcast messages. Because broadcast messages are not used, and because the address is received directly, computers can be on opposite sides of routers.

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

- All computers must be configured (typically through DHCP) to know the address of the WINS server.
- If the WINS server is down, computers that rely on it to resolve addresses cannot get to any other systems on the network.

M-Node

The m-node mode was created primarily to solve the problems associated with b-node and p-node. In an m-node environment, a computer first attempts registration and resolution using b-node. If that fails, it switches to p-node. Advantage are as follows:

- M-node can cross routers.
- 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.
- In theory, it should increase local area network (LAN) performance.

H-Node

The h-node mode solves the most significant problems associated with broadcast messages and with routed-environment operations. It is a combination of b-node and p-node that uses broadcast messages as a last effort. The h-node mode does more than change the order for using b-node and p-node: If the WINS server is down—making broadcast messages a necessity—the computer continues to poll the WINS server. When the WINS server can be reached again, the system returns to p-node. H-node can also be configured to use the LMHOSTS file after broadcast name resolution fails.

Because p-node is used first, no broadcast messages are generated if the WINS server is running, and computers can be on opposite sides of 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.

Note 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.

Other Combinations

Another variation, known as *modified b-node*, is also used in Microsoft networks so that messages can go across routers. Modified b-node does not use p-node mode or a WINS server. 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 the *Microsoft Windows NT Resource Kit Networking Guide*), but modified b-node is not an ideal solution.

Some sites might require both b-node and p-node modes. Although this configuration can work, administrators must exercise extreme caution, using it only for transition situations. Because p-node hosts disregard broadcast messages, and b-node hosts rely on broadcast messages for name resolution, the two hosts can potentially be configured with the same NetBIOS name, leading to unpredictable results. Also, 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.

Computers running Windows NT 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 (WINS) and Broadcast Name Resolution

WINS provides a replicated, dynamic database for registering and querying NetBIOS computer-name-to-IP address mappings in a routed network environment. WINS is designed to solve the problems that occur with name resolution in complex internetworks.

WINS reduces the use of local broadcast messages 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 administrator needs to make changes manually.

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

This section provides an overview of how name resolution is provided by WINS and name-query broadcast messages. For information about installing and configuring WINS servers, see Windows NT Help.

WINS in a Routed Environment

WINS consists of two components:

- The WINS server, which handles name queries and registrations
- The client software, which queries for computer name resolution

Windows-based networking clients (WINS-enabled Windows NT, Windows 95, or Windows for Workgroups 3.11 computers) can use WINS directly. Non-WINS computers that are b-node compatible (as described in RFCs 1001 and 1002) can access WINS through *proxies* (WINS-enabled computers that listen to name-query broadcast messages and then respond for names that are not on the local subnet or are p-node computers).

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

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

Figure 3-5 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 broadcast messages access the WINS server through proxies. Proxies intercept the broadcast messages and send them directly to the WINS server.

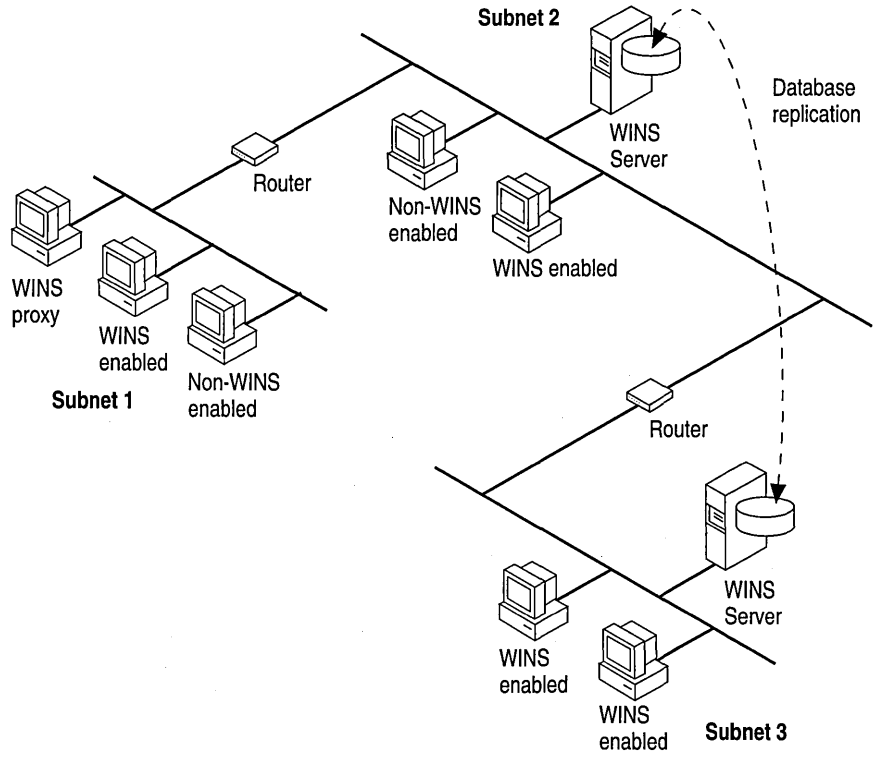


Figure 3-5 Example of an Internetwork with WINS Servers

The proxy communicates with the WINS server to resolve names and then caches the names for a certain time. The proxy serves as an intermediary, either communicating with the WINS server or supplying a name-to-IP address mapping from its cache. Figure 3-6 shows the relationships among WINS servers and clients, including proxies for non-WINS computers.

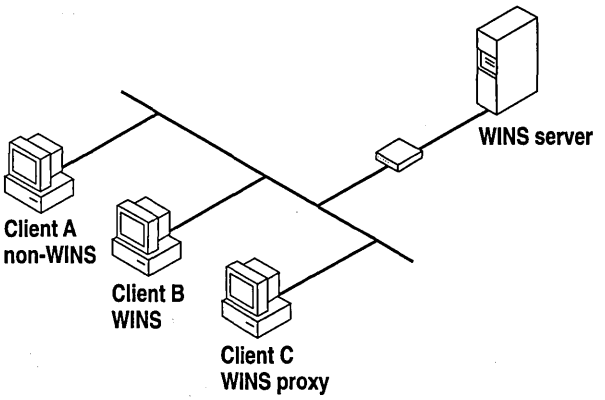


Figure 3-6 Example of Clients and Servers Using WINS

In Figure 3-6, Client A is a not enabled for WINS, Client B is enabled for WINS, and Client C is a WINS proxy agent. Table 3.3 shows the typical steps that Client A and Client B take when resolving names.

Table 3.3 Name Resolution on WINS and Non-WINS Clients

Client A (Non-WINS)	Client B (WINS)
Client A sends a query (as a broadcast message) for Client X's IP address. Client X (not shown) is not on the local subnet. [1]	Client B queries the WINS server for Client A's IP address.
Client C (WINS proxy) intercepts the broadcast message and sends it directly to the WINS server. [2]	The WINS server responds directly to Client B with Client A's IP address. [3]

(continued)

Table 3.4 Name Resolution on WINS and Non-WINS Clients

Client A (Non-WINS)	Client B (WINS)
The WINS server responds directly to Client C with Client X's IP address.	If the WINS server is unreachable, the query fails. Client B switches to b-node and sends the query as a broadcast message on the local subnet.
Client C responds directly to Client A with Client X's IP address.	Client A receives the broadcast and responds directly to Client B.

[1] If Client X was on the local subnet, it would respond directly to Client A's query.

[2] Client C may already have the requested information in cache. If so, Client C responds directly to Client A without going to the WINS server.

[3] Both examples assume that the requested information is available in the WINS database on the server.

Note If the client computer running Windows NT is also DHCP-enabled, and if 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 Windows NT Help.

In a WINS and broadcast name resolution environment, a WINS-enabled client computer will behave differently than a non-WINS-enabled client computer. These differences will be apparent in the way these clients handle *resolution*, *registration*, *release*, and *renewal*.

Name Resolution

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

If WINS is not enabled on the client: The computer registers its name by sending *name registration request* packets (as broadcast messages) to the local subnet. To find a particular computer, the non-WINS computer sends *name query request* packets (as broadcast messages) on the local subnet. (This broadcast message 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 on the client: The computer first queries the WINS server. If that fails, it sends name registration and query requests (as broadcast messages) in the following series of steps:

1. During TCP/IP configuration, the client computer registers its name with the WINS server. This is shown in Figure 3-7. (Notice that the WINS database is replicated among all WINS servers on the internetwork.)

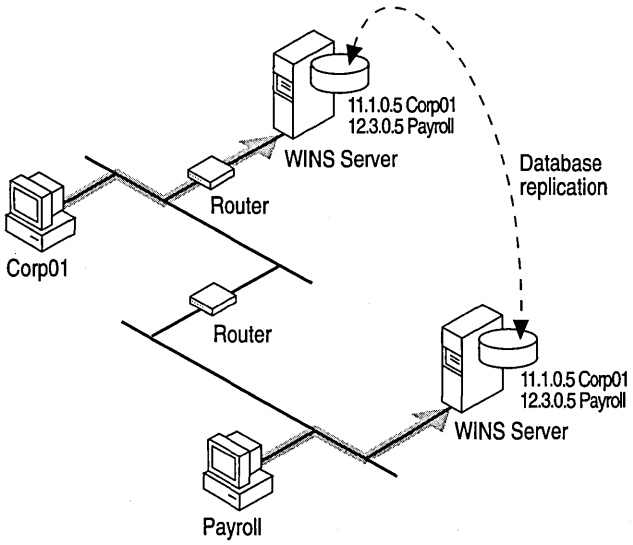


Figure 3-7 Name Registration in the WINS Database

2. As illustrated in Figure 3-8, a client's *name query request* is sent first to the WINS server. If the name is found in the WINS database, the client can establish a session based on the address mapping received from the WINS server.

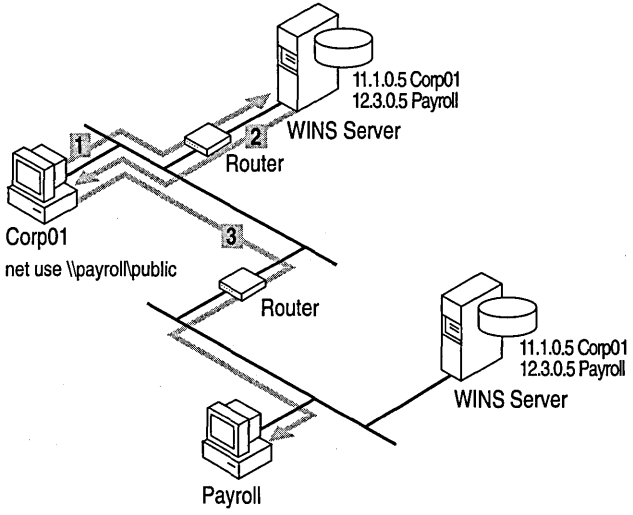


Figure 3-8 Processing a Name Query Request

3. If the WINS server query is unsuccessful, and if the client computer is configured as an h-node, the client computer sends *name query request* packets (as broadcast messages) in the same manner as a non-WINS-enabled computer.
4. Finally, if other methods fail, the local LMHOSTS file is checked. (Included in the search are any centralized LMHOSTS files referred to in #INCLUDE statements in the local file.)

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.

Name Registration

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

If WINS is enabled on the client: 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 on the client: For a non-WINS computer to register its name, a *name registration request* packet is broadcast to the local network, stating its NetBIOS 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 for the computer attempting to register the duplicate name. If the *name registration request* remains unchallenged for a specific time period, the requesting computer adopts that name and address.

After a non-WINS computer claims a name, it must challenge duplicate name registration attempts (with a *negative name registration response*) and respond positively to name queries issued on its registered name (with a *positive name query response*). The *positive name query response* contains the IP address of the computer so that the two systems can establish a session.

Name Release

When a computer finishes using a particular name (such as when the Windows NT 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 on the client: 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,* updates the version number, and notifies other WINS servers of the change.

- 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 the computer released its name during an orderly shutdown, the WINS server does not challenge the name when the computer is reconnected. If an orderly shutdown did not occur, the name registration with a new address causes the WINS server to challenge the registration.The challenge fails and the registration succeeds, because the computer no longer has the old address.

If WINS is not enabled on the client: 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, computers simply ignore the request, allowing other computers on the network to acquire the released name.

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 respond only to those name queries that originate on their local subnet.

Name Renewal

Periodically, client computers are required to *renew* their NetBIOS name registrations with the WINS server. When a client computer first registers with a WINS server, the WINS server returns a message that indicates when the client will need to renew its registration:

- The default renewal interval for entries in the WINS database is four days.
- WINS clients register and refresh every two days.
- The primary and backup WINS servers should have the same renewal interval.
- An entry defined as *static* never expires.

If the entry is owned by the local WINS server, the name is released at the specified time unless the client has renewed it. If the entry is owned by another WINS server, the entry is revalidated at the specified time. If the entry does not exist in the database of the WINS server that owns the entry, it is removed from the local WINS database. A name renewal request is treated as a new name registration.

Caution Incorrectly adjusting the renewal interval might adversely affect system and network performance.

Domain Name System Name Resolution

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. DNS specifications are defined in RFCs 1034 and 1035. Although DNS might seem similar to WINS, there is a major difference: WINS is fully dynamic, whereas DNS requires static configuration for computer name-to-IP address mapping.

The Domain Name Space

The DNS database is a tree structure called the *domain name space.* 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. A period (.) separates each part of the names for the network nodes of the DNS domain. For example, the DNS domain name *csu.edu,* specifies the *csu* subdomain whose parent is the *edu* domain; *csu.com* specifies the *csu* subdomain whose parent is the *com* domain. Figure 3-9 illustrates the parent-child relationships of DNS domains.

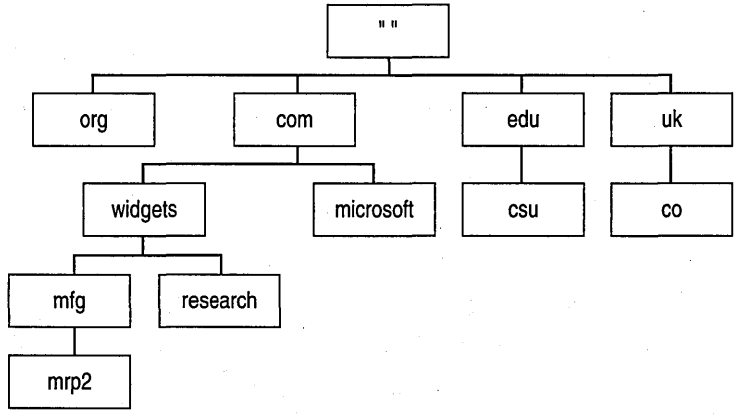


Figure 3-9 A Portion of the DNS Database

Note As shown in Figure 3-9, the root node of the DNS database is unnamed (null). It is referenced in DNS names with a trailing period (.). For example, in the name: "*research.widgets.com.*", it is the period after *com* that denotes the DNS root node.

Top-Level Domains

The root and top-level domains of the DNS database are managed by the InterNIC. The top-level domain names are divided into three main areas:

- *Organizational domains* (3-character names)
- *Geographical domains* (2-character country codes found in ISO 3166)
- The *in-addr.arpa. domain* (a special domain used for address-to-name mappings)

Organizational domain names were originally used in the United States, but as the Internet began to grow internationally, it became obvious that an organizational division was inadequate for a global entity. Geographical domain names were then introduced. Even though a **.us** country domain exists, domain names in the United States are still predominantly organizational. As shown in Table 3.3, there are currently seven organizational domains.

Table 3.5 The DNS Organizational Domains

DNS domain name abbreviation	Type of organization or institution
com	Commercial
edu	Educational
gov	Government
org	Noncommercial
net	Networking
mil	Military
int	International

Delegation

Responsibility for managing the DNS name space below the top level is delegated to other organizations by the InterNIC. These organizations further subdivide the name space and delegate responsibility down. This decentralized administrative model allows DNS to be autonomously managed at the levels that make the most sense for each organization involved.

Zones

The administrative unit for DNS is the *zone*. A zone is a subtree of the DNS database that is administered as a single separate entity. It can consist of a single domain or a domain with subdomains. The lower-level subdomains of a zone can also be split into separate zone(s). Figure 3-10 illustrates the relationship between DNS domains and zones.

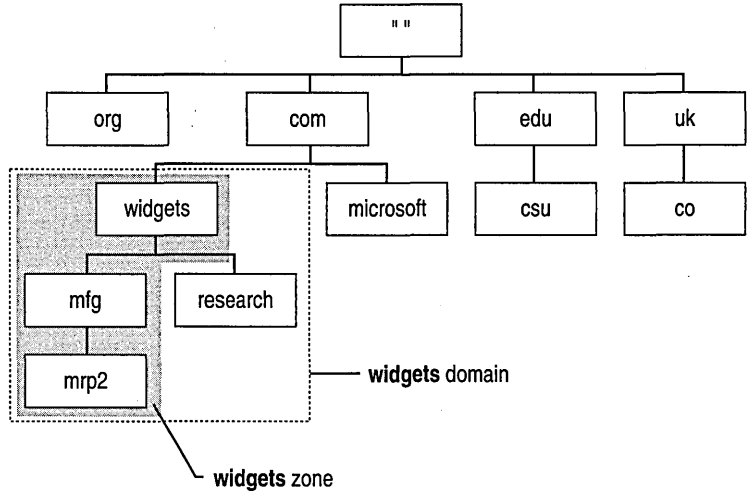


Figure 3-10 DNS Zones

Fully Qualified Domain Names

With the exception of the root, each node in the DNS database has a name (*label*) of up to 63 characters. Each subdomain must have a unique name within its parent domain. This ensures name uniqueness throughout the DNS name space. DNS domain names are formed by following the path from the bottom of the DNS tree to the root. The node names are concatenated, and a period (.) separates each part. Such names are known as *fully qualified domain names* (FQDN). Here's an example of one:

```
mrp2.widgets.mfg.universal.co.uk.
```

Note In practice, most DNS host entries appear no lower than the fifth level of the DNS tree, with three or four being more typical.

Name Servers and Resolvers

DNS uses a client-server model, where the DNS servers (*name servers*) contain information about a portion of the DNS database (*zone*) and make this information available to clients (*resolvers*). A resolver queries a name server for information about the DNS name space. This name server can, in turn, query other name servers as it tries to respond to the query from the resolver.

A DNS zone administrator sets up one or more name servers for the zone:

- A *primary master* name server. A primary server contains the master copy of the database files with resource records for all subdomains and hosts in the zone.
- A *secondary master* name server. A secondary server receives a replicated copy of the database files from the primary server. When the zone structure changes, the primary master database files are modified and copied to the secondary masters. The secondary master files are never touched.
- A *caching-only* name server. Unlike a primary or secondary server, a caching-only server is not associated with any specific DNS zone(s) and contains no database files. A caching-only server starts with no knowledge of the DNS domain structure and must rely on other name servers for this information. Each time a caching-only server queries a name server and receives an answer, it stores the information in its cache. When additional queries come in for this information, the caching-only server answers them directly from cache. Over time, the cache will grow to include the information most often requested.

Although they are not required by the DNS software, secondary servers are a good idea for the following reasons:

- Load balance. Secondary servers ease the load on the primary server. This can be significant in a busy network where name server queries can reach volumes of 20,000 per hour and beyond.
- Fault tolerance. Secondary servers allow DNS name resolution to continue when the primary server is unavailable.
- Reduced network traffic. Secondary servers placed in close proximity to client computers reduces internetwork traffic across routers.

Windows NT Server 4.0 includes RFC-compliant, DNS name-server functionality. Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. For more information about configuring TCP/IP to use DNS services, see Windows NT Help.

In addition to the DNS name server service, Windows NT Server 4.0 includes an RPC-based, graphical administration tool, DNS Manager, that enables administrators to remotely administer DNS name servers. The DNS Manager is similar in function to the Windows NT Server 4.0 WINS Manager. For more information about installing or using these tools, see Windows NT Help.

Name Resolution

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 an FQDN to find its specific address. As illustrated in Figure 3-11, the process begins when a resolver passes a query to its local name server. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. In the worst-case scenario, the local name server starts at the top of the DNS tree with one of the *root name servers* and works its way down until the requested data is found.

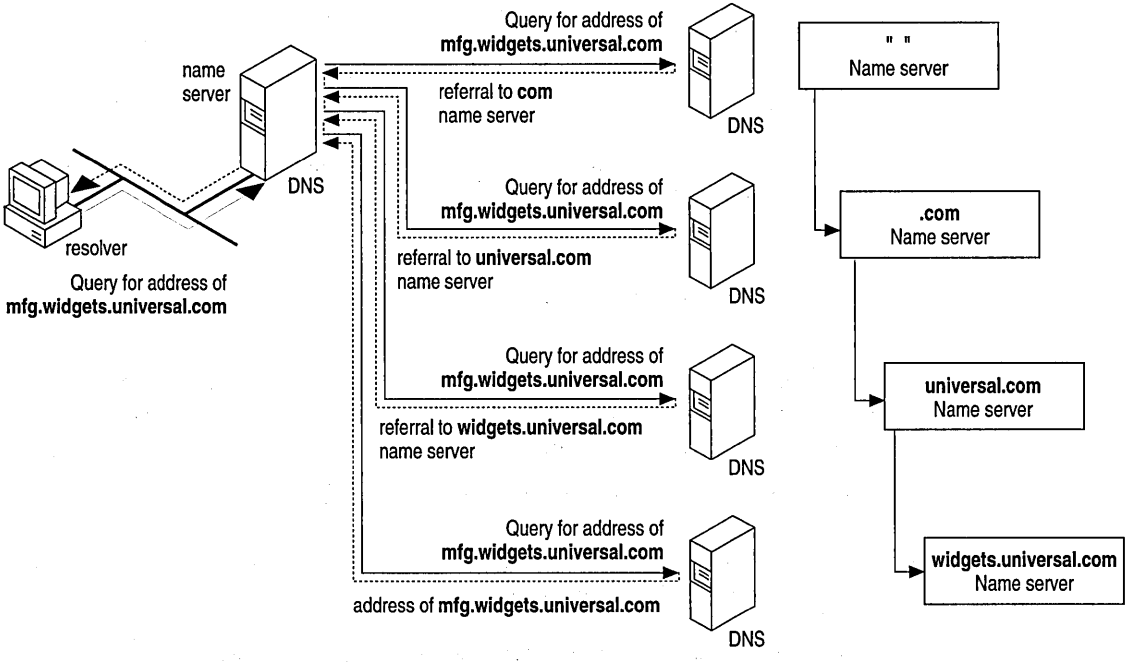


Figure 3-11 DNS Name Resolution

DNS name resolution consists of three key concepts: *recursion, iteration*, and *caching*.

- Recursion

  A resolver typically passes a *recursive resolution request* to its local name server. A recursive resolution request tells the name server that the resolver expects a complete answer to the query, not just a pointer to another name server. Recursive resolution effectively puts the workload onto the name server and allows the resolver to be small and simple.

- Iteration

  If the local name server cannot fully resolve the query, it enlists the aid of other DNS name servers throughout the DNS name space. A well-behaved local name server keeps the burden of processing on itself and passes only *iterative resolution* requests to other name servers. An iterative resolution request tells the name server that the requester expects the best answer the name server can provide without help from others. If the name server has the requested data, it returns it; otherwise it returns pointers to name servers that are more likely to have the answer. However, if a primary master name server is unable to resolve a request for data that should be in its zone, it returns an error to the requester.

- Caching

  As local name servers process recursive requests, they discover a lot of information about the DNS domain name space. To speed the performance of DNS and ease the burden on both the internetwork and the other name servers, local name servers temporarily keep this information in a local cache. Whenever a resolver request arrives, the local name server checks both its static information and the cache for an answer. Even if the answer is not cached, the identity of the name server for the zone might be, which reduces the number of iterative requests the name server has to process.

DNS and WINS Integration

The structure of a DNS zone changes whenever a new host is added or when an existing host is moved to a different subnet. Because DNS is not dynamic, someone must manually change the DNS database files if the zone is to reflect the new configuration. This results in increased administrative overhead, especially on zones that change frequently.

WINS, on the other hand, was created to ease this type of administrative burden. Coupling DNS with WINS capitalizes on the strengths of each to provide a form of *Dynamic DNS*. This coupling is supported by the DNS service that runs under Windows NT Server 4.0. With it, you can direct DNS to query WINS for name resolution of the lower levels of the DNS tree in your zones. All of this is transparent to the DNS resolvers, which perceive the DNS name server as handling the entire process. Figure 3-12 illustrates how name resolution works when WINS is integrated with DNS.

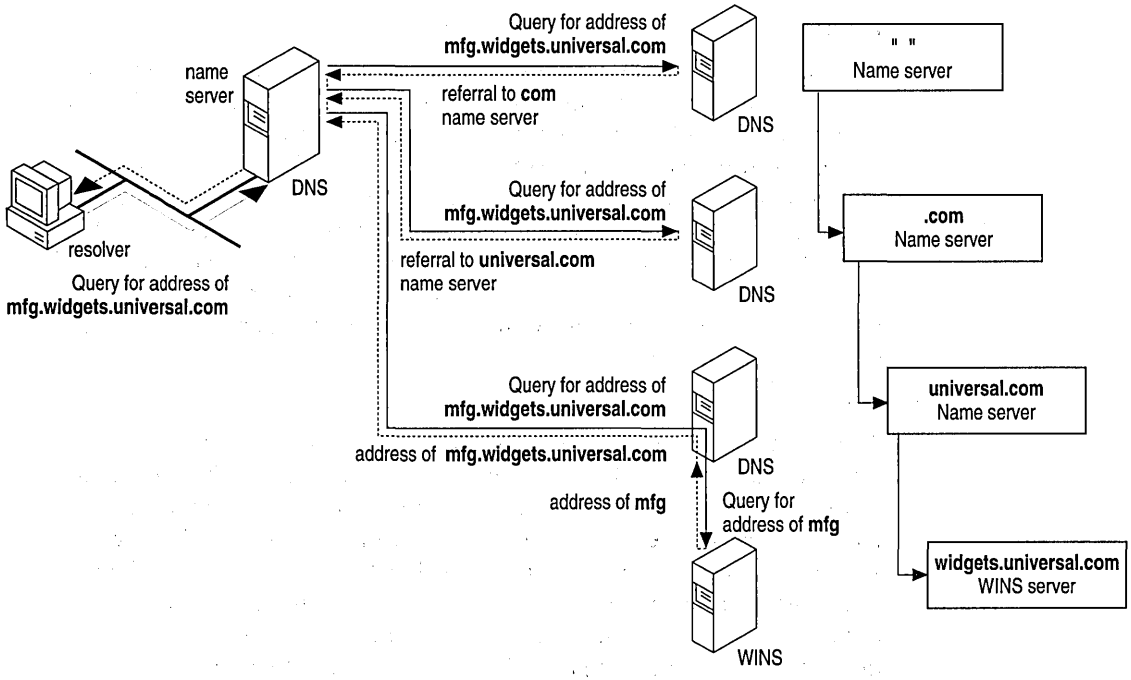


Figure 3-12 DNS Name Resolution Integrated with WINS

Suppose a user at a client workstation issues the following command:

```
net use \\mfg.widgets.universal.com.\public
```

This command establishes a connection between the client workstation and the *public* folder on the *mfg.widgets.universal.com.* server. However, before this connection can be established, the FQDN *mfg.widgets.universal.com.* must be resolved by DNS—and, in this case, WINS—into an IP address. The process, assuming no cached data on the name servers, is as follows:

1. The DNS resolver on the client sends a recursive request to the local DNS name server to resolve the FQDN.
2. The local DNS name server sends an iterative request to one of the DNS root servers requesting resolution of the FQDN. The DNS root servers are authoritative for the top-level DNS domains, such as *com*.
3. The DNS root server returns a referral to the name servers that are authoritative for the *universal* DNS domain.
4. The local DNS name server sends an iterative request to one of the *universal* name servers.
5. The *universal* name server responds with a referral to the *widgets* name servers.
6. The local DNS name server sends an iterative request to one of the *widgets* name servers.
7. The *widgets* name servers are running the DNS server on Windows NT Server and are configured to use WINS to resolve the leftmost portion (host name) of the FQDN. When the *widgets* name server receives the request from the local name server, it passes the *mfg* piece of the DNS name to its local WINS server for resolution. WINS returns the IP address for *mfg* to the *widgets* name server.
8. The *widgets* name server returns the IP address for the FQDN to the local DNS name server. The local DNS name server has no knowledge that WINS was involved in the name resolution process.
9. The local DNS name server completes the recursive request by sending the IP address back to the client resolver. Likewise, the client resolver is completely unaware of the WINS involvement in the process.
10. The client workstation establishes the session with *mfg.widgets.universal.com* and connects to the *public* folder.

Note DNS caching significantly reduces the number of iterative requests processed by name servers throughout the DNS name space.

In this example, only the *widgets* name server had knowledge of WINS. To the client resolver and all other name servers, it appeared that DNS was responsible for the entire nameresolution process. Furthermore, if the IP address changes for *mfg.widgets.universal.com.*, WINS will automatically handle it. Nothing needs to change with DNS.

For more information about integrating WINS with DNS, see the *Microsoft Windows NT Resource Kit Networking Guide*. For information about installing and configuring DNS and WINS Servers, see Windows NT Help.

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 name-resolution method was 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.

Note Sample versions of LMHOSTS and HOSTS files are added to the Windows NT *\systemroot*\SYSTEM32\DRIVERS\ETC directory when you install Microsoft TCP/IP.

HOSTS

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 mfg1.widgets.com looks like this:

```
192.102.73.6     mfg1.widgets.com
```

Edit the sample HOSTS file (created when you install TCP/IP) to include remote host names and IP addresses for each computer with which you will communicate.

LMHOSTS

The LMHOSTS file is a local text file that maps IP addresses to NetBIOS computer names. It contains entries for Windows-networking computers located outside the local subnet. The LMHOSTS file is read when WINS or broadcast name resolution fails; resolved entries are stored in a local cache for later access.

For example, the LMHOSTS table file entry for a computer with an address of 192.45.36.5 and a computer name of mrp2 looks like this:

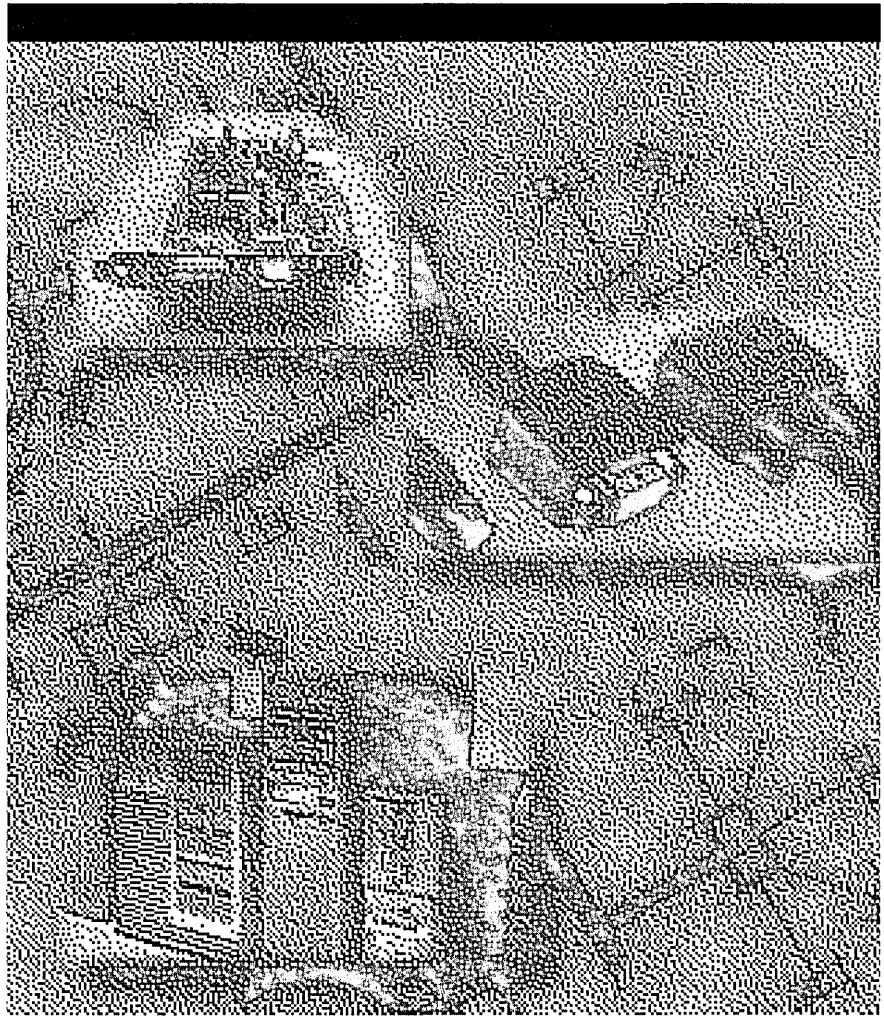
```
192.45.36.5      mrp2
```

Edit the sample LMHOSTS file (created when you install TCP/IP) to include remote NetBIOS names and IP addresses for each computer with which you will communicate.

The LMHOSTS file is typically used for small-scale networks that do not have servers. For more information about the LMHOSTS file, see Windows NT Help and the *Microsoft Windows NT Resource Kit Networking Guide*.

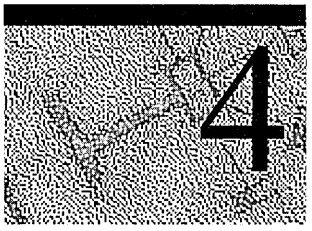
PART 2

Routing in Windows NT



CHAPTER 4

Routing in Windows NT

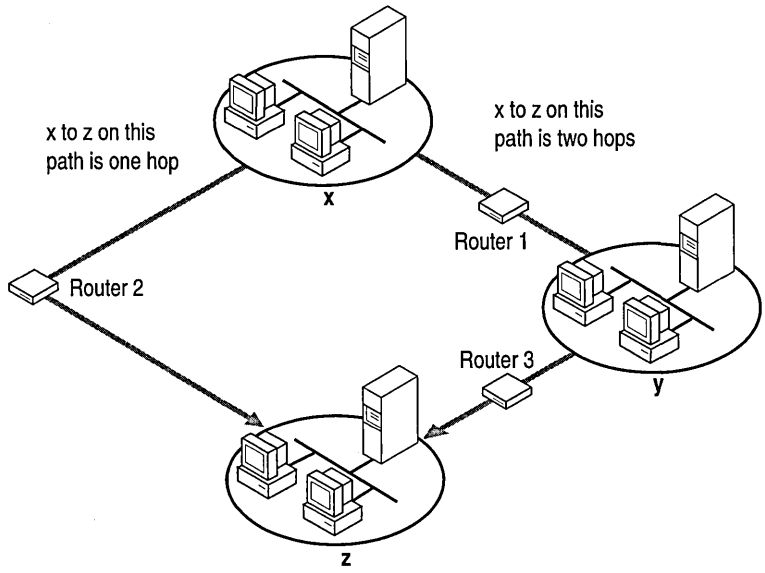


A Microsoft Windows NT Server includes Windows NT Server Multi-Protocol Routing support which enables routing over IP and IPX networks by connecting local area networks (LANs) or by connecting local area networks to wide area networks (WANs) without needing to purchase a dedicated router.

Note Windows NT also enables routing over AppleTalk networks. AppleTalk routing is part of Windows NT Services for Macintosh (SFM) which has its own separate planning and setup procedures in Chapter 17, "Planning Your AppleTalk Network." The AppleTalk section in this chapter covers basic routing information only.

Overview

A *router* helps LANs and WANs achieve interoperability and connectivity and can link LANs that have different network topologies (such as Ethernet and Token Ring). Each packet sent over a LAN has a *packet header* that contains source and destination address fields. Routers match packet headers to a LAN segment and choose the best path for the packet, optimizing network performance. For instance, for a packet to go from Computer x to Computer z in the following illustration, the best route uses only one hop. If Router 1 is the default router for x, the packet will be rerouted through Router 2 and Computer x will be notified of the better route to use to get to Computer z.



Routers choose the best path for packets to travel

See the online glossary Help file for a brief overview of other types of common LAN connection devices: repeaters, bridges, routers, and gateways.

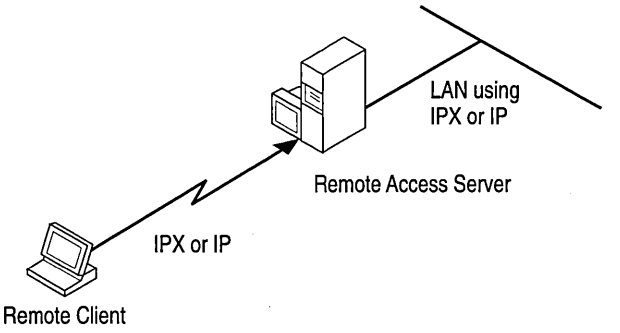
Windows NT Server Multi-Protocol Routing

After you install Windows NT Server Multi-Protocol Routing and enable the Routing Information Protocol (RIP) routing options, your Windows NT Server computer should be able to route network packets between two or more network adapters by using RIP on Internet Protocol (IP), Internetwork Packet Exchange (IPX), or both. Your computer can also be a DHCP Relay Agent (depending on your configuration) which allows a computer to relay DHCP messages across an IP network.

Note Windows NT Server Multi-Protocol Routing is intended for use by system administrators already familiar with routing protocols and routing services. This document provides installation instructions and a brief overview on routing and assumes that the reader has a basic understanding of routing and dynamic routing protocols. For more information on routing in general and dynamic routing protocols, consult a TCP/IP or IPX protocol-related book.

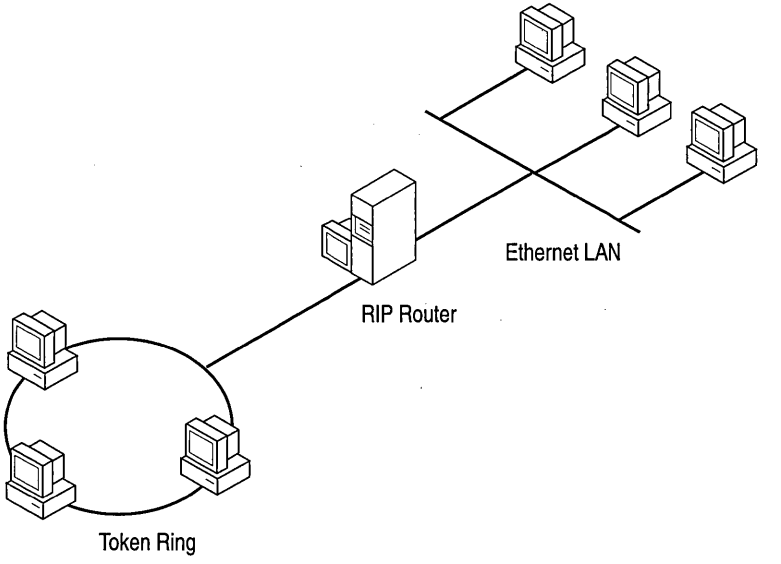
Routing Capabilities

In Windows NT Server, you can use a RAS server as a route between a remote client and a LAN, as shown in the following figure:



Routing between a remote client and a LAN

In Windows NT Server, you can also route between two LANs, as shown in the following figure:



Routing between two LANs

It is not possible to route between WANs over switched circuits or dial-up lines. The only exception to this rule is a WAN card (for example, T1 or Frame Relay) that appears to the router as a LAN card.

Understanding the Routing Information Protocol

The *Routing Information Protocol* (RIP) facilitates the exchange of routing information. A *RIP router* is a computer or other piece of hardware that broadcasts routing information (such as network addresses) and forwards IP frames on connected networks.

RIP allows a router to exchange routing information with neighboring routers. As a router becomes aware of any change in the internetwork layout (for instance, a downed router), it broadcasts the information to neighboring routers. Routers also send periodic RIP broadcast packets containing all routing information known to the router. These broadcasts keep all internetwork routers synchronized.

For more information about the RIP, see the public specification RFC 1058.

Note For details on retrieving RFCs by means of FTP or email, send an email message to "rfc-info@ISI.EDU" with the subject "getting rfcs" and the message body "help:ways_to_get_rfcs."

RFCs can be obtained by means of FTP from NIS.NSF.NET, NISC.JVNC.NET, VENERA.ISI.EDU, WUARCHIVE.WUSTL.EDU, SRC.DOC.IC.AC.UK, FTP.CONCERT.NET, DS.INTERNIC.NET, or NIC.DDN.MIL. You can also find RFCs at http://ds.internic.net.

Installing the DHCP Relay Agent

The DHCP Relay Agent allows a computer to relay DHCP messages from one LAN to another. For example, suppose a network has two LANs (LAN A and LAN B) with a router between them but only one Dynamic Host Configuration Protocol (DHCP) server on LAN A. In a traditional scenario, for LAN B clients to get addressing information, a DHCP server would be required on both networks (resulting in higher maintenance and cost). Instead, install a DHCP Relay Agent on any computer in LAN B, and it will relay messages through the router to the DHCP server on LAN A.

For more information about the DHCP Relay Agent, see the public specification RFC 1542.

▷ To install the DHCP Relay Agent

1. Using the Network icon in Control Panel, in the **Services** tab, click **Add**, and then select **DHCP Relay Agent**. When prompted for the source file location, enter the drive letter where the installation files are located (for example, A:\I386).

In the **IP Address** tab of the **TCP/IP Properties** dialog box, specify the IP address of the DHCP server.

When installing the DHCP Relay Agent, choose the default configuration, and then click **OK** in the **Configuration** dialog box.

The DHCP Relay Agent is installed as a service and is enabled automatically.

2. To change default values for the DHCP Relay Agent (Maximum Hops, Seconds Threshold, or list of DHCP Server addresses), choose the **DHCP Relay** tab in the **TCP/IP Properties** dialog box.
3. In the **Network** dialog box, click **OK**, and then restart the computer when prompted.

Installing LAN-to-LAN Routing

To enable routing on your Windows NT Server computer, install LAN-to-LAN routing support. Your Windows NT Server computer must have at least two network adapters to install LAN-to-LAN routing. For more information on enabling LAN-to-LAN routing, see the sections titled "Enabling IP Routing" and "Enabling IPX Routing."

Depending on your network, you can install LAN-to-LAN routing support for IP or IPX. Before installing LAN-to-LAN routing, ensure that the selected protocol (IP or IPX) is already installed on the Windows NT Server computer. Use the Network icon in Control Panel to install the IP or IPX protocol.

▷ **To install LAN-to-LAN routing on a Windows NT Server computer**

1. Using the Network icon in Control Panel, in the **Services** tab, click **Add**, and then select **RIP for Internet Protocol** or **RIP for NWLink IPX/SPX Compatible Transport** in the **Network Software** box. When prompted for the source file location, enter the drive letter where the installation files are located (for example, A:\I386).

   When installing RIP for NWLink IPX, Setup displays a message that NetBIOS Broadcast Propagation (broadcast of type 20 packets) is currently disabled. If you are using NetBIOS over IPX, click **Yes** to enable broadcasts of type 20 packets.

2. After installing RIP routing for IPX, you must enable it by configuring the IPX protocol. For instructions on how to do so, see "Enabling IPX Routing," later in this chapter.

   RIP for IP is installed as a service and is enabled automatically.

3. In the **Network** dialog box, click **OK**, and then restart the computer when prompted.

Note To remove the RIP service, choose RIP for IP or IPX in the **Services** tab and then click **Remove**. Because this deletes the files from your computer, you must reinstall before you can use the RIP service again.

IP Routing

Windows NT Server supports RIP for dynamic management of Internet Protocol (IP) routing tables. RIP eliminates the need to establish static IP routing tables. This version of RIP routing does not support RIP over dial-up (switched WAN) links.

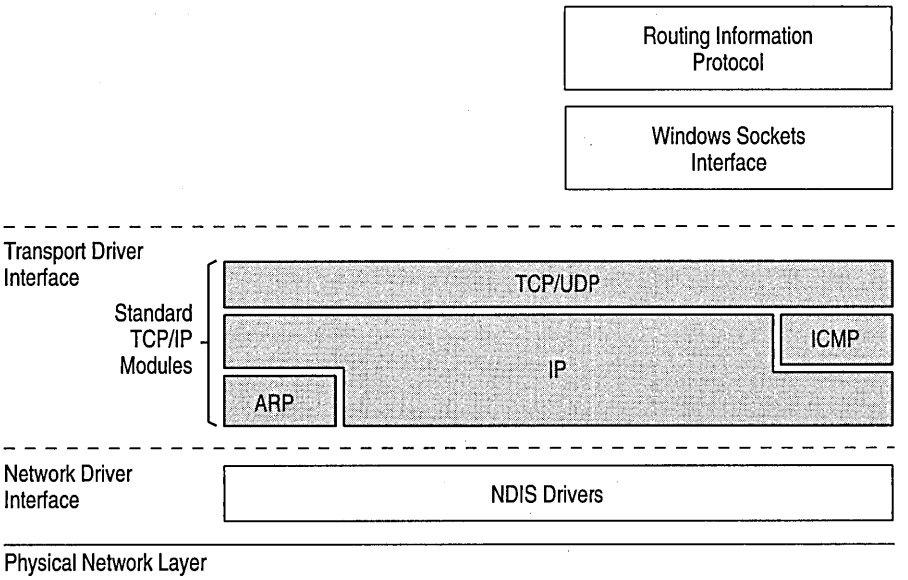
If RIP for IP is installed on a computer that has only one network card, the computer will be placed in *Silent Mode*. In Silent Mode, the computer listens to RIP broadcasts and updates its route table but does not advertise its own routes. If an additional network card is installed later and you want RIP to broadcast, you must change the SilentRip parameter in the Registry to *0*.

Silent Mode might be used on a computer between two disjoint networks (that is, networks that are not connected to each other), such as a computer connected to both a network and the Internet. The computer receives routes from both networks and adds them to its routing table using RIP. When sending a packet to a remote destination, the computer knows exactly how to route it based on its routing table.

RIP for IP is installed as a Windows NT Server service through Control Panel, and is therefore configured through the Services icon in Control Panel. By default, the RIP service starts automatically when the computer starts.

RIP for IP requires the Microsoft TCP/IP protocol family: Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP). The following figure illustrates the relationship between RIP and these three main protocols.

For more information about TCP or UDP, see the TCP/IP part in the *Networking Supplement.*



IP and RIP architectural model

IP datagrams, the basic IP information units, are sent directly from one host to another if the destination host is on the same network. If the destination host is on a different network, the datagram is sent to a router on the local network, which forwards it toward its destination.

If the destination host is not directly connected to the LAN that the router connects to, the router looks up the IP address of the next router in its routing table that lies along the path to the ultimate destination. The router then passes the datagram on to the next router. This continues until the ultimate destination router is reached and the datagram is sent to the destination host.

In this implementation of RIP routing over IP, routing over dial-up (switched WAN) links is not supported. For more information on static IP routing over dial-up lines, see "Installing a Simple Dial-up Router," later in this section.

Enabling IP Routing

Installing RIP for IP provides dynamic routing. When you install RIP for IP, the RIP routing service is automatically enabled and the **Enable IP Routing** option in the **Advanced TCP/IP Configuration** dialog box is automatically checked: No manual configuration is necessary. RIP for IP runs as a service and can be stopped and started through the Services icon in Control Panel. If you want static routing only, see the following section, "Enabling Static Routing."

Note IP permits two kinds of routing: *static* and *dynamic*. Static routing limits you to fixed routing tables. Dynamic routing automatically updates the routing tables, reducing administrative overhead (but increasing traffic in large networks).

▷ **To Enable Static Routing**

1. Choose the Network icon in Control Panel.
2. If you have installed RIP for IP, you must remove it to enable static routing. In the **Services** tab, choose **RIP for IP** from the Network Services list, and then click **Remove.**
3. In the **Protocols** tab, select **TCP/IP Protocol**, and then click **Properties.**
4. In the **Routing** tab, select the **Enable IP Forwarding** check box, and then click **OK.**

   This option is not available if your computer has only one network adapter and one IP address.

You might need to make additional static routing entries. For information about creating static routing tables, see the following section "Managing an IP Router."

Managing an IP Router

You can use the **route** utility to configure static routing tables.

- At the command prompt, type **route** with the appropriate options:

route [**-f**] [**-p**] [*command* [*destination*] [**MASK** *netmask*] [*gateway*] [**METRIC** *metric*]]

The following options are available:

-f

Clears the routing tables of all gateway entries. If this parameter is used in conjunction with a command, the tables are cleared before the command is run..

-p

Enables persistent routes. (Routing table changes are carried over automatically after restarting your computer.)

command
One of the following commands:

Command	Purpose
print	Prints a route
add	Adds a route
delete	Deletes a route
change	Modifies an existing route

destination
The host or network to which you want to route.

MASK
Specifies that the next parameter be interpreted as the *netmask* parameter.

netmask
The subnet mask value to be associated with this route entry. If not present, this parameter defaults to 255.255.255.255.

gateway
The gateway to the destination.

METRIC
Specifies that the next parameter be interpreted as the *metric* parameter.

metric
Associates a cost/hop count for the destination specified by the route entry. Generally, this specifies the distance in number of hops from the destination. If not specified, the metric is set to 1 by default.

The **route** utility does not accept a subnet mask value of 255.255.255.255 on the command line. To specify a subnet mask with this value, you must accept the default.

The **route** utility can use the NETWORKS file to convert destination names to addresses. For the **route** utility to work correctly, the network numbers in the NETWORKS file must specify all four octets in dotted decimal notation. For example, a network number of 184.122.107 must be specified in the NETWORKS file as 184.122.107.0, with trailing zeroes appended.

The gateway must be on the same logical network that your computer is on. Otherwise, the route will not be added.

Default Gateways In TCP/IP configuration, you can add default gateways for each network card. On a computer on which multiple default gateways are defined, all remote network traffic that does not match an entry in the route table is passed over the first default gateway defined. Since only one default gateway is used, you should configure only one card to have a default gateway. This reduces confusion and ensures the results you intended. If you add a second gateway to the same network, the entry is added to the route table and is used if the first gateway goes down.

Example of Adding a Static Route

At the command prompt, type

route add 199.199.41.0 **mask** 255.255.255.0 199.199.40.1 **metric** 2

This route means that to get to the 199.199.41.0 subnet with a mask of 255.255.255.0, use gateway 199.199.40.1. The address 199.199.41.0 is two hops away.

A static route will also need to be added on the next router telling it how to get back to subnets that can be reached by the first router. With a network of a few routers or more, static routes can become very complicated.

Troubleshooting IP RIP

This section describes the various TCP/IP utilities that help determine whether RIP for IP is running correctly.

For more information, see Command Reference in Help.

ARP -a Shows the mapping of IP addresses to hardware addresses. This is useful for tracking down duplicate IP addresses.

IPCONFIG or WINIPCFG Verifies the correct configuration for the client, including IP address, subnet mask, and default gateway.

NBTSTAT -A XXX.XXX.XXX.XXX shows the NetBIOS name cache on a remote computer. Helpful not only for NetBIOS name resolution problems, it also helps you track down the computer name after a duplicate address is found. If there is no response to **NBTSTAT -A,** the computer might be a router, or a computer without NetBIOS over TCP/IP (i.e. a non Microsoft computer.)

Note If you have multiple network cards, **NBTSTAT -A** runs over the first card in the binding list.

PING Verifies connections to one or more remote hosts.

Ping your computer (by address not hostname to determine that TCP is functioning. (Ping does not verify that your network card is functioning.)

Ping your default gateway or next hop router. This shows that the router is up.

Ping beyond the next hop router. A failed response such as "Request timed out" can mean that the destination host is down or that there is no route back to you. A failed response such as "Destination Unreachable" shows the IP address of the router that tried to route the packet but did not have a valid route.

Some useful ping options:

- **-n** *count*
- **-l** *size*
- **-f**

ROUTE PRINT Prints the routing table. Subnet or network routes with a metric of 2 or greater are learned by RIP. (Note that a RAS client will also make a metric of 2 when the RAS connection is up.)

Use this command to see if the route table makes sense for the situation. You should see routes for other networks or subnets in your autonomous system. If the route table contains no routes with the metric of 2,verify that RIP for IP is running by checking the Services icon in Control Panel.

Check to see if the default gateway is correct on the Windows NT router. You should use only one default gateway configured on the appropriate network card. Remember that the default gateway route is used only if no other valid route to the destination is available. Therefore, the default route will only be used for addresses outside of your company or autonomous system. All routes in the company will be learned by RIP.

TRACERT Shows the path of routers a packet used to get to its destination.

Reading Route Tables

Every computer that runs TCP/IP makes routing decisions. Such decisions are controlled by the *route table*. To display the route table, type **route print** at the command prompt. The following route table is an example from a computer with one netcard and is built automatically by Windows NT based on the IP configuration of your computer. A description of each column follows the table.

Network Address	Netmask	Gateway Address	Interface	Metric
0.0.0.0 (default route)	0.0.0.0	10.57.8.1	10.57.11.169	1
127.0.0.0 (loopback address)	255.0.0.0	127.0.0.1	127.0.0.1	1
10.57.8.0 (local subnet address)	255.255.248.0	10.57.11.169	10.57.11.169	1
10.57.11.169 (network card address)	255.255.255.255	127.0.0.1	127.0.0.1	1
10.57.255.255 (subnet broadcast address)	255.255.255.255	10.57.11.169	10.57.11.169	1
224.0.0.0 (multicast address)	224.0.0.0	10.57.11.169	10.57.11.169	1
255.255.255.255 (limited broadcast address)	255.255.255.255	157.57.11.169	157.57.11.169	1

Network Address The network address is the destination. The search order is from unique routes to general routes. The network address and netmask work together to determine the search order. The network address specifies a destination (such as a host or a network address), and the netmask specifies which part of the network address must match (such as the first byte only or all four bytes).

The network address column can contain

- Host address
- Subnet address
- Network address
- Default gateway

Netmask Defines what portion of the network address must match for the route to be used. When the mask is written in binary a "1" must match and a "0" need not match. For example, a 255.255.255.255 mask is used for a host entry. The mask of all 255s (all 1s) indicates that the destination address of the packet to be routed must exactly match the network address for this route to be used.

In another example, the network address 10.57.8.0 has a netmask of 255.255.248.0. This netmask indicates that the first two octets must match exactly, the first 5 bits of the third octet must match (248=11111000), and that the last octet does not matter. Since the third octet, 8, equals 00001000 then a match would have to start with 00001. Thus any address of 157.57 and the third octet of 8 through 15 (15=00001111) will use this route. Because this is a netmask for a subnet route, it is called the *subnet mask.*

Gateway Address Where the packet needs to be sent. This can be the local network card or a gateway (router) on the local subnet.

Interface The network card on which the packet should be sent out.

Metric The number of hops to the destination. Anything on the local LAN is one hop, and each router crossed after that is an additional hop. The metric determines the best route.

Registry Parameters for IP RIP

This section presents configuration parameters that affect the behavior of RIP routing for IP. They can be modified only through Registry Editor.

Registry parameters for IP RIP are specified under the following key:

```
..SYSTEM\CurrentControlSet\Services\IpRip\Parameters
```

▷ **To make changes using Registry Editor**

1. Start the Registry Editor by running the REGEDT32.EXE file from the **Run** command on the Start menu.

   –Or–

   At the command prompt, type the **start regedt32** command, and then 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.

AcceptDefaultRoutes

Data type = REG_DWORDRange = 0 or 1Default = 0

If set to 1, default routes in received RIP announcements are accepted. By default, they are ignored.

AcceptHostRoutes

Data type = REG_DWORDRange = 0 or 1Default = 0

If set to 1, host routes in received RIP announcements are accepted. By default, they are ignored.

AnnounceDefaultRoutes

Data type = REG_DWORDRange = 0 or 1Default = 0

If set to 1, default routes are included in RIP announcements.

AnnounceHostRoutes

Data type = REG_DWORDRange = 0 or 1Default = 0

If set to 1, host routes are included in RIP announcements.

EnablePoisonedReverse

Data type = REG_DWORDRange = 0 or 1Default = 1

By default, routes learned through an interface will be announced having a metric of 16 on the interface.

EnableSplitHorizon

Data type = REG_DWORDRange = 0 or 1Default = 1

By default, routes learned on a network are suppressed in updates sent on that network. If the parameter is set to 0, routes learned on a network are announced on the same network, as well.

EnableTriggeredUpdates

Data type = REG_DWORDRange = 0 or 1Default = 1

By default, new routes and metric changes trigger an immediate update which includes only the changes. This is called a *triggered update*. The time between updates depends on the value of MaxTriggeredUpdateFrequency.

GarbageTimeout

Data type = REG_DWORDRange = 15 seconds - 259200 seconds (72 hours)Default = 120 seconds

The number of seconds to wait before removing old, inactive routes.

LoggingLevel

Data type = REG_DWORDRange = 0 - 3Default = 1

The minimum level of information for entries being made to the system log: 0 = no logging, 1 = errors, 2 = warnings, 3 = information.

MaxTriggeredUpdateFrequency

Data type = REG_DWORDRange = 1 second - 884400 seconds (24 hours)Default = 5 seconds

The minimum number of seconds that must elapse between triggered updates.

RouteTimeout

Data type = REG_DWORDRange = 15 seconds - 259200 seconds (72 hours)Default = 180 seconds

The number of seconds to wait before marking a route for garbage collection.

SilentRip

Data type = REG_DWORDRange = 0 or 1Default = 0

If set to 1, suppresses periodic RIP announcements. This is used when the computer is in Silent Mode. For more information see the "IP Routing" section.

UpdateFrequency

Data type = REG_DWORDRange = 15 seconds - 884400 seconds (24 hours)Default = 30 seconds

The number of seconds between periodic updates which contain the entire routing table.

Installing a Simple Dial-up Router

Windows NT RAS version 3.5 or later was not designed to route packets from a large LAN over a dial-up link. However, by correctly configuring both the RAS computer acting as a router and the other computers on your small LAN with a static network configuration, you can use the computer running Windows NT RAS as a simple router to the Internet or to an enterprise TCP/IP network.

Note Your LAN must be small and not require the automatic routing configuration provided by RIP. (You probably do not need RIP functionality if you have a small LAN that is not expected to grow or change.)

The following requirements are necessary for using Windows NT RAS as a dial-up router between your LAN and the Internet:

- A Windows NT computer with a high-speed modem or ISDN line and a network adapter card
- A *Point-to-Point Protocol (PPP)* connection to the Internet or enterprise TCP/IP network
- A valid network or a subnet, different from the subnet of the Internet service provider
- The proper Registry and Default Gateway configurations on the computer acting as a router and the LAN clients. The configurations are described later in this section.

To be identified using names rather than IP addresses, you also need a domain name. Your Internet service provider can help you obtain a domain name.

After you have a PPP connection, IP addresses for your subnet (and correct subnet mask), and (optionally) a domain name, you can configure the RAS and LAN computers for Internet gateway.

▶ To configure a small LAN for routing to the Internet over a PPP account

1. On the RAS computer acting as a router to the Internet, add the value **DisableOtherSrcPackets** to the following Registry path, and then set the value to 0.

   ```
   \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
       \RasArp\Parameters
   ```

   DisableOtherSrcPackets **REG_DWORD**
   Range: 0-1Default: 1 (not in Registry)

   By default, the header of each packet sent by the RAS computer over the PPP link uses the IP address of the RAS computer as the source. Since the packets that come from LAN clients are not originating from the RAS computer, you must set **DisableOtherSrcPacket** to 0 so that the packets will be forwarded over the PPP link.

2. If your subnet is on the same logical IP subnet as your service provider (which is likely in this scenario), you must also add the value **PriorityBasedOnSubNetwork** to the Registry of the RAS computer that routes packets from the LAN to the Internet, and then set this parameter to 1.

   A computer can connect to the LAN by using a network card and a RAS connection. If the RAS connection and the LAN network adapter card are assigned addresses with the same network number, and if the **Use Default Gateway On Remote Network** check box is selected, then all packets are sent over the RAS connection, even though the two addresses are in different subnetworks within the same network.

   For example, if the network adapter card has IP address 17.1.1.1 (subnet mask 255.255.0.0) and the RAS connection is assigned the address 17.2.1.1, RAS sends all 17.x.x.x packets using the RAS connection. If the parameter is set, RAS sends 17.2.x.x packets using the RAS connection and 17.1.x.x packets using the network adapter card.

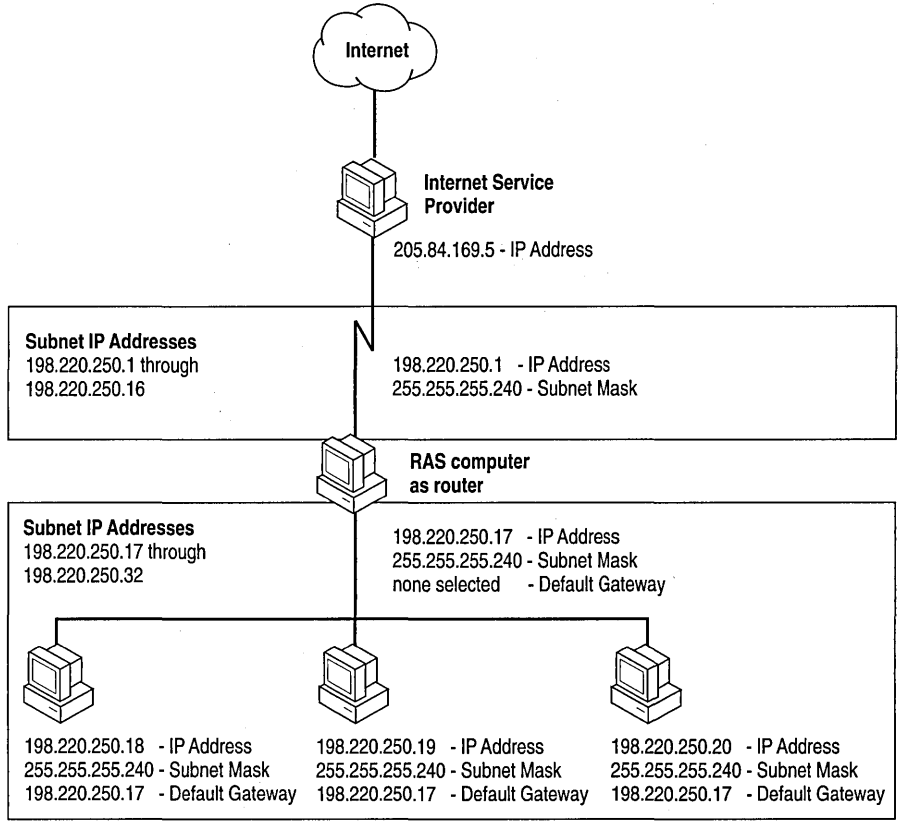
   ```
   \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
       \RasMan\PPP\IPCP
   ```

   PriorityBasedOnSubNetwork **REG_DWORD**
   Range: 0-1Default: 0 (not in registry)

3. Configure the default gateway of all the computers on the LAN using the Network icon in Control Panel.

The default gateway is set when you configure the TCP/IP protocol.

The default gateway for all computers on the LAN should be the IP address of the network card in the RAS computer acting as a router to the Internet. The default gateway for the computer acting as the router to the Internet should be left blank. The following figure can help you determine the correct assignment pattern of IP addresses, subnet masks, and default gateways.



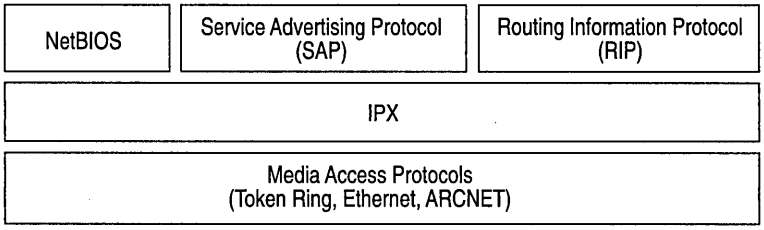
Sample configuration using RAS as a Simple Internet Router

IPX Routing

The implementation of IPX by Windows NT Server (NWLink IPX/SPX Compatible Protocol [NWLink]) conforms to the Novell® IPX Router Specification.

IPX Routing Protocol

Routers interconnect different network segments and, by definition, are *network layer devices*. In other words, routers receive their instructions for forwarding a packet from one segment to another from a network layer protocol. IPX, with the help of the RIP and the SAP, performs these network layer tasks. These tasks include addressing, routing, and forwarding from one location to another on an internetwork. The following figure shows how these protocols are related.



IPX Protocol Model

Features and Limitations

This version of IPX internal routing for Windows NT supports LAN-to-LAN routing (sending datagrams from one network segment to another based on routing information)and forwarding type 20 packet broadcasts, including NetBIOS over IPX packets propagation.

When you enable IPX routing, you can choose whether or not to enable type 20 broadcast propagation. If this option is selected, the Windows NT Server computer can use NetBIOS over IPX for browsing and name resolution.

Note Type 20 packets will only propagate up to 8 hops away from the original sender. This means that on a large network—if the receiving computer is more than 8 hops away from the sender—it will not receive this packet.

If you disable type 20 broadcasts, and IPX is the only protocol installed on this server and on clients connect to this server, then the clients cannot communicate with servers on other networks.

IPX provides the addressing mechanism that allows packets to be delivered to a desired destination. RIP and SAP enable routers to gather internetwork information and share that information with other routers. The RIP and SAP agents combine to make an IPX router, although SAP is not necessary in all cases. You need to install the SAP agent only if services running on your network (such as NetWare-compatible file servers or SQL servers) use SAP.

This version of IPX internal routing does not have filtering capability. Therefore, all entries in the RIP and SAP tables are propagated. On large networks, the bandwidth required for forwarding RIP and SAP tables can be considerable. Internal routing is not supported over dial-up lines.

If you have a fixed synchronous line (for example, T1) with network drivers that emulate the LAN, then RIP and SAP tables will be forwarded over those lines. Note that in this case, bandwidth usage for large networks can be exorbitant. Another advanced third-party router might be best suited for this situation.

Enabling IPX Routing

To enable IPX routing, you must install the IPX protocol and RIP for IPX. The SAP agent is installed automatically when RIP for IPX is installed. Use the Networks icon in Control Panel to install this software on the computer you want to use as a router. You will need to restart the computer before your changes take effect. For more information on installing RIP for IPX, see "Installing LAN-to-LAN Routing."

▷ To enable IPX routing

1. Choose the Network icon in Control Panel.
2. In the **Protocols** tab, select NWLink IPX/SPX Compatible Transport, and then click **Properties**.
3. In the **Routing** tab, select the **Enable RIP Routing** check box, and then click **OK**.

   This step enables IPX routing over LANs.

Note This release does not provide LAN to WAN to LAN routing.

Troubleshooting IPX RIP

In addition to current source routing information, the **ipxroute** utility provides information on RIP, SAP, and statistics. Use the **ipxroute** utility to display and modify information about the source routing tables used by IPX.

Note All parameters should be separated by spaces. The **ipxroute** console utility can be used remotely by means of the **remote** utility in the Windows NT Resource Kit version 3.5 or later.

- At the command prompt, type **ipxroute** with the appropriate options.

ipxroute board=*n* **[clear] [def] [gbr] [mbr] [remove=***xxxxx***]**
ipxroute config
ipxroute table
ipxroute servers [/type=*xxx***]**
ipxroute stats [/show] [/clear]

The following options can be used:

board=*n*
Specifies the network adapter card for which to query or set parameters.

clear
Clears the source routing table.

def
Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to a unique *media access control (MAC)* address that is not in the source routing table, the default is to send the packet to the SINGLE ROUTES broadcast.

gbr
Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to the broadcast address (FFFF FFFF FFFF), the default is to send the packet to the SINGLE ROUTES broadcast.

mbr
Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to a multicast address (C000 xxxx xxxx), the default is to send the packet to the SINGLE ROUTES broadcast.

remove=*xxxxx*
Removes the given node address from the source routing table.

config
Displays information on all the bindings for which IPX is configured.

table
Displays the IPX routing table.

servers
Displays the SAP table.

/type=*xxx*
xxx refers to server type. The default is all server types.

stats
Displays or clears IPX internal routing statistics.

/show
Displays the internal routing table. This is the default option.

/clear
Clears the internal routing table.

Routing on AppleTalk Networks

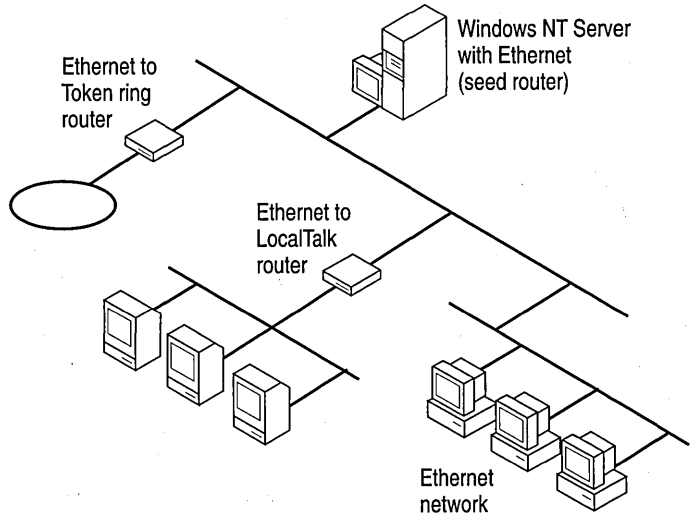
Because AppleTalk networks differ from PC networks, you must consider some special concepts and issues when you set up an AppleTalk network.

The first concept you need to understand is the *internet*. Note that this is a different concept than the Transport Control Protocol/Internet Protocol (TCP/IP) Internet. Most large AppleTalk networks are not single physical networks, in which all computers are attached to the same network cabling system. Instead, they are *internets*, which are multiple smaller physical networks connected by *routers*. Routers maintain a map of the physical networks on the internet and forward data received from one physical network to other physical networks. Routers are necessary so that computers on different physical networks can communicate with one another. They also reduce network traffic on the internet by isolating the physical networks. In other words, routers send only data that is usable by a network.

Some routers on the network are *seed routers*. A seed router initializes and broadcasts routing information about one or more physical networks. This information tells routers where to send each packet of data. Each physical network must have one or more seed routers that broadcast the routing information for that network.

Not all routers must be seed routers. Routers that are not seed routers maintain a map of the physical networks on the internet and forward data to the correct physical network. Seed routers perform these functions too, but they also initialize the routing information (such as network numbers and zone lists) for one or more physical networks.

A computer running Windows NT Server with Services for Macintosh can function as a seed router or as a nonseed router. If it is a seed router, it must be the first server you start so that it can initialize the other routers and nodes with network information. If it is a nonseed router, it cannot be started until a seed router has initialized all ports. You can also use dedicated hardware routers (such as those made by Cayman Systems®, Shiva®, Solana, Hayes®, and others) on your network.



Routing Information

Routing information includes:

- A network number or network range associated with each physical network.
- The zone name or zone list associated with each physical network.
- The default zone for the network (if the network has multiple zones)

The *network number* or *network range* is the address or range of addresses assigned to the network. A network number is unique and identifies a particular AppleTalk physical network. By keeping track of network numbers and network ranges, routers can send incoming data to the correct physical network. A network number can be any number from 1 through 65, 279.

LocalTalk networks can have only a single network number; EtherTalk, TokenTalk and FDDI networks can have network ranges.

A *zone* is a logical grouping, which simplifies browsing the network for resources, such as servers and printers. It is similar to a domain in Windows NT Server networking, as far as browsing is concerned. In LocalTalk networks, each physical network can be associated with only one zone. However, for EtherTalk, TokenTalk, or FDDI, you have more flexibility in assigning zones. Each EtherTalk, TokenTalk, or FDDI network can have one or more zones associated with it, and each zone can include servers and printers on one or more physical networks. This way, you can group servers and printers logically into zones so users can easily locate and access the servers and printers, no matter what physical networks they are on.

Each Macintosh client on the network is assigned to a single zone. However, each client can access servers and printers in any zone on the network. Zones make accessing network resources simpler for users. When users use the Chooser to view the network, they see only the resources in a single zone at a time, preventing them from having to navigate through huge numbers of resources on large networks to find the resources that they need. You can put the clients, servers, and printers used by a single group into a single zone, so users will see only the resources they typically use but will still be able to access resources in other zones when required.

A *zone list* includes all the zones associated with that network. One of these zones is the network's *default zone*, to which the Macintosh clients on that network are assigned by default. Users can configure the client to be in a different zone, however.

Working with Seed Routers

When you install Windows NT Server and set up Services for Macintosh, you must specify whether the Windows NT Server computer will seed each physical network to which it is attached. For example, a computer running Windows NT Server attached to three physical AppleTalk networks might serve as a seed router on two of the networks but not on the third.

For networks that the server will seed, specify the routing information. The Windows NT Server computer will then function as a seed router, seeding the routing information that you provided. If you specify that a server will not seed a network (that is, if you label it as a nonseed router), the port will be seeded by another AppleTalk router attached to it.

Using Multiple Seed Routers on a Network

To make your network more reliable in case of system crashes and power outages, install multiple seed routers on the same physical network.

When you install multiple seed routers for a particular network, all the seed routers must seed the same information for that network. When the network starts, the first seed router that starts on the network becomes the actual seed router.

When a network starts, if the first seed router to start has different routing information than seed routers that start later, the information established by the first seed router is used. If a seed router that starts subsequently with different information is a server running Windows NT Server, the conflicting information is ignored, an event is written to Windows NT Server Event Viewer, and the server ceases to be a seed router. Non-Microsoft routers might behave differently.

For more information on seed routers in a network, see Chapter 17, "Planning Your AppleTalk Network."

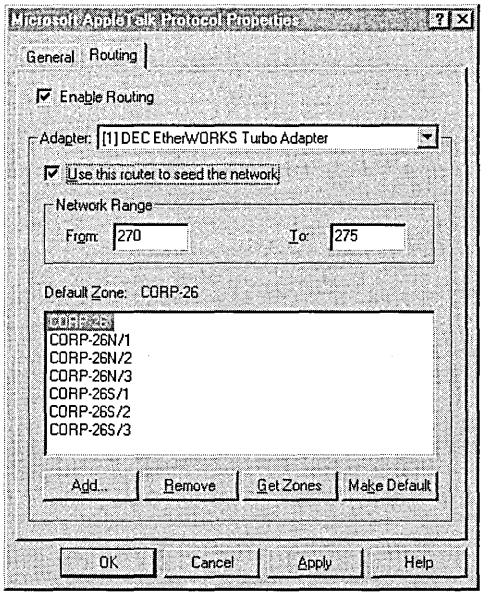
Configuring AppleTalk Routing

You must install Services for Macintosh (SFM) before you can configure AppleTalk Routing. For information on setting up SFM, see Chapter 18, "Setting Up Services for Macintosh."

If you enable routing, the computer running Windows NT Server becomes an AppleTalk router. This enables the computer running Windows NT Server to be seen from Macintoshes connected to all the bound networks. If the server has more than one network card and it is not a router, then the server can be used only from the Macintoshes connected to the default network (unless another router broadcasts the information for the other networks).

▷ To enable AppleTalk Routing

1. In Control Panel, choose the Network icon.
2. In the **Services** tab, choose **Services for Macintosh** and then click **Properties**.
3. In the **Routing** tab, select the **Enable Routing** check box.



Seeding the Network

In the Routing tab, the **Adapter** box shows a list of network cards that correspond to the networks the Windows NT Server computer is attached to. Seeding can be enabled on any or all of the networks. To seed a specific network, choose the corresponding adapter and then select the **Use This Router to Seed the Network** option.

Caution The seeding information must agree with all routing information on that network and internet. Otherwise, all routers on the internet could fail to function.

Selecting to seed the network makes the present state of the Zone List and the Network Range options available.

Setting the Network Range

Setting the network range is part of seeding a network. Each AppleTalk network in an internet is assigned a range of numbers, and each node is identified to the network by one of those numbers, which is combined with a dynamically assigned AppleTalk node identification number. Because of this, no two networks on an internet should have overlapping ranges.

The value you specify for a network must range from 1 through 65,279. If you specify a range that overlaps another network range on the computer running Windows NT Server, you'll see a warning message. For more information about ranges, refer to Chapter 17, "Planning Your AppleTalk Network."

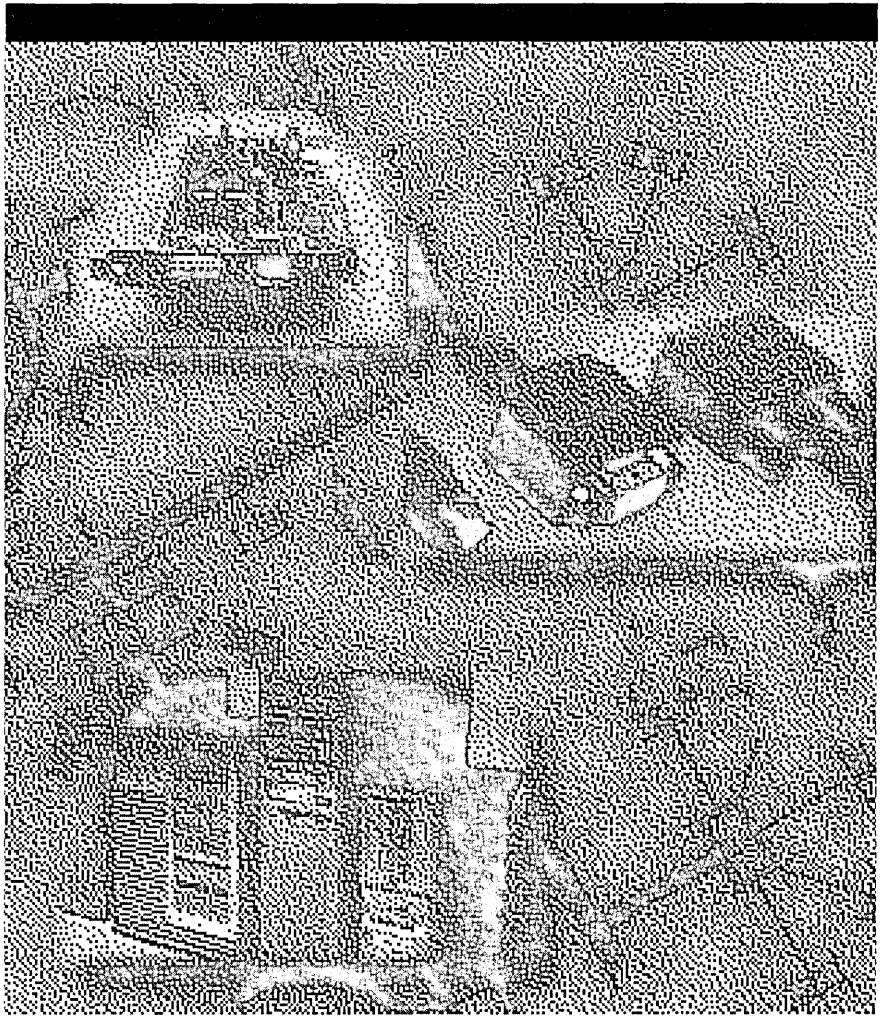
Setting Zone Information

Setting zone information is also part of seeding a network. You can see the current list of zones, add and remove zones, and set the default zone. The *default zone* is the zone in which all AppleTalk devices will appear if a desired zone has not been specified for the device.

For procedures and more information see the online Help.

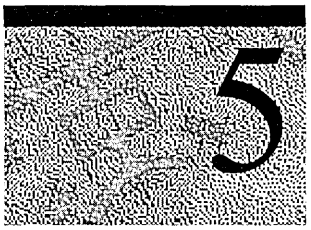
PART 3

Remote Access Service



CHAPTER 5

Understanding Remote Access Service



Windows NT Remote Access Service (RAS) connects remote or mobile workers to corporate networks. Windows NT RAS is a dial-up networking product and appears on the desktop as a Dial-Up Networking icon.

This chapter explains the basic operation of Windows NT RAS and how to implement Windows NT Server RAS in a Windows NT Server network. This includes

- Overview of the major components of RAS
- Remote access clients and servers
- Local-area network (LAN) protocols—TCP/IP, IPX, and NetBEUI
- Remote access protocols—Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), and Microsoft RAS protocol
- Wide-area network (WAN) options—telephone lines, ISDN, X.25, and PPTP
- Security features

For additional information about the Remote Access Service, see RAS online Help.

RAS Capabilities and Functionality

RAS allows remote users on the following systems to work as if they were connected directly to the network: Windows NT, Windows for Workgroups, MS-DOS version 3.1 or later (RAS version 1.1a), and MS OS/2 version 3.1 (RAS version 1.1).

Users run the RAS graphical phonebook on a remote computer and then initiate a connection to the RAS server using a local modem, X.25, or ISDN card. The RAS server, running on a Windows NT Server computer, authenticates the users and services the sessions until terminated by the user or network administrator. All services typically available to a LAN-connected user (including file- and print-sharing, database access and messaging) are enabled by means of the RAS connection. The following figure depicts the RAS architecture:

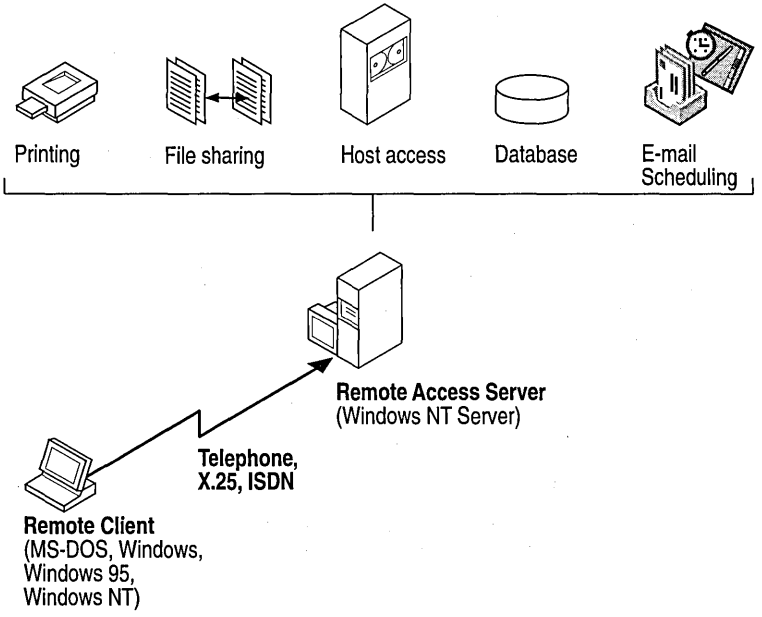


Figure 9.1 RAS Architecture

Note that remote clients use standard tools to access resources. For example, the Explorer is used to make drive connections and used to connect printers. Connections are persistent: Users do not need to re-connect to network resources during their remote sessions. Because drive letters and Universal Name Convention (UNC) names are fully supported in RAS, most commercial and custom applications work without modification.

Remote Access Versus Remote Control

The distinctions between RAS and remote control solutions (such as Cubix and pcANYWHERE) are important:

- RAS is a software-based multi-protocol router; remote control solutions work by sharing screen, keyboard and mouse over the remote link.
- In a remote control solution, users share a CPU or multiple CPUs on the server. The RAS server's CPU is dedicated to communications, not to running applications.

This architectural difference has significant implications in two areas: scalability and software applications architecture.

In the area of scalability, consider the problem of increasing the capacity or performance of a remote-control server. For best performance, an additional or upgraded CPU or computer would need to be purchased for every port to be added or upgraded. With RAS, additional ports can be added without upgrading the server computer. When it does require an upgrade, the RAS Server would generally get additional RAM, a less costly approach than with remote-control. With Windows NT, a single server can scale to support hundreds of remote users, using far fewer hardware resources than a remote control solution.

In software applications architecture, the RAS client normally executes applications from the remote workstation. Because network traffic is reduced, the user achieves higher performance. So the RAS arrangement is better suited to graphical, client-server–based applications. Contrast this with the remote control client, which runs applications from the host-side CPU. Remote control, however, can be useful in nonclient-server environments; for example when you are remotely debugging a computer and you want to see the current desktop of the remote computer.

Overview

A Windows NT RAS configuration includes the following components:

Remote access clients

Windows NT, Windows™ for Workgroups, MS-DOS, and LAN Manager RAS clients can all connect to a Windows NT RAS server. Clients can also be any non-Microsoft PPP client.

RAS servers

The Windows NT Server RAS permits up to 256 remote clients to dial in. The RAS server can be configured to provide access to an entire network or restrict access to the RAS server only.

LAN and Remote Access Protocols

LAN protocols transport packets across a local-area network (LAN), whereas remote access protocols control the transmission of data over the wide-area network (WAN).Windows NT supports LAN protocols such as TCP/IP, IPX, and NetBEUI, which enable access to the Internet and to NetWare and UNIX servers. Windows NT supports Remote Access Protocols such as PPP, SLIP on RAS clients, and the Microsoft RAS Protocol.

WAN options

Clients can dial in using standard telephone lines and a modem or modem pool. Faster links are possible using ISDN. You can also connect RAS clients to RAS servers using X.25, an RS-232C null modem, or using the new Point-to-Point Tunneling Protocol (PPTP).

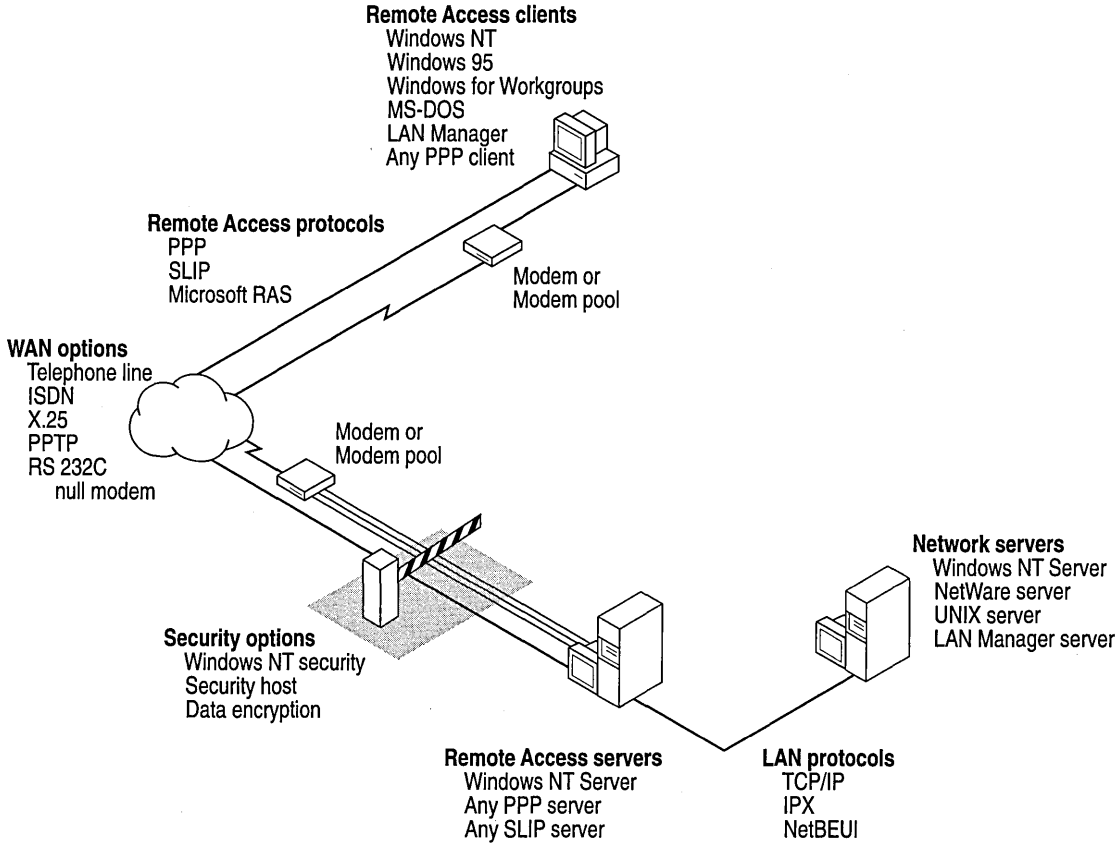
Internet Support

RAS enables Windows NT to provide complete services to the Internet. A Windows NT Server computer can be configured as an Internet service provider, offering dial-up Internet connections to a PPP client. A computer running Windows NT Workstation can dial into an Internet-connected computer running Windows NT Server 3.5 or later or to any one of a variety of industry-standard PPP or SLIP-based Internet servers. For more information see the *Windows NT Resource Kit Internet Guide.*

Security options

Windows NT logon and domain security, support for security hosts, data encryption, and callback provide secure network access for remote clients.

The following picture illustrates all RAS features and possible configurations. Actual implementations and configurations will vary and are discussed in this book.



Overview of Windows NT Server RAS

Remote Access Clients

Clients connecting to Windows NT RAS servers can be Windows NT, Windows 95, Microsoft Windows for Workgroups, MS-DOS, LAN Manager, or any PPP client. The client must have a modem (9600 baud or above is recommended for acceptable performance), an analog telephone line or other WAN connection, and remote access software installed.

Connecting is automatic with the new RAS AutoDial feature. AutoDial learns every connection made over the RAS link and automatically reconnects you when you access a resource for the second time. For more information, see the section on automatic dialing in Chapter 6, "Installing and Configuring Remote Access Server."

Connecting can also be automated for any Microsoft client with a simple batch file and the **rasdial** command or with a custom, RAS-aware application using the appropriate Application Programming Interface for RAS. You can also schedule automatic backups to or from remote computers by using RAS and the **at** command.

Windows NT Version 3.5, 3.51 and Windows 95 Clients

Windows NT version 3.5x and Windows 95 clients can take full advantage of Windows NT version 4.0 RAS features, except for Multilink functionality. Windows NT version 3.5x and Windows 95 clients can also connect to any non-Microsoft remote access PPP server or SLIP server.

Windows NT version 3.5x and Windows 95 clients negotiate logon and authentication with the server, whether the server is a Microsoft RAS server, a PPP server, or a SLIP server. You can also configure RAS phonebook entries to use scripts that can completely automate logon.

Windows NT Version 3.1 Clients

Windows NT version 3.1 clients use the Microsoft RAS protocol and are fully compatible with all versions of Microsoft RAS.

These clients do not support the PPP protocol introduced in Windows NT version 3.5. Only Windows NT version 3.5x or other PPP clients provide the support necessary to run TCP/IP or IPX applications on clients that directly communicate with servers on the LAN using TCP/IP or IPX.

Windows For Workgroups, MS-DOS, and LAN Manager Clients

Windows NT Server provides a Microsoft Network Client version 3.0 for MS-DOS and a Windows for Workgroups client that provide remote access. Separately purchased Windows for Workgroups and LAN Manager RAS clients can also connect to Windows NT version 3.5 or later RAS servers. These clients are fully (3.5x) compatible with all versions of Microsoft RAS protocol.

The Microsoft Network Client version 3.0 for MS-DOS must be set up to use the full redirector (the default setting.) If the basic redirector is used, the Remote Access program **rasphone** will not start.

The Windows for Workgroups, MS-DOS, and LAN Manager clients can use the RAS NetBIOS gateway to access NetBIOS servers running TCP/IP, IPX, or NetBEUI, but these clients cannot run applications that must use TCP/IP or IPX on the client.

These clients also do not support the PPP protocol introduced in Windows NT version 3.5.

PPP Clients

Non-Microsoft PPP clients using TCP/IP, IPX, or NetBEUI can access a Windows NT version 3.5 or later RAS server. The RAS server will automatically negotiate authentication with PPP clients; the Windows NT RAS software needs no special configuration for non-Microsoft PPP clients.

For more information about your PPP client, see the software documentation for your PPP client.

Remote Access Servers

Windows NT Server administrators use the Remote Access Admin program to control the Remote Access server, view users, grant permissions, and monitor Remote Access traffic. For more information about using the Remote Access Admin program, see RAS online Help.

The server must have a multiport adapter or modems (9600 baud or above is recommended for acceptable performance), analog telephone lines or other WAN connections, and the RAS software installed. If the server will provide access to the network, a separate network adapter card must be installed and connected for each network the server will provide access to.

RAS servers are configured during initial RAS setup. You must specify whether access will be to the entire network or to the RAS server only. You must also select the protocols to use on the LAN (IPX, TCP/IP, and NetBEUI) and an authentication encryption option. For more information about remote access protocols and LAN protocols, see those sections elsewhere in this chapter.

Ports on RAS servers are configured individually. Each port can be set to **Dial Out Only**, **Receive Calls Only**, or **Dial Out And Receive Calls**. These settings affect only the port specified, not all ports. For example, your RAS server can be configured to provide access to the entire network, COM1 can be configured to receive calls, and COM2 can be configured for dial out and receive. A remote user can call in on either COM port, but a local user can use only COM2 for outbound RAS calls.

Events and errors are recorded in Event Viewer on Windows NT RAS clients and servers. Evaluating the log in Event Viewer can help you determine the source of problems.

Use the **Control Panel Network** option to install and configure RAS. Use the **Control Panel Services** option to specify startup options.

The Windows NT Server RAS permits up to 256 remote clients to dial in. The RAS server can be configured to provide access to an entire network or restrict access to resources on the RAS server only.

For more information about installing and configuring RAS, see Chapter 6, "Installing and Configuring Remote Access Service."

Protocols

Windows NT supports LAN protocols such as TCP/IP, IPX, and NetBEUI, and Remote Access Protocols such as PPP, SLIP, and the Microsoft RAS Protocol. LAN protocols transport packets across a local-area network (LAN), whereas remote access protocols control the transmission of data over the wide-area network (WAN).

LAN Protocols

The protocol(s) used in the existing network affect how you plan, integrate, and configure RAS.

Windows NT RAS supports TCP/IP, IPX, and NetBEUI. This support means you can integrate Windows NT RAS into existing Microsoft, UNIX, or NetWare networks using the PPP remote access standard. Windows NT RAS clients can also connect to existing SLIP-based remote access servers (primarily UNIX servers).

When you install and configure RAS, any protocols already installed on the computer (TCP/IP, IPX, and NetBEUI) are automatically enabled for RAS on inbound and outbound calls.

You must also specify if you want to provide access to the entire LAN; otherwise, users will be able to access only the RAS server. If you provide access to the entire LAN using TCP/IP or IPX, you must also configure how the server will provide IP addresses or IPX net numbers. If you provide access to the entire LAN using NetBEUI, no additional configuration is needed.

TCP/IP and RAS

TCP/IP is one of the most popular protocols. Its routing capabilities provide maximum flexibility in an enterprise-wide network.

On a TCP/IP network, you must provide IP addresses to clients. Clients might also require a naming service or method for name resolution. This section explains IP addressing and name resolution for Windows NT RAS servers and clients on TCP/IP networks.

For information about implementing the Microsoft TCP/IP protocol in a network, see Chapter 1 "Microsoft TCP/IP and Related Services for Windows NT."

Assigning IP Addresses to RAS Clients

In Windows NT, each remote computer connecting to a RAS server through PPP on a Microsoft TCP/IP network is automatically provided an IP address from a static range assigned to the RAS server by the administrator during setup.

Windows NT RAS clients can also use a preassigned IP address specified in their phonebook. In this case, the Windows NT RAS server must be configured to permit users to request a specific address.

Name Resolution for RAS Servers and Clients

In addition to requiring an IP address, RAS servers and clients on a TCP/IP network might require a mechanism to map computer names to IP addresses. Four name resolution options are available on a Windows NT network: Windows Internet Name Service (WINS), broadcast name resolution, Domain Name System (DNS), and the HOSTS and LMHOSTS files.

RAS servers can use all these name resolution methods for operations performed on the server.

RAS clients are assigned the same WINS and DNS servers that are assigned to the RAS server. You must use the Registry to override this automatic assignment. For more information about overriding the automatic assignment of WINS and DNS servers, see Appendix A, "RAS Registry Values."

RAS clients in small networks where IP addresses do not change can use a HOSTS or LMHOSTS file for name resolution. By using these files on the local drive, you do not need to transmit name resolution requests to a WINS server and wait for the response over the modem.

For information about name resolution on a Microsoft TCP/IP network, see Chapter 3 "Implementation Considerations."

Connecting to Third-party Remote Access Servers Using IP

The Windows NT RAS server enables remote clients to share subnet addresses with computers on the LAN, thereby conserving IP addresses.

For more information on TCP/IP addressing, see Chapter 2, "Microsoft TCP/IP Architecture."

Note Remote access servers from other vendors might require that remote clients have a different subnet address than clients on the LAN. If remote clients dial into another vendor's remote access server and cannot connect to resources on the LAN, check the following configuration on your remote access server:

- If your third-party remote access server does not support proxy-ARP (Address Resolution Protocol), your remote clients must be assigned a different subnet address than LAN clients. Be sure your server is configured to assign remote clients with a subnet address that is unique on your LAN.
- Ensure that your network routers are configured so that remote access clients can use **ping** on target hosts, and vice versa. Use **ping** in the following order:
  1. Remote client to target server, then remote client to remote access server, then remote access server to target server.
  2. Target server to remote client, then target server to remote access server, then remote access server to remote client.

SLIP on TCP/IP Networks

Support for Serial Line Internet Protocol (SLIP) allows Windows NT RAS clients to connect to third-party remote access servers that use the SLIP remote communication standard. Clients can use SLIP only if the port for the Phonebook entry is a serial COM port.

When a user connects to a SLIP server, a Windows Terminal dialog box pops up for an interactive logon session with the UNIX SLIP server. The UNIX logon overrides and prevents the RAS logon from appearing. After a connection is established, remote network access becomes transparent to the user.

IPX and RAS

IPX is the native NetWare protocol used on many Novell networks. Because it is a routable protocol, IPX is suitable for enterprise-wide networks. This section explains how to integrate Windows NT RAS clients and servers into a NetWare IPX network.

Windows NT Support for NetWare

If Windows NT RAS computers must see a Novell NetWare network, the client computer must run a NetWare redirector. In Windows NT Workstation computers this redirector is called the *Client Service for NetWare* and in Windows NT Server computers this is called the *Gateway Service for NetWare.*

A Windows NT RAS server is also an IPX router and Service Advertising Protocol (SAP) agent for RAS clients only. RAS servers and their clients use the PPP IPX Configuration Protocol (IPXCP) defined in RFC 1552 to configure the remote access line for IPX. Once configured, RAS servers enable file and print services and the use of Windows Sockets applications over IPX on the NetWare network for RAS clients.

RAS servers provide clients connecting to an IPX network with an IPX net number and act as their SAP agent. The following section explains the addressing options available for Windows NT RAS using the IPX protocol.

For information about installing the connectivity services on a NetWare/Windows NT interconnected network, see Chapter 13 "Gateway Service for NetWare."

IPX Addressing for Remote Clients

RAS clients are always provided an IPX address by the RAS server. The IPX network number is either generated automatically by the RAS server, or a static pool of network numbers is given to the RAS server for assignment to RAS clients.

For automatically generated IPX network numbers, the Windows NT RAS server uses the NetWare Router Information Protocol (RIP) to determine an IPX network number that is not in use in the IPX network. The RAS server assigns that number to the remote client.

You can override the automatic assignments of network numbers. Manual assignments can be useful if you want more control of network number assignments for security or monitoring. When assigning IPX network numbers to a RAS server, ensure that duplicate network numbers are not assigned and that other NetWare services cannot assign the RAS IPX addresses. You can also assign the same network number to all clients to minimize RIP announcements from the RAS server.

For information about IPX addressing, see Chapter 13 "Gateway Service for NetWare."

NetBEUI and RAS

NetBEUI is suited for use in small workgroups or LANs. A NetBIOS gateway and the NetBEUI client protocol are installed by default on all Windows NT RAS servers and on most Windows networking clients. Previous versions of Windows NT RAS clients, LAN Manager RAS clients, MS-DOS RAS clients, and Windows for Workgroups RAS clients require NetBEUI.

Remote Access Protocols

Remote access protocols control transmission of data over the wide-area network (WAN). The operating system and LAN protocol(s) used on remote access clients and servers dictate which remote access protocol your clients will use. The remote access protocols are of four types: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Microsoft RAS Protocol, and NetBIOS Gateway.

Point-to-Point Protocol (PPP)

Windows NT supports the Point-to-Point Protocol (PPP) in RAS. PPP is a set of industry standard framing and authentication protocols that enable remote access solutions to interoperate in a multi-vendor network. Microsoft recommends that you use PPP because of its flexiblity and its role as an industry standard as well as for future flexibility with client and server hardware and software.

PPP support enables computers running Windows NT to dial into remote networks through any server that complies with the PPP standard. PPP compliance also enables a Windows NT Server computer to receive calls from, and provide network access to, other vendors' remote access software.

The PPP architecture also enables clients to load any combination of IPX, TCP/IP, and NetBEUI. Applications written to the Windows Sockets, NetBIOS, or IPX interface can be run on a remote Windows NT Workstation computer. The following picture illustrates the PPP architecture of RAS:

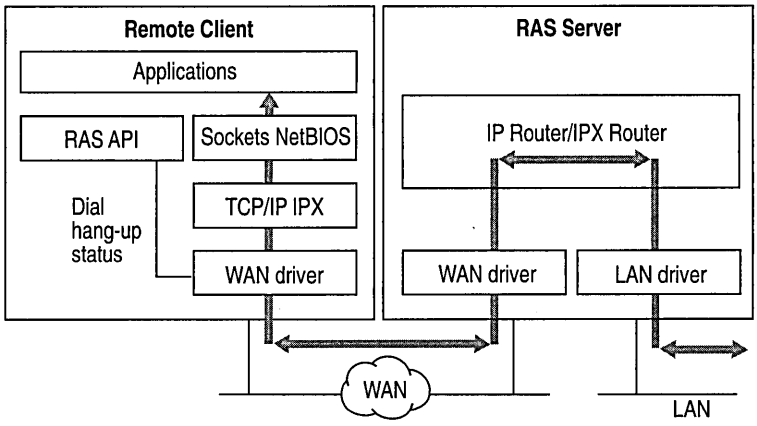


Figure 1.13 PPP Architecture of RAS

PPP has become the standard for remote access.

Remote Access protocol standards are defined in *Requests for Comments* (RFCs), which are published by the Internet Engineering Task Force and other working groups. The RFCs supported in this version of Windows NT RAS are

- RFC 1549 PPP in HDLC Framing
- RFC 1552 The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1661 Link Control Protocol (LCP)
- RFC 1717 PPP Multilink Protocol

If your remote clients connect to third-party PPP servers, they might need to enable a post-connect terminal script to log on to the PPP server. After the server informs them it is switching to PPP framing mode, the user must start Terminal to complete logon.

RAS Connection Sequence

Upon connecting to a remote computer, PPP negotiation begins:

Framing rules are established between the remote computer and server. This allows continued communication (frame transfer) to occur.

The RAS server then authenticates the remote user using the PPP authentication protocols (PAP, CHAP, SPAP). The protocols invoked depend on the security configurations of the remote client and server.

Once authenticated, the Network Control Protocols (NCPs) enable and configure the server for the LAN protocol used on the remote client.

When the PPP connection sequence has completed successfully, the remote client and RAS server can begin to transfer data using any supported protocol, such as Windows Sockets, RPC, or NetBIOS. The following figure illustrates the location of the PPP protocol on the OSI model.

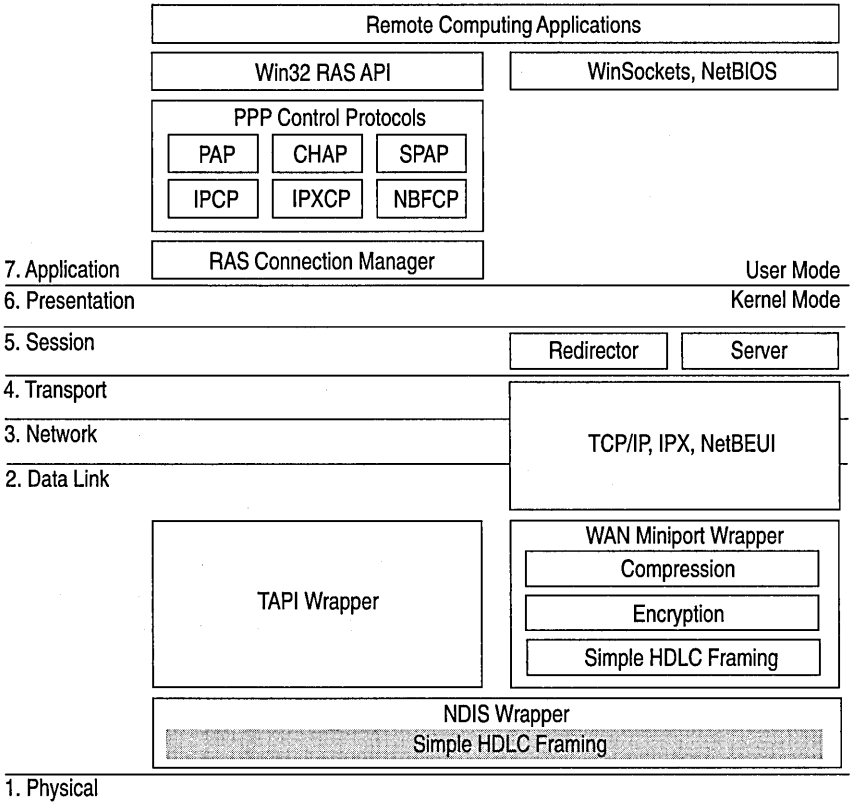


Figure 1.14 Location of the PPP Protocol on the OSI Model

If your remote client is configured to use the NetBIOS gateway or SLIP, this sequence is invalid.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol (SLIP) is an older remote access standard typically used by UNIX® remote access servers. Windows NT Remote Access clients support SLIP and can connect to any remote access server using the SLIP standard. This permits Windows NT version 3.5 clients to connect to the large installed base of UNIX servers. The Windows NT Remote Access server does not support SLIP clients.

The RFCs supported in this version of Windows NT RAS are

- RFC 1144 Compressing TCP/IP Headers for Low-Speed Serial Links
- RFC 1055 A Nonstandard for Transmission of IP Datagrams Over Serial Lines: SLIP

Microsoft RAS Protocol

The Microsoft RAS protocol is a proprietary remote access protocol supporting the NetBIOS standard. The Microsoft RAS protocol is supported in all previous versions of Microsoft RAS and is used on Windows NT version 3.1, Windows for Workgroups, MS-DOS, and LAN Manager clients.

A RAS client dialing into an older version of Windows (Windows NT version 3.1 or Windows for Workgroups) must use the NetBEUI protocol. The RAS server then acts as a "gateway" for the remote client, providing access to servers that use the NetBEUI, TCP/IP, or IPX protocols.

NetBIOS Gateway

Windows NT continues to support NetBIOS gateways, the architecture used in previous version of Windows NT and LAN Manager. Remote users connect using NetBEUI, and the RAS server translates packets, if necessary, to IPX or TCP/IP. This enables users to share network resources in a multi-protocol LAN but prevents them from running applications which rely on IPX or TCP/IP on the client. The NetBIOS gateway is used by default when remote clients are using NetBEUI. The following figure illustrates the NetBIOS gateway architecture of RAS.

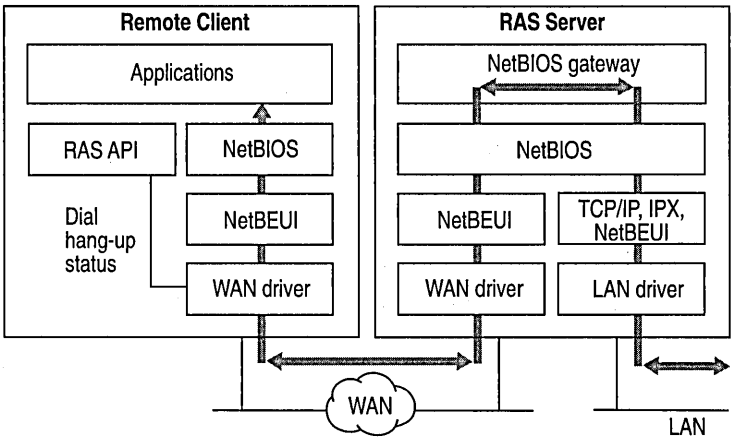


Figure 1.15 NetBIOS Gateway Architecture of RAS

An example of the NetBIOS gateway capability is remote network access for Lotus® Notes® users. Although Lotus Notes does offer dial-up connectivity, dial up is limited to the Notes application. RAS complements this connectivity by providing a low-cost, high-performance remote network connection for Notes users which not only connects Notes, but offers file and print services, and access to other network resources.

WAN Options

Clients can connect to servers through phone lines and modems, ISDN, X.25, RS-232C null modem, or Point-to-Point Tunneling Protocol (PPTP). The following sections describe these options.

Phone Lines and Modems

The most common WAN connection is a standard analog telephone line and a modem. Standard analog phone lines are available worldwide and will meet most RAS needs for roving users.

Note Standard analog phone lines are also called PSTN (Public Switched Telephone Network) or POTS (Plain-old Telephone Service).

Nearly 200 modems are compatible with Windows NT. Most modems that comply with industry standards should interoperate. However, many difficult-to-detect problems can come from incompatible modems. To prevent such problems, use the same modem on clients and servers.

Modems are automatically detected. Automatic modem detection is especially useful for users who are not sure what modem is installed (for example, an internal modem).

Third-party modem pools can be used on either the client side or the server side. Modem pools are made available to RAS through the Network icon in Control Panel. Consult your modem pool documentation for more information.

Modem data compression and error control are available. However, built-in software compression offers enhanced performance over modem data compression.

For more information about modems, see the "Choosing Modems" section in Chapter 6, "Installing and Configuring Remote Access Service."

ISDN

To enhance WAN speeds at a stationary remote site or at sites that will use RAS, use an Integrated Services Digital Network (ISDN) line. Whereas standard phone lines typically transmit at 9600 bits per second (bps), ISDN lines can transmit at speeds of 64 or 128 kilobits per second.

An ISDN line must be installed by the phone company at both the server and at the remote site. ISDN also requires that an ISDN card be installed in place of a modem in both the server and remote client. Costs for ISDN equipment and lines can be higher than standard modems and phone lines. However, the speed of communication reduces the duration of connections, possibly saving toll charges.

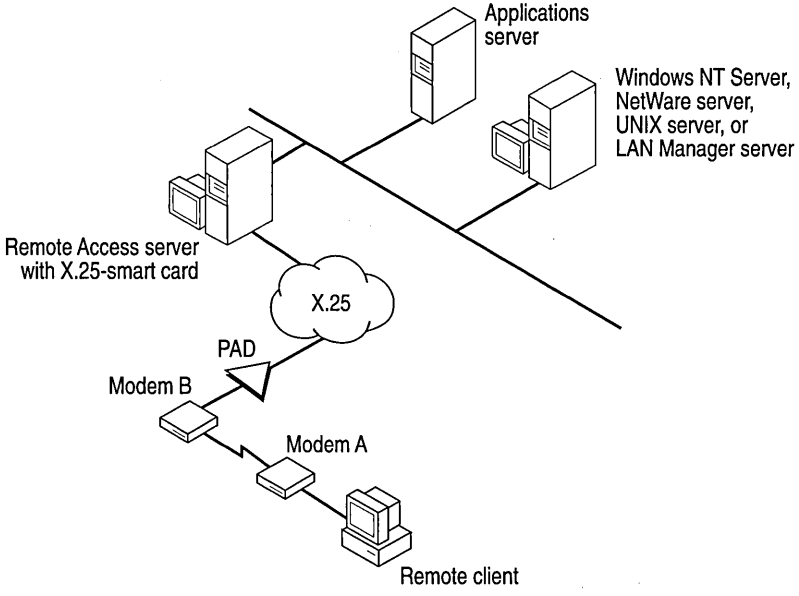
For more information about how to install and configure ISDN cards, see RAS online Help.

X.25

X.25 is a standard packet-switching communication protocol (or transport) designed for WAN connectivity.

Windows NT RAS suppports connections based on the X.25 standard using Packet Assemblers/Disassemblers (PADs) and X.25 smart cards. You can also use a modem and special dial-up X.25 carriers (such as Sprintnet and Infonet®) in place of a PAD or smart card on RAS clients. For more information about RAS and X.25, see RAS online Help or Chapter 9, "X.25 PAD Support."

The following illustration shows how a client connects to the Remote Access server through a dial-up PAD and the X.25 network.



How a Remote Access Client Connects to the Server Through a Dial-Up PAD

RS-232C Null Modem

Suppose two or more networks are in the same location but are not physically connected. To use resources on both networks from one computer, use an RS-232C null modem. The client connects an RS-232C cable from a COM port to a COM port on the RAS server. RAS is used to create network access.

An RS-232C null modem can also be used as a substitute for a network card in a computer located physically near (less than 50 feet of cable) a RAS server.

Point-to-Point Tunneling Protocol (PPTP)

A RAS server is usually connected to a PSTN, ISDN, or X.25 network, allowing remote users to access a server through these networks. RAS now allows remote users access through the Internet by using the new Point-to-Point Tunneling Protocol (PPTP).

PPTP is a new networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet by dialing into an Internet Service Provider (ISP) or by connecting directly to the Internet. PPTP offers the following advantages:

- Lower Transmission Costs
- Lower Hardware Costs
- Lower Administrative Overhead
- Enhanced Security

For more information, see Chapter 11, "Point-to-Point Tunneling Protocol."

Security Features

Windows NT is a secure operating environment, designed to meet the requirements of C-2 level (U.S. Department of Defense) security:

- Access to system resources can be discretely controlled.
- All system access can be recorded and audited.
- Access to the system requires a password and leaves an audit trail.

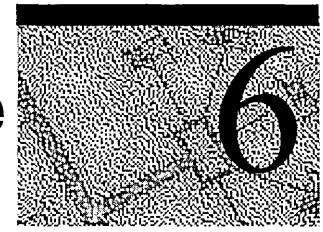
Windows NT Server uses a *trusted domain, single-network logon* model:. Users and groups of one domain can be granted access to resources in a trusting domain. After being authenticated, users carry access credentials that are presented whenever access to a resource is requested on the network. A Windows NT Server computer—provided it is secured physically—can be locked-down using software.

This single-network logon model extends to RAS users. RAS access is granted from the pool of all Windows NT user accounts. An administrator grants the right to dial into the network, and users then use their domain login to connect via RAS. After being authenticated by RAS, users can use resources throughout the domain and in any trusted domains.

Finally, Windows NT provides the Event Viewer for auditing. All system, application, and security events are recorded to a central secure database which, with proper privileges, can be viewed from anywhere on the network. Attempts to violate system security, to start or stop services without authorization, or to gain access to protected resources, are recorded in the Event Log and can be viewed by the administrator. For more information on RAS authentication and security features such as Data Encryption and Callback, see Chapter 7, " RAS Security."

CHAPTER 6

Installing and Configuring Remote Access Service



This chapter describes how to install Windows NT Remote Access Service (RAS) on your computer and how to configure the service to work on your network. (Note: It assumes that Windows NT has already been successfully installed on your computer.)

RAS can be installed during the initial Setup or after the initial Windows NT Setup is complete.

To install and configure RAS, you must be logged on as a member of the Administrators group.

Hardware Requirements for RAS

Before you install RAS, all hardware should be installed and working. Depending on your network and requirements, you might need the following hardware:

- Network adapter card with a certified Network Driver Interface Specification (NDIS) driver
- One or more compatible modems (see the *Hardware Compatibility List* or the Remote Access Setup program) and an available COM port
- Multiport adapter card for acceptable performance with multiple remote connections
- X.25 smart card (if using an X.25 network)
- ISDN card or modem (if using an ISDN line)

See the *Hardware Compatibility List* to verify the compatibility of all hardware in a Windows NT computer.

Choosing Modems

To ensure that your modems work with Remote Access Service, select them from the list of supported modems in the *Hardware Compatibility List*. Microsoft has tested and verified these modems with Remote Access Service.

Compatibility and Speed

Modems from different manufacturers—and even different models from one manufacturer—might be incompatible in some settings and circumstances. Even modems that claim to follow the Hayes AT command set might, at times, be unable to communicate with other Hayes-compatible modems.

And because modems achieve high speeds in different ways, compatibility problems increase with high-speed modems. Even modems that follow a standard for compression and error correction might be unable to communicate with each other at higher speeds and, therefore, might fall back to a slower speed. So, if you buy high-speed modems from different manufacturers to benefit from high data-exchange rates, you might be disappointed.

Note To ensure compatibility, have clients and servers use the same kind of modem. This is less critical if your modems conform to industry standards, but still it is safer to choose the same model for both clients and server. For more information on RAS and modem compatibility standards, see the RAS Reference appendix in the *Networking Guide* of the *Windows NT Server Resource Kit version 4.0*.

For rates of 12,000 bps and higher, modem manufacturers often require that computer-to-modem communication occur at 19,200 bps. For this reason, Remote Access software assumes that modems able to connect at 12,000 or 14,400 bps can function at the computer-to-modem speeds of 19,200 bps or faster. Virtually all high-speed modems can do so.

Supported Modems

Modems supported by Remote Access do not necessarily work in all modes with other modems in the list. For example, the Hayes® V-Series 9600 modem connects at 9600 bits per second (bps) only with another Hayes V-Series 9600 modem. So if you install this modem on a Remote Access server, make sure that Remote Access clients also have Hayes V-Series 9600 modems. Otherwise, connections will probably be made at 2400 bps.

If you use one of the modems named in the *Hardware Compatibility List* when you set up Remote Access, and you cannot connect, follow these steps:

▶ To troubleshoot a supported modem

1. Make sure your cabling is correct. (See Appendix B, "RAS Cabling.")
2. If you still cannot connect, check the modem's documentation to verify that the modem has been correctly installed.
3. Using a terminal emulator program (such as Windows NT HyperTerminal), try to issue commands to the modem. See the procedure "To test a modem with Windows NT HyperTerminal" in this chapter.
4. Turn on device logging in the Registry by changing the following key to 1:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RASMan\Parameters\Logging.`

For more information, see Chapter 8, "Maintenance and Troubleshooting."

Unsupported Modems

Although modems not supported by Microsoft can work with the Remote Access Service, they have not yet been tested with the software. If you choose unsupported modems, make sure they support one of the modulation schemes shown in Table 2.1.

Table 2.1 shows the most popular modulation schemes in the left column and their corresponding speed range in bits per second (bps) in the right column.

Table 0.1 Modulation Schemes and Modem Speeds

Popular Modulation Schemes	Modem to Modem speed
V.22 (ITU-T (formerly CCITT) Standard)	1200 bps
V.22 *bis* (ITU-T (formerly CCITT) Standard)	2400 bps
V.32 (ITU-T (formerly CCITT) Standard)	4800 - 9600 bps
V.32 *bis* (ITU-T (formerly CCITT) Standard)	4800 - 14400 bps
V.fc and V.fast (Proprietary Modulation Schemes)	2400 - 28800 bps
V.34 (ITU-T (formerly CCITT) Standard)	2400 - 28800 bps

For details about industry standard protocols, see the glossary in online Help.

When configuring an unsupported modem for RAS, you must select from the list of supported modems a modem that matches yours as closely as possible. For best results, compare entries in the MODEM.INF file with commands for your modem (located in your modem's documentation).

To see a list of supported modems, you can also have RAS try to autodetect your modem.

▶ To configure an unsupported modem

1. In Control Panel, click Network.
2. In the **Services** tab, select **Remote Access Service**.
3. Click **Properties**.
4. In the **Remote Access Setup** dialog box, select the port you want to configure for the unsupported modem, and click **Add**.
5. In the **Add RAS Device** dialog box, click **Install Modem**.
6. In the RAS Setup Wizard, select the checkbox to select a modem from a list of supported modems.
7. From the list of modems, select the one that is most similar to your modem.
8. Click **Next**, and continue with the Setup Wizard.
9. If you configure a new port for the unsupported modem, restart your computer.

   If you reconfigure a port already in use, you do not need to restart your computer, but you do need to stop and then restart RAS.

If you have trouble connecting through an unsupported modem, test the modem's compatibility.

▶ To test a modem's compatibility

1. Check the modem's documentation to make sure you have installed and configured the modem correctly.
2. Make sure your modem is connected to a serial communication (COM) port on your computer and that your software is set for the same port.
3. Turn on your modem.
4. Check to see if the modem works properly with Windows NT HyperTerminal.

   (For instructions, see the following procedure.) If the test works, you can assume the modem is not malfunctioning.
5. If the modem fails to work after you have verified that it works with Windows NT HyperTerminal, contact the manufacturer and request a modem command file compatible with the RAS Modem.inf file.

   For information about creating a correct modem command file, see "Adding a New Modem to Modem.inf" in Appendix C, "Understanding MODEM.INF."

▶ To test a modem with Windows NT HyperTerminal

1. From the Accessories folder, click the HyperTerminal folder and select HyperTerminal.
2. In the **Connection Description** dialog box, enter any name in the **Name** box and click **OK**.
3. In the **Connect To** dialog box, click **Cancel**.

Note HyperTerminal tests the first modem listed in the **Connect Using** box.

4. In the HyperTerminal window, type **at**.

   Your modem should return *OK*, which is echoed on the screen. Some modems return *0*, depending on their result code settings.

5. If your modem will not work through HyperTerminal, call the manufacturer.

Connecting Without a Modem

To establish a direct serial connection between two computers, select a null modem. Although a direct serial connection eliminates the need for a network adapter card, it is a slow link, and password authentication is still required. A null modem configuration works best only for computers physically near each other.

▷ **To configure your system for a direct serial connection**

- Select a null modem from the list of modems during setup when configuring the COM ports for a serial connection.

  A null modem must be configured on both the client and the server.

For information about configuring COM ports for RAS usage, see "Installing Remote Access Software" in this chapter. For information about installing ports, see the Ports icon in Control Panel.

Important For information about cabling required for null modems, see Appendix B, "RAS Cabling" or see the topic "Cabling Requirements" in the RAS online Help.

Modem-Pooling Equipment

Windows NT works with a variety of third-party modem pooling equipment.

▷ **To configure a server to work with modem-pooling equipment**

1. Configure the equipment to behave like one of the modem types listed in the Setup program. (In other words, the modem-pooling equipment must generate and accept command strings as if it were a modem of the chosen type.) The switching equipment must also have the same RS-232 signal behavior as the specified modem.
2. Connect COM ports to this equipment, and specify the modem type in the Remote Access Setup program.

   Microsoft suggests that the equipment be configured as a Hayes-compatible modem, a widely-known standard.

Installing Remote Access Software

Although RAS is part of Windows NT Setup, you can also install it using the Network icon in Control Panel after you have installed Windows NT.

Note RAS installation will vary slightly, depending on which network protocols are installed. If you will use the TCP/IP or IPX protocol with RAS, install the protocol before you install RAS. (Note that selecting an uninstalled protocol will cause that protocol to be installed at the conclusion of RAS Setup.) For information about installing either protocol, see the *Windows NT Server Start Here*.

▶ **To add the Remote Access software**

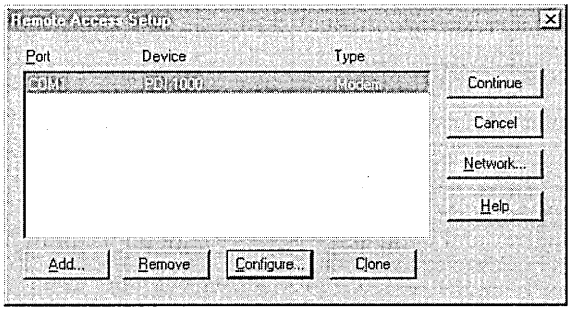
1. In Control Panel, click the Network icon.
2. In the **Services** tab, click **Add**.
3. From the **Network Service** box, select **Remote Access Service** and then click **OK**.

   When prompted for the path to the distribution files, provide the path and click **OK**. The RAS files will be copied to your computer.
4. If you have no devices installed on your computer, the Modem Wizard appears and helps you install a RAS capable device.
5. The **Add RAS Device** dialog box displays a list of all ports available to Windows NT for RAS. If you have successfully installed a multiport adapter, ISDN card, X.25 card, or other device, it will appear in this list.

   Select the port you will use for remote access, and click **OK**.
6. Click **Install Modem** to have RAS Setup automatically detect the modem connected to the selected port.

   If RAS Setup cannot distinguish between two or more modems, a dialog box will appear, requiring you to select your modem from a short list.
7. Click **Install x.25 Pad** to install an x.25 Pad.
8. In the **Remote Access Setup** dialog box, select the port and click **Configure**.
9. In the **Configure Port Usage** box, choose how the port is to be used and click **OK.**
   - **Dial out only** means the computer will be a RAS client only.
   - **Receive calls only** means the computer will be a RAS server only.
   - **Dial out and Receive calls** means the computer can be a client or server. (Note: The computer cannot be both at the same time.)

10. In the **Remote Access Setup** dialog box, configure RAS network-wide settings by clicking **Network**. For more information, see the following section, "Choosing a Protocol for a RAS Server."



11. Consult the following table for a description of each button in the **Remote Access Setup** dialog box. Default settings are usually ideal.

Option	Use to
Add	Make a port available to RAS.
Remove	Make a port unavailable to RAS.
Configure	Change the Remote Access settings for the port, such as the attached device or the intended usage (dialing out only, receiving calls only, or both).
Clone	Copy the same modem setup from one port to another.
Continue	Proceed to the next step in Setup when you finish with this dialog box.
Cancel	Leave the Setup program.
Network	Configure RAS network-wide settings. Set network access to entire network or RAS computer only. Select and configure network protocols the RAS server will support. Select network protocols the computer will use for dial-out (client) connections. Set authentication and data encryption options.
Disable Automatic Restoration Of Network Connections At Logon	Clear this check box to restore your previous network connections when you log on to your computer. If no netcard is detected on your computer, this box is checked by default because restoring connections over a remote link can be especially time consuming..

12. Click **Continue** when you are finished setting up the port and network configurations.

    RAS Server Configuration dialog boxes will appear for the protocols installed on your computer. See the appropriate topics in the following section for configuring LAN protocols for RAS use.

13. Click **Close** in the **Confirmation** dialog box, and click **OK** in the **Network** dialog box.

    You might be prompted to confirm network protocols or other settings.

14. You must restart your computer for the Remote Access installation and configuration take effect.

The Remote Access software includes the following applications:

- Dial-Up Networking is the client version of RAS and is used to connect to dial-up servers. The Dial-Up Networking icon is located in the My Computer dialog box and in the Accessories folder on the Start menu.
- Dial-Up Networking Monitor, used to monitor connections and devices, is located in Control Panel.
- Remote Access Admin, used to monitor remote users connecting to a RAS server, is located in the Administrative Tools folder on the Start menu.

Choosing a Protocol for a RAS Server

Because RAS provides access to a LAN, you must select and configure the protocols to use on the LAN. A Windows NT Workstation or Server computer can be either a RAS server or a client. You must configure the LAN protocols RAS will use in each role.

A RAS computer's role is determined when you specify how RAS-enabled ports will be used. See the previous procedure for information on the various port settings.

Setting network LAN protocols affect all RAS operations for all RAS-enabled ports. For example, you must enable TCP/IP for the LAN before you can choose to use TCP/IP for a specific RAS entry. For more information on choosing protocols for RAS entries, see the section "Choosing a Protocol for a RAS Entry" later in this chapter.

For information about choosing a LAN protocol, see "Configuring RAS to Use LAN Protocols" in Help.

Configuring a RAS Server to Use NetBEUI

NetBEUI gives the best performance for NetBIOS applications in small LANs. Removing NetBEUI still allows you to use RAS with TCP/IP or IPX. You can configure whether NetBEUI clients can access the entire network or the RAS computer only.

For information about using NetBEUI on a RAS server, see "Configuring a RAS Server to Use NetBEUI" in Help.

Configuring a RAS Server to Use TCP/IP

Use the Network icon in Control Panel to configure or reconfigure the TCP/IP settings for RAS connections.

The RAS server has two TCP/IP configurations:

- Its own basic configuration and IP address as a server on the LAN. For information on this configuration, see the TCP/IP Help file.
- Its RAS configuration to supply IP addresses to RAS clients.

For information about how to configure RAS to supply IP addresses to RAS clients, see "Configuring a RAS Server to Use TCP/IP" in Help.

Configuring Name Resolution for RAS Clients

RAS client name resolution is based on the available network services and on the RAS server configuration:

- If the RAS server is configured to use a WINS server and a DNS server on the network, RAS clients will use them as well.
- If the RAS server has multiple network adapter cards, clients will use the WINS servers on the first network configured for INS and DNS.

Note Clients can also specify addresses of WINS and DNS servers on a per-entry basis by configuring TCP/IP Settings in the Dial-Up Networking Server tab.

- RAS clients in small networks where IP addresses do not change can use a HOST file and LMHOSTS file for name resolution. Using these files on the local drive saves transmitting the name resolution request to the WINS server and waiting for a response over the modem.

Note Standard broadcast name resolution does not work over RAS. Users must have a name resolution method, such as WINS or a LMHOSTS file, or they must use IP addresses.

For more information about name resolution on a Microsoft TCP/IP network, see Chapter 3, "Implementation Considerations."

Configuring a RAS Server to Use IPX

Use the Network icon in Control Panel to configure or reconfigure the IPX settings for RAS connections. For information about using IPX on a RAS server, see "Configuring a RAS Server to Use IPX" in Help.

Choosing a Protocol for a RAS Entry

Dial-Up Networking clients can enter and maintain names and telephone numbers of remote networks. Clients connect to and disconnect from remote networks using the Dial-Up Networking program. Users can select the network protocols to use for a specific Phonebook entry, depending on the type of server you are dialing (PPP, SLIP, or Microsoft RAS).

For information about choosing a protocol on a RAS client, see "Choosing a Protocol for a RAS Entry" in Help.

Special Configurations

This section contains information about configuring RAS in special situations and using specialized hardware.

Configuring Stand-alone Remote Servers to Appear to Local Network Browsers

Users who set up a RAS server at home and dial into it from a computer at work must follow the referenced procedure to have the name of their home server appear in the browsing list of remote clients.

For information about configuring a remote RAS server to appear to local network browsers, see "Configuring Stand-alone Remote Servers to Appear to Local Network Browsers" in Help.

Configuring Other Vendors' Dial-Up Servers for NetBIOS IP and IPX

If Windows NT clients dialing into other vendors' dial-up servers must access NetBIOS resources using IP and IPX, the dial-up servers must be configured to forward NetBIOS broadcast traffic. Such forwarding might result in poor performance over the RAS connection if the LAN has substantial NetBIOS activity. For information about configuring a server to forward NetBIOS broadcasts, see "IPXRouter Parameters" in Appendix A, "RAS Registry Values."

For better performance on TCP/IP networks, Windows NT clients can use WINS servers or proxies when dialing into other vendors' servers if the server can provide access to a Windows NT Server WINS server or proxy agent on the LAN.For more information, see TCP/IP online Help.

Granting Remote Access Permissions

After installing Remote Access software on a server, you must grant Remote Access permissions to users. Without them, users cannot successfully connect to the Remote Access computer (even if Remote Access client software is installed on their computers).

For more information see "Setting Up RAS Security on Accounts," in Chapter 7 "RAS Security."

Dialing Options

Windows NT RAS features several new dialing options such as AutoDial and Multilink. With these options you can automatically connect to remote sites and resources and use multiple WAN devices to connect to the same remote resource, thereby increasing bandwidth.

RAS Automatic Dialing

RAS AutoDial maps and maintains network addresses to RAS phonebook entries, allowing them to be automatically dialed when referenced—whether from an application or from the command line. A network address can be an Internet host name, an IP address, or a NetBIOS server name.

AutoDial also learns about every connection made over a RAS link for possible automatic reconnection later.

There are two possible scenarios when AutoDial attempts to make a connection:

- If you are disconnected from a network, AutoDial attempts to create a network connection whenever an application references a remote address.
- If you are connected to a network, AutoDial attempts to create a network connection for only those addresses that it has previously learned. Incorrectly typed server or Internet host names will not cause an AutoDial attempt.

Although AutoDial is automatically enabled when you start your computer, you can turn it off if desired. (For example, you might have multiple Internet providers on a computer at one location and want to use different providers at different times).

▷ **To turn off AutoDial**

1. In Dial-Up Networking, select an entry to dial from the Phonebook list.
2. Click **More** and select **User preferences**.
3. In the **Dialing** tab, click to clear each location listed in the **Enable auto-dial by location** list.

You can turn on AutoDial by reselecting a location in the **Enable auto-dial by location** list.

Known Problems for this Release

- AutoDial does not yet work over IPX connections. AutoDial works only with the TCP/IP and NetBEUI protocols. In Dial-Up Networking, select the entry for each RAS connection over which you expect to AutoDial. Then click **More** and select **Edit Entry and Modem Settings**. In the Server tab, click to clear the **IPX/SPX compatible** check box.
- If you need to disable your network card, you cannot simulate being disconnected from the network by simply unplugging the cable from the network adapter card. Instead, create a new hardware profile with your network adapter card disabled:

  In the System icon in Control Panel, in the Hardware Profiles tab, make a copy of your original installation. Then, in the Devices icon, select your network card and click **HW Profiles**. Select the new hardware profile and disable your network card. When you reboot, you can choose this no-network profile.

  This is useful if you have a portable computer with a PCMCIA network card installed all the time and you want to connect to the network from a remote location.
- If the following three conditions exist, make sure your DNS server does not resolve Internet hostnames:
  - a DNS server on your network
  - your network is not directly connected to the Internet
  - you want to AutoDial Internet addresses

Most Internet utilities (ftp, www browsers, etc.) do not ask DNS for exact matches, and it is possible for the DNS server to successfully resolve an address to one within your local domain. For example, try typing a similar command at the Command Prompt while connected to your network:

```
C:> ping ftp.microsoft.com
Bad IP address ftp.microsoft.com
```

If the **ping** command resolves the name to an IP address, you must disable DNS on your computer for AutoDial to automatically dial Internet addresses when connected to your network.

- AutoDial requires at least one TAPI dialing location. AutoDial can automatically dial different RAS phonebook entries for the same address, depending on the current TAPI dialing location.

  For example, suppose two TAPI dialing locations are created (Home and Office), and suppose you run the command **ftp ftp.microsoft.com**. AutoDial automatically dials the RAS phonebook entry INTERNET1 when your current TAPI dialing location is set to Home, and it automatically dials the RAS phonebook entry INTERNET2 when your current TAPI dialing location is set to Office.

  To create TAPI dialing locations, use the Telephony icon in Control Panel.

- When Explorer is initializing, it might reference remote paths in your desktop shortcut icons or targets which, in turn, will cause an AutoDial attempt. If AutoDial tries to create a connection when you log on to your computer, either delete remote paths from your Desktop shortcut icons or targets, or change them to reference a local file.

- If commands in your Explorer Start/Run list access remote paths, selection of one causes an AutoDial attempt. Currently, you cannot selectively delete items in this list. But to work around this issue, remove the HKCU\Software\Windows\CurrentVersion\Explorer\RunMRU key in the Registry, log out, and log back on again. Your Explorer Start/Run list should now be empty.

- The Registry configuration for AutoDial has changed. It is recommended that you delete the Autodial registry key in:

  ```
  HKEY_CURRENT_USER\Software\Microsoft\RAS
  ```

  AutoDial will then relearn your addresses.

Troubleshooting AutoDial

If you have problems, run the following command from the Command Prompt to give basic AutoDial status:

C:> rasautou -s

Status ouptput has two parts: network adapter card bindings and a list of learned AutoDial addresses. At least one network adapter card binding must be reported as working for AutoDial to realize you are connected to the network. For AutoDial to automatically create a network connection while you are connected to a network, the address must be in the list of learned AutoDial addresses. Here is an example listing network adapter card bindings and a list of learned addresses:

```
Checking netcard bindings...
NetworkConnected: network (\Device\Nbf_IEEPRO1, 0) is up

Enumerating AutoDial addresses...
There are 3 Autodial addresses:
ftp.microsoft.com
198.105.232.1
SCRATCH
```

Multilink Dialing

Multilink combines multiple physical links into a logical "bundle." This aggregate link increases your bandwidth.

RAS performs PPP Multilink dialing over multiple ISDN, X.25, or modem lines. The feature is available only if multiple WAN adapters are available on the computer.

To use Multilink, both the clients and servers must have Multilink enabled.

Note If a client uses a multinked phonebook entry to dial a server that is configured to call that user back for security reasons (*enforced callback*), then only one of the multilinked devices will be called back. This is because only one number can be stored in a user account. Therefore, only one device will connect and all other devices will fail to complete the connection, and the client loses multilink functionality.

A situation that will work is if the multilinked phonebook entry is ISDN with two channels that have the same phone number.

▶ **To enable Multilink on a RAS client**

1. In Dial-Up Networking select an entry to dial from the Phonebook list.
2. Click **More** and select **Edit entry and modem properties**.
3. In the **Basic** tab, in the **Dial using** box, select multiple lines.
4. Click **Configure** to choose which modems or adapters to use for the connection and then click **OK**.

For more information about Multilink connection options, see the online Help.

▶ **To enable Multilink on a RAS server**

1. In Control Panel, click the Network icon.
2. In the **Services** tab, select **Remote Access Service** in the **Network Services** box and click **Properties**.
3. In the **Remote Access Setup** dialog box, click **Network**.
4. In the **Network Configuration** dialog box, select **Enable Multilink** and click **OK**.

Monitoring Connections

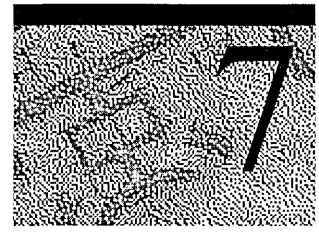
The Dial-Up Networking Monitor (located in the Control Panel) provides the status of a call, and allows you to see

- the speed at which you connected
- the duration of the connection
- the names of users connected to a RAS server
- protocols used during the connection
- which devices are part of a connection

For more information on using Dial-Up Monitor, see Chapter 8, "Maintenance and Troubleshooting."

CHAPTER 7

RAS Security



Windows NT user accounts and domains provide security with encrypted authentication. RAS provides additional security features such as callback and data encryption. You can also install 3rd-party security hosts to prevent unauthorized access to your LAN.

This chapter covers the following RAS security features:

- Setting RAS up in a domain
- Granting RAS permission to user accounts
- Setting RAS security on user accounts
- Data encryption
- Callback security
- Support for security hosts
- Auditing

Setting RAS up in a Domain

Applying RAS security to clients involves three steps: Setting RAS up in a Windows NT domain, granting RAS permission to Windows NT user accounts, and then setting RAS security on these accounts.

This section explains Windows NT user accounts and approaches for implementing domain-based security for RAS. This section assumes you have a domain structure established and provides information about integrating RAS into your existing domain scheme. Remote Access servers using Windows NT Server domain-based security can be centralized in a single domain or distributed among several domains that might have trust relationships.

Centralized Servers

If your goal is to simplify administration, centralize all Remote Access servers in a single domain: Only one user account database will need to be maintained, and the system administrator will be able to monitor all RAS servers and users at one time. (Use trust relationships if departments maintain their own user accounts.)

Note Because the domain is logical rather than physical, centralized servers can be in different locations and still be part of the same domain.

In a trusted domain model, it is best to set up a user account on only one domain for each user, especially for users dialing in through RAS version 1.1 or earlier. If the Remote Access server cannot find the user's account in the server's domain, it simultaneously checks the trusted domains and accepts the first response. If the first response comes from a domain where the user has a different password or does not have Remote Access permission, authentication fails even though a second response from another domain might have the same user account with Remote Access permission.

Distributed Servers

Smaller organizations that value flexibility and local control, or organizations that have no clear need for centralized security, might prefer a *distributed server system,* in which individual departments or workgroups set up and maintain their own Remote Access domains. Trust relationships can be used to permit access across domains.

Note For additional information about Windows NT Server user accounts and domains, see the *Windows NT Server Concepts and Planning Guide.*

Granting RAS Access and Permissions

After a RAS server is installed, you must specify who can dial in to it. Use the **Remote Access Admin** utility or User Manager to select a computer's or domain's user accounts. Then grant RAS permission to the user accounts, as shown in the following sections. After passing Remote Access authentication and connecting to the LAN, remote users can access resources on the application server for which they have permission. Remember: You grant or revoke remote access privileges on a user-by-user basis. So although RAS is running on a Windows NT Server computer, access to the network must be explicitly granted to each user who needs it.

Note Remote users are subject to Windows NT Server security, just as they are at the office. In other words, they cannot do anything for which they lack sufficient privilege, nor can they access resources for which they do not have permission.

You do not need to create user accounts just for RAS users. RAS servers use the user accounts of any trusted domain or computer on the Windows NT network.

For information about adding a remote client to a domain, see Remote Access online Help or Control Panel Help.

Setting up RAS Security on Accounts

Remote users must be authenticated by a Remote Access server before they can access or generate traffic on the network. This authentication is a separate step from logging on to Windows NT. User passwords and the authentication procedure are encrypted when transmitted over phone lines.

You can restrict remote users' access to the network and to the Remote Access server. This allows an administrator to tightly control what information is available to remote users, and to limit their exposure in the event of a security breach.

For more information about granting RAS permission to users, see the Remote Access Admin online Help.

Granting and Preventing Network Access

By enabling and disabling sets of protocols and adapters called *bindings*, you dictate network access by remote users:

Enable bindings to grant user access to resources.

Disable bindings to prevent user access to resources.

Figure 0.1 shows a configuration with two bindings that allow remote users to see and access all connections in the Remote Access gateway:

- TCP/IP and Adapter 1
- NetBEUI and Adapter 2

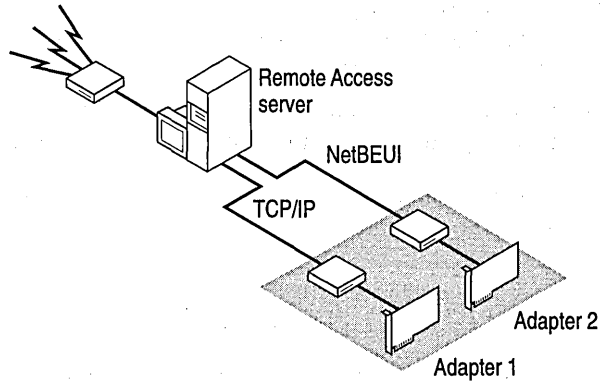


Figure 7.1 Remote Users Allowed Access to the Network

For more information about bindings, see the Network icon in Control Panel and Control Panel online Help.

Restricting Remote Users to the Dial-In Server

Even if the Remote Access server is connected to a network, you can restrict remote users to the server they dial in to, as shown in Figure 7.2

For more information, see "Network Configuration" in online Help.

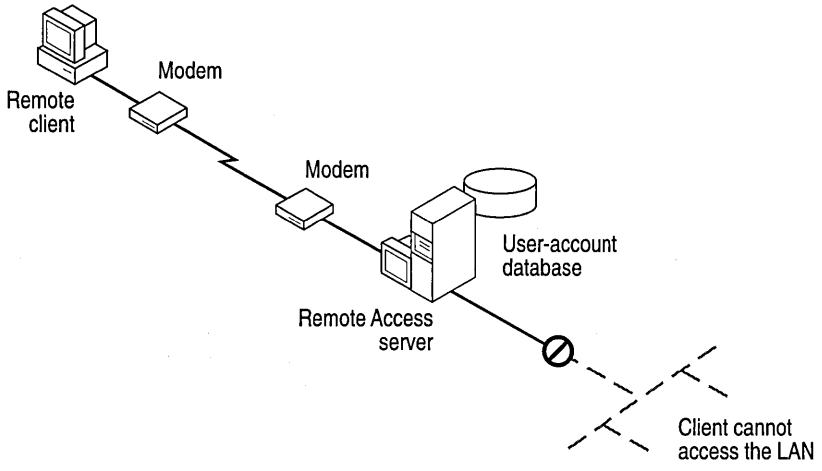


Figure 7.2 Remote Users Restricted to the Dial-In Server

How Security Works at Connection

The following steps show what happens during a call from a client to a RAS server:

1. Through Dial-Up Networking, a client dials a Remote Access server.
2. The server sends a challenge to the client.
3. The client sends an encrypted response to the server.
4. The server checks the response against the user database.
5. If the account is valid, the server checks for Remote Access permission.
6. If Remote Access permission has been granted, the server connects the client.

If callback is enabled, the server calls the client back and repeats steps 2–6.

Note When using RAS in a domain environment, changes in Remote Access permission do not take effect immediately on all servers. It can take up to 15 minutes for replication of the change to other servers in the domain. If necessary, you can resynchronize the domain to ensure that a user with revoked permissions cannot gain access to the network before the change is automatically replicated.

Security Features

RAS security features include password encryption using different forms of authentication protocols, data encryption to maintain security in case of unauthorized interception of remote access transmissions, and callback security to predetermine a client's number before allowing access to the network.

Authentication

Authentication is an important concern for many corporations. This section shows how RAS helps ensure password privacy.

Authentication Protocols

RAS uses the Challenge Handshake Authentication Protocol (CHAP) to negotiate the most secure form of encrypted authentication supported by both server and client. CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP allows the RAS server to negotiate downward from the most-secure to the least-secure encryption mechanism, and it protects passwords transmitted in the process.

Table 7.1 Security Levels and RAS Encryption Protocols

Level of security	Type of encryption	RAS encryption protocol
High	One-way	CHAP, MD5
Medium	Two-way	SPAP
Low	Clear-text	PAP

CHAP allows different types of encryption algorithms to be used. Specifically, RAS uses DES and RSA Security Inc.'s MD5. Microsoft RAS uses DES encryption when both the client and the server are using RAS. DES encryption—the U.S. government standard—was designed to protect against password discovery and playback. Windows NT 3.5 or later, Windows for Workgroups, and Windows 95 *always* negotiate DES-encrypted authentication when communicating with each other. When connecting to third-party remote access servers or client software, RAS can negotiate SPAP or clear-text authentication if the third party product does not support encrypted authentication.

MD5, an encryption scheme used by various PPP vendors for encrypted authentication, can be negotiated by the Microsoft RAS client when connecting to other vendors' remote access servers. MD5 is not available in the RAS server.

The Shiva Password Authentication Protocol (SPAP) is a two-way (reversible) encryption mechanism employed by Shiva. Windows NT Workstation, when connecting to a Shiva LAN Rover, uses SPAP, as does a Shiva client connecting to a Windows NT Server. This form of authentication is more secure than clear text but less secure than CHAP.

Password Authentication Protocol (PAP) uses clear-text passwords and is the least sophisticated authentication protocol. It is typically negotiated if the remote workstation and server cannot negotiate a more secure form of validation.

The Microsoft RAS server has an option that prevents clear-text passwords from being negotiated. This option enables system administrators to enforce a high level of security.

Data Encryption

Data encryption protects data and ensures secure dial-up communications. This is especially important for financial institutions, law-enforcement and government agencies, and corporations that require secure data transfer. For installations where total security is required, the RAS administrator can set the RAS server to force encrypted communications. Users connecting to that server automatically encrypt all data sent.

RAS provides data encryption in addition to password encryption as described in the "Authentication" section. To maintain security in case of unauthorized interception of remote access transmissions, clients configure each Phonebook entry to use data encryption. Windows NT RAS provides data encryption using the RSA™ Data Security Incorporated RC4 algorithm.

Callback

As an additional measure of security, RAS offers a Callback feature, which ensures that only users from specific locations can access the RAS server. It also saves toll charges for the user.

When using call back, the user initiates a call and connects with the RAS server. The RAS server then drops the call and calls back a moment later to the pre-assigned call-back number. This security method thwarts most impersonators.

You configure each user's callback privilege when granting Remote Access permission. For information about granting permission, see Chapter 6, "Installing and Configuring Remote Access Service" and online help for Remote Access Admin.

In Remote Access Admin, the **Remote Access Permissions** dialog box contains three callback options to choose from:

- **Preset To**
- **Set By Caller**
- **No Callback** (the default)

Note Until the user has been authenticated and called back (if Callback is set), no data from the remote client or the Remote Access server is transferred.

Preset To

For maximum security, select **Preset To** and type the number of the phone to which the user's modem is connected. When the user's call reaches the Remote Access server, the server takes the following steps:

1. Determines whether the user name and password are correct.
2. If they are, responds with a message announcing that the user will be called back.
3. Disconnects and calls the user back at the preset number.

Set this option for stationary remote computers, such as those in home offices.

Set By Caller

Although **Set By Caller** is not really a security feature, it is useful for clients who call from various locations and phone numbers. It also minimizes telephone charges for these users. When the user's call reaches the Remote Access server, the following events occur:

1. The server first determines if the user name and password are correct.
2. If they are, the Callback dialog box appears on the user's computer.
3. The user types the current callback number in the dialog box and waits for the server to return the call.

No Callback

If the user account has not been configured for callback, RAS establishes a connection as soon as the user's name and password is authenticated.

Support for Security Hosts and Switches

RAS supports various kinds of *intermediary devices* (security hosts and switches) between the Remote Access client and the Remote Access server. These devices include

- Modem-pool switch
- Security host
- X.25 network

Figure 7.2 shows a sample configuration incorporating a modem pool and a security host.

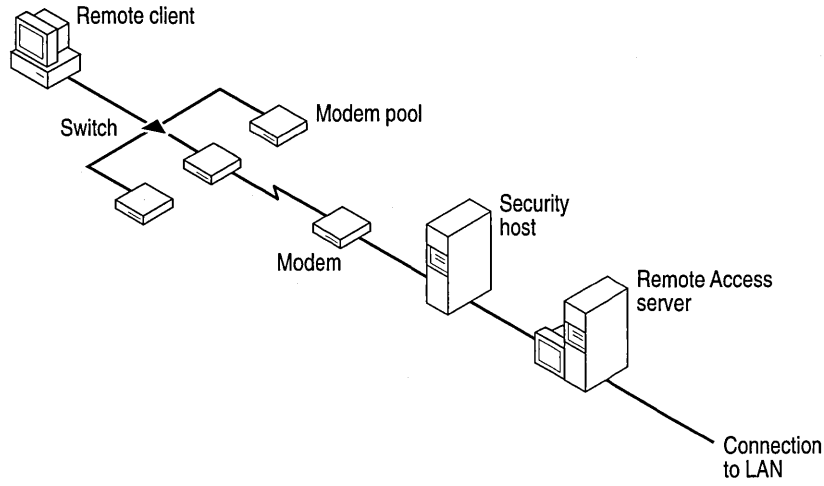


Figure 7.2 Sample Configuration with Modem Pool and Security Host

Connecting Through Intermediary Devices

Before connecting to the Remote Access server, a client can have one of two possible dialogs (user input and computer response screens) with each intermediary device:

Static (a dialog that's always the same and requires no input from the user)

Interactive (a dialog that always changes, requiring input from the user)

You must configure the client to work with each intermediary device.

If you require both static and interactive dialogs, you must take two steps:

1. Write a script for the static dialog. (See the next section, "Writing Scripts.")
2. Activate terminal mode for the interactive dialogs. (See "Activating Terminal Mode on the Client," later in this chapter.)

If you require only one kind of dialog, take only one of the above steps. For example

- If your clients connect through only one intermediary with a static dialog (such as an X.25 network), skip step 2.
- If your clients connect through a security host with an interactive dialog, skip step 1.

Writing Scripts

Figure 7.3 is an example of when two dialogs are required: Preconnect (a modem-pool switch) and postconnect (a security host). Although preconnect and postconnect dialogs can be either static or interactive, the preconnect dialog is normally static and the postconnect is normally interactive.

With static dialogs, the user selects from the **Switch** dialog box a user-written custom script. With interactive dialogs, the user selects Terminal from the **Switch** dialog box.

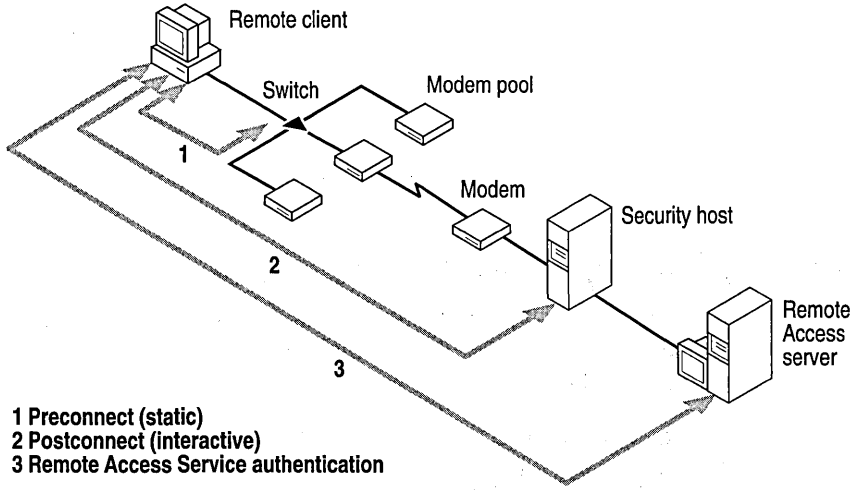


Figure 7.3 Sample Dialogs Between Client and Intermediary Devices

The SWITCH.INF file included in Windows NT provides a generic script that will probably work with little or no modification when connecting to many PPP servers. Try to connect using the generic script. If that does not work, you can copy—then modify—the generic script to match the logon sequence of the remote computer you want to connect to.

For more information about how to write scripts, see Chapter 10 "Logging on to Remote Computers Using RAS Terminal and Scripts."

Security Hosts

A *security host* is a third-party authentication device that verifies whether a caller from a remote client is authorized to connect to the Remote Access server. This verification supplements security already supplied by RAS and by Windows NT Server.

The security host sits between the remote user and the RAS Server. The security host generally provides an extra layer of security by requiring a hardware key of some sort in order to provide authentication. Verification that the remote user is in physical possession of the key takes place before access to the RAS Server is granted. This open architecture allows customers to choose from a variety of security hosts to augment the security in RAS.

For example, one kind of security system consists of two hardware devices: the security host and the security card. The *security host* is installed between the Remote Access server and its modem. The *security card* is a small unit the size of a credit card, resembling a pocket calculator without keys. The security card displays a different access number every minute. This number is synchronized with the same number calculated in the security host every minute. When connecting, the remote user sends the number on the security card to the host. If the number is correct, the security host connects the remote user with the Remote Access server.

Another kind of security host prompts the remote user to type in a username (which may or may not be the same as the Remote Access username) and a password (which differs from the Remote Access password).

The security host must be configured to allow the RAS server to initialize the modem before the security functions take effect. The RAS server must also be able to directly initialize the modem connected to the security host without security checks from the security host. The security host might interpret the RAS server's attempt to initialize the modem as an attempt to dial out.

You should also set up the host for a fixed bits-per-second (bps) speed rather than autobaud. The fixed bps should equal the value of the **MAXCONNECTBPS** parameter for the entry you created for this device in the Modem.inf file.

▶ **To make third-party security devices work with the Remote Access Service**

1. If the Remote Access server's modem is different from the modem in the security host's section in Modem.inf, the Modem.inf file on the Remote Access server needs to be customized to link the security host to the server's modem.
2. The remote user must activate Terminal mode to interact with the security host.

Note To use a Security Dynamics security host, you must order two connectors through your Security Dynamics provider to permit initialization of the RAS modem. When you order, specify that you want the dial-out option. The provider will then send you an AND gate and a jumper box. For the ACM/400 security host, you will also receive different software.

Customizing the Remote Access Server's Modem.inf

When you install a security host between the Remote Access server and its modem(s), the server's modem and the security host act together as a new type of modem. The Modem.inf file is shipped with a template for each supported security host paired with a particular modem. (For example, the ACM/400 is paired with an AT&T® Comsphere 3820 modem.)

To use the security host with a different modem, you must modify the Modem.inf file. For details about customizing Modem.inf, see the RAS online Help or see Appendix C, "Understanding Modem.inf."

Activating Terminal Mode on the Client

Remote Access Terminal lets the remote user send the correct access number to the security device. If the number is correct, the user is connected to the Remote Access server.

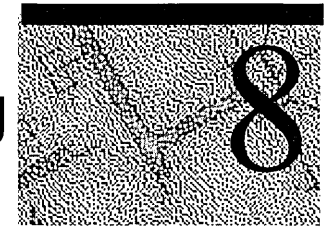
For information about how to prepare the client for Terminal mode or connect to the Remote Access server, see "Activating Terminal Mode on the Client" in online Help.

Auditing

RAS generates audit trails of remote connections. With this feature, you can audit all Remote Access activity using Windows NT Server Event Viewer to see whether network security is intact. You can also monitor servers and users with RAS Admin. For more information about audits and monitoring, see Chapter 8, "Maintenance and Troubleshooting."

CHAPTER 8

Maintenance and Troubleshooting



After you have installed RAS, routine maintenance consists of the following tasks:

- Monitoring servers and users systematically with Remote Access Administrator.
- Reviewing the Windows NT Server Event Viewer regularly to see whether network security is intact. (See "Troubleshooting" and "Audits" later in this chapter. For complete information about using Event Viewer, see *Windows NT Server Concepts and Planning*.)
- Viewing status and connection information with Dial-Up Networking Monitor.

By conveying real-time information about users, ports, modems, and data transmissions, the Remote Access Administrator's utility simplifies the monitoring of servers and users and provides valuable clues that assist in troubleshooting. By running the utility continuously, you can track activity on your Remote Access servers and respond promptly to problems with user accounts and hardware.

With the Remote Access Administrator's utility, you can look at two aspects of a Remote Access Service domain:

- The Remote Access servers in a domain. This view of the domain lets you manage multiple Remote Access servers from a central location.
- All users connected to those Remote Access servers.

  This view lets you monitor user activity on all Remote Access servers in the domain.

The Remote Access Admin window shows a single RAS server or all RAS servers in a domain. The default view is whatever you last viewed. You can change the focus to a different domain, or you can focus on a single server in the current domain.

The Remote Access Administrator utility requires the user to be logged on as an Administrator.

Troubleshooting

The Administrator's utility provides real-time information about active users and current connections and is often the best place to begin troubleshooting. Consider the following examples that put the utility to use:

- The Remote Access Admin window might show that fewer ports than expected are in constant use on a server. This suggests that one or more of them might not be operating properly.
- If users cannot make a connection, ask them to attempt to reconnect while you monitor their efforts in the **Port Status** dialog box.

When real-time data is insufficient to solve a problem, refer to the audit and error messages generated by Remote Access. The Windows NT Server Event Viewer records all audits and error messages for Remote Access.

Events are classified into three categories:

Event	Description
Audit	Normal behavior recorded for administration, for example, information about a connected client—user name, connection time, and current status.
Warning	An irregular or unexpected condition that doesn't affect the system's functionality.
Error	A major function fails or a network error occurs.

Audits are further divided into two categories:

Category of Audit	Example
Success audit	Client connects and disconnects normally.
Failure audit	Server disconnects a client that's been inactive too long, or a client tries to connect with the wrong password.

Note For a list of error messages and what they mean, see the online Help topic, "Error Messages." For a list of idiosyncrasies in modems supported by RAS see the online Help topic, "Modem Idiosyncrasies."

Audits

The Windows NT Server Event Viewer records activity on each Remote Access server. Because audits recorded in the log are the best evidence of possible attempts to violate network security, you should review them regularly. For information about using Event Viewer, see *Windows NT Server Concepts and Planning*.

To enable audits, make sure the **EnableAudit** parameter is set to the default value of 1. For more information, see Appendix A, "RAS Registry Values."

The Remote Access Service generates, among others, the following audit records:

Success Audits

Message	Explanation
The user *username* has connected and has been successfully authenticated on port *portname*.	This message signifies a normal connection by a certain user on a given port.
User *username* has disconnected from port *portname*.	This message records a successful disconnection initiated by the user.
The user *domainname\username* on port *number* was called back at the number *callback number*.	This records a successful callback to a user at the specified phone number.

Failure Audits

Message	Explanation
The user connected to port *portname* has been disconnected due to inactivity.	The line was idle for a period longer than configured using the **AutoDisconnect** parameter in the Registry.
The user has connected and failed to authenticate on port *portname*. The line has been disconnected.	The user supplied an incorrect username, password, or both. The number of failed authentications before access is denied and the line is dropped depends on the value of the **AuthenticateRetries** parameter in the Registry.

(continued)

Message	Explanation
The user connected to port *portname* has been disconnected due to authentication timeout.	Authentication took longer than the value set for timing out. You might need to increase the value of the **AuthenticateTime** parameter. See "Remote Access Parameters" in Appendix A, "RAS Registry Values."
The user connected to port *portname* has been disconnected because of a transport-level error during the authentication conversation.	Too many errors occurred during the authentication conversation, possibly because of noisy lines or incompatible modems. Ask the user to try connecting with a lower initial speed.
The user connected to port *portname* has been disconnected because the port could not be projected onto the network.	Most likely the user's computer name already exists on the network. Ask the user to configure the remote computer with a different computer name or to make sure the computer is not already connected to the network through another means, such as the Ethernet or token ring.

Note If the Remote Access Service fails to start, check Event Viewer for a description of the error that occurred. For information about using Event Viewer, see *Windows NT Server Concepts and Planning*. After you find the error, look it up in the online error messages Help file on the *Windows NT Server Resource Kit CD*, and take the recommended corrective action.

Client Problems

Because client problems usually stem from improper hardware or software configuration on the computer, first check the error message and audit logs for clues. If this doesn't help, see "Answers to Common Questions" in the Remote Access online Help.

RAS-Specific Logs

To enable two RAS-specific logs (the PPP log and the device log), change parameters in the Registry. These logs are text files and can be viewed in any text editor or at the command prompt. They cannot be viewed using Event Viewer.

The PPP Log

When enabled, the PPP log records all PPP events in the file *\systemroot*\SYSTEM32\RAS\PPP.LOG. This log file can help you determine problems with PPP connections. To enable the PPP log, go to the following key and change the Logging parameter to *1*:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP
```

The Device Log

When enabled, the device log is created in the file *\systemroot*\SYSTEM32\RAS \DEVICE.LOG. The device log records all communication from serial ports to the device connected to them during command mode. Logging stops after successful connection to the device and after data is transmitted. To enable the device log, go to the following key and change the Logging parameter to *1*:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
```

For more information about enabling these logs, see Appendix A, "RAS Registry Values."

Status Reporting

The Dial-Up Networking Monitor (located in Control Panel) provides the status of a call, and allows you to see

- the speed at which you connected
- the duration of the connection
- the names of users connected to a RAS server
- protocols used during the connection
- which devices are part of a connection

You also use the Dial-Up Networking Monitor to hang-up active connections. If you have Multilink connections, you can hang up a specific device if you want to use it for another call.

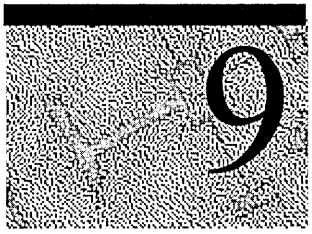
By default, the Dial-Up Networking Monitor appears on the taskbar as you dial out. Use the Preferences tab to change the view and configure it to appear as window. The Dial-Up Networking Monitor displays lights to indicate traffic over dial-up lines: A button flashes blue when sending or receiving data, and a button flashes red when an error occurs.

Also, when Dial-Up Monitor is viewed as a window, you can configure it to show rows of lights for multiple devices. To do this, in the **Preferences** tab, click **Lights**.

For detailed information on the dialog box properties, see online Help.

CHAPTER 9

X.25 PAD Support



An X.25 network uses a packet-switching protocol to transmit data. This protocol relies on an elaborate worldwide network of packet-forwarding nodes (Data Communications Equipment [DCEs]) that participate in delivering an X.25 packet to its designated address.

Dial-up Asynchronous Packet Assemblers/Disassemblers (PADs) constitute a practical choice for Remote Access clients because they don't require an X.25 line to be plugged into the back of the computer. Their only requirement is the telephone number of the PAD service for the carrier.

Note This chapter is specific to X.25 PADs. X.25 cards can also be supported through WAN miniport drivers.

The Remote Access Service lets you access the X.25 network in two general ways:

Server/Client	Method of access
Client (for the Windows™ or Windows NT operating systems)	Asynchronous Packet Assemblers/Disassemblers (PADs)
Server and client (for Windows NT systems only)	Direct connections

The next section tells how to access the X.25 network in both ways for specific configurations.

X.25 Configurations

The Remote Access Service for X.25 networks offers two configurations for the client and one for the server:

Table 9.1 X.25 Configurations

Client/Server	Configuration
Client	Dial-up PAD
Client	Direct connection to the X.25 network through X.25 smart card
Server	Direct connection to the X.25 network through X.25 smart card

Pad.inf Format

Similar in format to Modem.inf (which contains script information used to talk to the modem), Pad.inf contains conversations between the client software and the PAD. For details, see Appendix C, "Understanding Modem.inf." Pad.inf is located in the *\systemroot*\SYSTEM32\RAS folder.

The macros in the following list are *reserved words*, which you cannot define in Pad.inf to create a new entry. Reserved words are case insensitive.

- **x25address**
- **diagnostics**
- **userdata**
- **facilities**

Caution Using reserved words as macro names in Pad.inf could result in unpredictable behavior of the Remote Access software.

Sample Pad.inf

The following sample Pad.inf file will help you create a section within Pad.inf for your X.25 network. This example shows an entry for Sprintnet:

```
[SPRINTNET]

;The following three lines are temporary.
DEFAULTOFF=
MAXCARRIERBPS=9600
MAXCONNECTBPS=9600

; The next line will give a delay of 2 secs -
; allowing the PAD to initialize
```

```
COMMAND=
NoResponse

COMMAND=
NoResponse

; The @ character sets the SPRINTNET PAD for 8 databit communication.
COMMAND=@
NoResponse

COMMAND=
NoResponse

; The D character requests a 9600 speed.
COMMAND=D<cr>
; We don't care for the response so we ignore it.
OK=<ignore>

; A carriage return line feed again to initialize
; the PAD read/write buffers
COMMAND=<cr><lf>
OK=<ignore>

COMMAND=<cr><lf>
OK=<ignore>

; Set X.3 settings on the PAD which make it work well with RAS.
; Broken into two parts since the line is too long.
COMMAND=SET 1:0,2:0,3:0,4:1,5:0,6:1,7:0,8:0,9:0,10:0,11:0<cr>
OK=<ignore>

; Set the other half of X.3 parameters
COMMAND=SET 12:0,13:0,14:0,15:0,16:0,17:0,18:0,19:0,20:0,21:0,22:0<cr>
OK=<ignore>

; Finally try to call RAS X25 server
COMMAND=C <x25address><cr><lf>

CONNECT=<match>"CONNECT"
ERROR_DIAGNOSTICS=<cr><lf><Diagnostics>

; CONNECT response means that the connection completed fine.
; X25ERROR response means connection attempt failed - the X25 CAUSE and
; DIAGNOSTIC information will be extracted from the response and
; sent to the user.
; ERROR responses are for generic failures.
```

After this sample conversation for SPRINTNET is completed (with the correct responses), the X.25 connection is established. If errors are detected during the PAD conversation, no connection is made.

Note The Remote Access Service currently works with PADs set to 8 data bits, 1 stop bit, and no parity. Consult the documentation for the PAD to see how to install these settings.

In Pad.inf, you can use the **COMMAND_** series of commands (**COMMAND_INIT**, **COMMAND_DIAL**, and **COMMAND_LISTEN**) or the generic **COMMAND**. But do not mix the two families of commands. For more information on the **COMMAND_** series, see Appendix C, "Understanding Modem.inf."

Troubleshooting

For troubleshooting information, see the Remote Access online Help.

Accessing X.25 Through Dial-Up PADs

Operating between the client and the Remote Access server, an asynchronous PAD converts serially-transmitted data into X.25 packets. When the PAD receives a packet from an X.25 network, it puts the packet out on a serial line, making communication possible between the client and the X.25 network.

Remote Access clients can connect with Remote Access servers through dial-up PAD services supplied by X.25 carriers, such as Sprintnet and Infonet. After the client's modem (modem A in Figure 9.1) connects to the PAD's modem (modem B), the client software must converse with the dial-up PAD. When their conversation is successfully completed, a connection is established between client and server. The conversation (command/response scripts) for the PADs supported by an X.25 carrier is stored in the Pad.inf file. Remote Access software supplies one example. To customize your PAD, see "Pad.inf Format," in this chapter.

For example, Pad.inf contains two Sprintnet entries: Sprintnet Standard and Sprintnet Alternate. Generally, if you are calling through 9600 bits-per-second (bps) or faster dial-up PADs, try Sprintnet Standard. If you are calling through 2400 bps or slower dial-up PADs, try Sprintnet Alternate.

If one Sprintnet entry fails to connect reliably, try the other one. Sprintnet dial-up PADs should work with both.

Note For dial-up PADs, you must use the **COMMAND=** format, not the **COMMAND_INIT**, **COMMAND_DIAL**, and **COMMAND_LISTEN** format.

Figure 9.1 shows how a client connects to the Remote Access server through a dial-up PAD and the X.25 network.

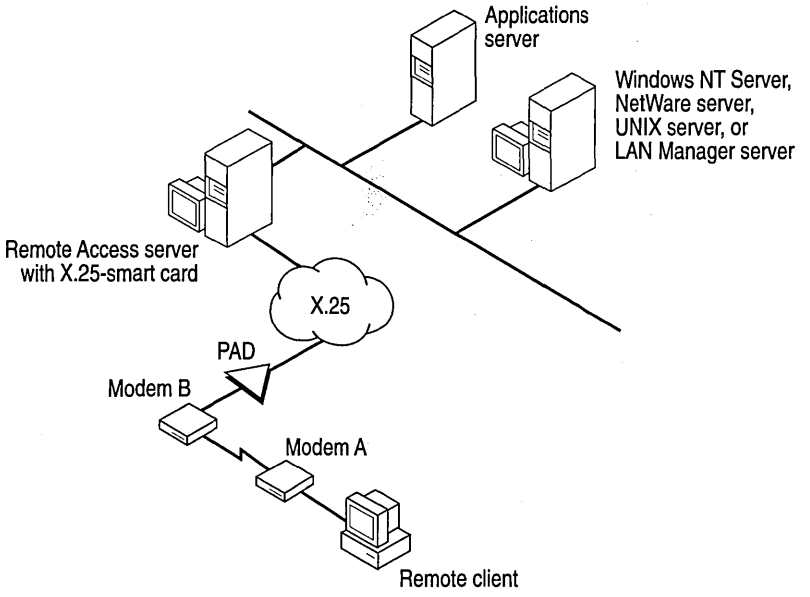


Figure 9.1 Connecting to the Server Through a Dial-Up PAD

Note For best results when using a dial-up PAD, use a modem that matches the one used by the PAD carrier (or at least matches the V. protocol supported by the carrier's modem).

The following table compares connecting through dial-up PADs and connecting directly to the X.25 network:

Table9.2 Comparison of Dial-Up PADs to Connecting Directly

Dial-Up PAD	Direct connection
Saves the expense of a dedicated leased line (direct connection).	Requires expensive leased line.
Allows connections from hotels, airports, homes—anywhere a phone line is available.	Requires users to dial in from a fixed location.
Requires two steps to connect.	Connects conveniently in one step.

(continued)

Table9.3 Comparison of Dial-Up PADs to Connecting Directly

Dial-Up PAD	Direct connection
Limits maximum communication speed to whichever speed is slower, the modem's or the PAD's.	Lets communication take place up to the speed of a leased line, 56 kilobytes (K).
Allows less control in configuring PADs.	Offers greater reliability.
Only a client can connect through a dial-up PAD.	Both servers and clients can connect directly.

PAD and Serial Configuration

To configure your PAD correctly, set the X.3 parameters according to the information shown in Table 9.3 later in this chapter.

The configuration of the dial-up PAD should be as follows:

- 8 data bits
- 1 stop bit
- No parity serial communication

For dial-up PADs, make sure your vendor supports this configuration. The PADs might already be set to the correct configuration for connecting directly through an internal X.25 smart card. If they are, do not change the configuration.

Connecting to the X.25 Network Directly

RAS also supports connecting directly from the remote computer to the X.25 network through a smart card, which acts like a modem. An *X.25 smart card* is a hardware card with a PAD embedded in it. To the personal computer, a smart card looks like several communication ports attached to PADs. To access the X.25 network through a direct connection, you must have

- a direct line connection to an X.25 network (clients only)
- a smart card

Note The server side always requires an X.25 smart card, but the client side requires one only when connecting to the X.25 network directly.

Note For connecting to the network directly, you must use the **COMMAND_INIT**, **COMMAND_DIAL**, and **COMMAND_LISTEN** format.

Figure 9.2 shows how the server and a Windows NT client (both equipped with smart cards) connect to the X.25 network directly.

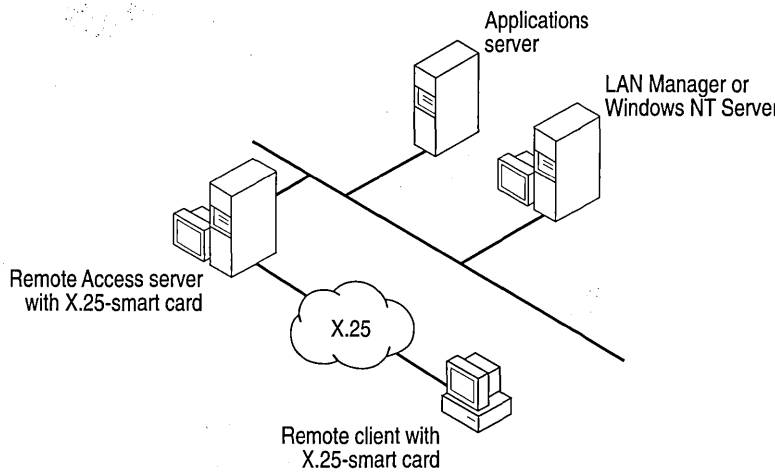


Figure 9.2 Connecting to X.25 Directly

Callback

The Remote Access server does not support callback on X.25 networks.

Setting Up the Remote Access Server for an X.25 Network

After installing Windows NT Server and adding the Remote Access Service, follow these steps:

▶ **To set up the Remote Access server for an X.25 network**

1. Install the X.25 smart card (according to the manufacturer's instructions).

   A communications driver for the X.25 smart card that emulates communication ports is supplied by the hardware manufacturer or by a third party.
2. Make sure your X.25 smart card is configured with the X.3-parameter values shown in Table 9.3.
3. From the list of devices on the **Remote Access Setup** dialog box, select an entry corresponding to the X.25 smart card.
4. In setting up the Remote Access server, make sure that the ports selected are configured for dial-in.

Note Make sure that the speed of the leased line can support all the serial communication (COM) ports at all speeds at which clients will dial in. For example, 4 clients connecting at 9600 bps (through dial-up PADs) will require a 38,400-bps (4 times 9600) leased line on the server end. If the leased line does not have adequate bandwidth, it can cause time-outs and can cause the performance for connected clients to degrade.

Table 9.3 X.25 Configuration Values

Parameter number	X.3 parameter	Value
1	PAD Recall	0
2	Echo	0
3	Data Fwd. Char	0
4	Idle Timer	1
5	Device Ctrl	0
6	PAD Service Signals	1
7	Break Signal	0
8	Discard Output	0
9	Padding after CR	0
10	Line Folding	0
11	*Not Set*	
12	Flow Control	0
13	Linefeed Insertion	0
14	Padding after LF	0
15	Editing	0
16	Character Delete	0
17	Line Delete	0
18	Line Display	0
19	Editing PAD Srv Signals	0
20	Echo Mask	0
21	Parity Treatment	0
22	Page Wait	0

Caution Failure to set these values as shown prevents the Remote Access Service from functioning properly. For information on setting these values, see the instructions with your X.25 smart card.

Setting Up Remote Access Clients

This section tells how to set up Remote Access clients for connecting to the X.25 network through PAD services and for connecting to the X.25 network directly.

Connecting Through Dial-Up PADs

Following these steps to connect a client to an X.25 network:

1. Dial from the client's modem to a PAD (modem-to-modem).
2. Establish a connection over the X.25 network between the PAD and the server-side X.25 smart card.

After you've established a connection, communicate as you would through any asynchronous connection. For a complete description of connecting through dial-up PADs, see "Accessing X.25 Through Dial-Up PADs," earlier in this chapter.

Configuring Client PADs

The client PAD, through which a remote computer connects to the X.25 network, might have previously been set to X.3-parameter values that are incompatible with the Remote Access Service. Therefore, it is important to configure the X.25 smart card on the Remote Access server so that it changes the client PAD's X.3 settings to the values in Table 9.3 as soon as a connection is established through X.29 commands. To configure an X.25 smart card to make these changes, see the configuration manual for your specific card.

Note If the X.25 smart card on the server end does not support commands for the X.29 language, the client PAD script must set the X.3 parameters locally. If you have problems, contact the support site for your X.25 smart card vendor.

Connecting Directly

To set up the client for connecting directly to the X.25 network, follow the procedures used in setting up the Remote Access server. See "Setting Up the Remote Access Server for an X.25 Network," earlier in this chapter. Make sure the communication ports are selected as dial-out.

Configuring Remote Access Software for X.25

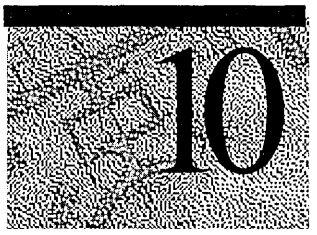
Connecting to a server through an X.25 network is similar to connecting through a phone line. The only difference is that the phone book entry must specify an X.25 PAD type and an X.121 address.

▶ **To add a phone book entry with X.25 or to add X.25 to an existing entry**

- See RAS online Help. This online Help also provides troubleshooting information.

CHAPTER 10

Logging on to Remote Computers using RAS Terminal and Scripts



The exact logon process for remote computers varies as widely as the remote computers themselves. Remote computers you might log on to include a Windows Remote Access Service (RAS) server giving you access to your corporate network or the Internet, a UNIX computer in a commercial network that gives you an Internet connection, or a proprietary security computer that protects your corporate network from intruders.

Most remote logons require you to provide a username (frequently called *login*) and a password. This chapter covers how you provide the username, password, and any other information required by remote computers before you log on.

This chapter also describes how to connect to Microsoft, Point-to-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP) servers, when and how to use RAS Terminal, how to create and activate scripts that automate remote logons, and how to debug your scripts. Most of the information regarding Terminal screens, scripts, and Device.log also applies to RAS for Windows for Workgroups version 3.11. However, the PPP, SLIP, and <username> and <password> macro information does not apply.

Connecting to Remote Servers

The three most common remote connections are to

- Microsoft RAS servers(including LAN Manager 2.1, Windows for Workgroups 3.11 with server extension, Windows NT 3.1 or later, and Windows 95)
- Non-Microsoft PPP servers
- SLIP servers

Microsoft RAS Servers

Connecting to a Microsoft RAS server is a simple process that uses the credentials specified when you logged on to Windows NT. If you use Windows NT RAS to connect to computers that are not running Windows NT RAS, the remote computer might require a specific sequence of commands and responses through a terminal window to successfully log you on to the remote system.

If the client is a Windows NT computer and the remote server is any Microsoft RAS server, logon is completely automated using Windows NT security.

PPP Servers

Point-to-point protocol (PPP) is a newer protocol used to negotiate connections between remote computers. Remote server and client software that supports PPP authentication protocols automatically negotiate network and authentication settings. The following steps are necessary to connect to a PPP server:

- In Dial-Up Networking application, edit an entry and choose the Server tab. In the **Dial-up server type** box, select PPP. This is the default selection.
- If the server you are calling requires a text-based logon exchange, choose the Script tab and select the **Pop up a terminal window** option. Now, during the connect sequence, you will see a terminal dialog that allows you to perform the text-based logon exchange.

The PPP standard provides for fully automated authentication using encrypted or clear-text authentication protocols. Some PPP providers do not implement the PPP authentication protocols; instead they require a text-based exchange prior to starting PPP.

To automate the text-based exchange, use a Switch.inf script instead of the clear-text logon dialog. For more information see "Automating Remote Logons Using Switch.inf Scripts," "Activating Switch.inf Scripts," and "Troubleshooting Scripts Using Device.log" later in this chapter.

SLIP Servers

Serial Line Internet Protocol (SLIP) is an older protocol that does not support authentation as part of the protocol. SLIP connections typically rely on text-based logon sessions. Encryption and automatic network parameter negotiations are not supported. The following steps are important when you are connecting to a SLIP server:

- In Dial-Up Networking, edit a Phonebook entry and choose the **Server** tab. In the **Dial-up server type** box, select SLIP.
- If the server you are calling requires a text-based logon exchange, choose the **Script** tab and select the **Pop up a terminal window** option. Now, during the connect sequence, you will see a terminal dialog that allows you to perform the text-based logon exchange.

To automate the text-based exchange, use a Switch.inf script instead of the clear-text logon dialog. For more information see "Automating Remote Logons Using Switch.inf Scripts," "Activating Switch.inf Scripts," and "Troubleshooting Scripts Using Device.log" later in this chapter.

Note Although Windows NT RAS is not a SLIP server, Windows NT RAS clients can *connect* to SLIP servers.

Using RAS Terminal for Remote Logons

For a PPP or SLIP server, if the remote computer you dial in to requires that you log on with a terminal screen, you must configure the Script settings for that RAS entry to use a *RAS Terminal logon.* With such a logon, after RAS connects to the remote system, a character-based window displays the logon sequence from the remote computer. You use this window to interact with the remote computer for logging on. Alternatively, you can automate this manual logon as described in the section, "Automating Remote Logons Using Switch.inf Scripts."

Some commercial networks will present a large menu of available services before you log on. On old, established SLIP servers, you might go through an extensive sequence of commands that updates files, collects data about you, or configures your SLIP connection during your logon process. On a new PPP server, you might be prompted for only your username and password before you are given a connection.

Note If the remote computer is a Microsoft RAS server, you do not need to use a terminal logon. Instead, logon is completely automated for you.

▶ **To configure a Windows NT RAS entry to use RAS Terminal after dialing**

1. In Dial-Up Networking, select the entry to which you want to connect.
2. Click **More** and choose **Edit entry and modem settings**.
3. In the **Script** tab, choose the **Pop up a terminal window** option.
4. Click **OK** and then click **Dial**.

After you dial and connect to this entry, the After Dial Terminal window appears, and you will see prompts from the remote computer. You then log on to the remote computer using the After Dial Terminal window. After you have completed all interactions with the remote computer, click **Done**.

If the logon sequence does not vary, you can write a script that automatically passes information to the remote computer during the logon sequence, enabling completely automatic connections.

For more information see "Automating Remote Logons Using Switch.inf Scripts," "Activating Switch.inf Scripts," and "Troubleshooting Scripts Using Device.log" later in this chapter.

Automating Remote Logons Using Switch.inf Scripts

To automate the logon process, you can use the Switch.inf file (or Pad.inf on X.25 networks) instead of the manual RAS Terminal window described in the "Using RAS Terminal for Remote Logons" section.

Automated scripts are especially useful when a constant connection to a remote computer is needed. If the RAS entry is configured to use a script, and if a remote connection fails, RAS automatically redials the number and reestablishes the connection. Scripts also save time if you frequently log on to a remote system and do not want to manually log on each time.

The Switch.inf file provides a generic script that will probably work with little or no modification. Try it first and if it does not work, copy and modify the generic script to match the logon sequence of the remote computer you want to connect to.

Note The script language described in this chapter was also designed to communicate with other devices, including modems. If you are unfamiliar with modem scripts, scripting can be difficult to understand. The following section explains how to create scripts, although you will probably find it easiest to copy, then modify, one of the generic sample scripts.

Creating Scripts for RAS

The Switch.inf file, located in the *systemroot*\SYSTEM32\RAS folder, is like a set of small batch files (scripts) contained in one file. The Switch.inf file contains a different script for each intermediary device or online service that the RAS user will call.

A Switch.inf script has six elements: a section header, comments, commands, responses, response keywords, and macros.

Section Headers

Section headers divide the Switch.inf file into individual scripts. A section header marks the beginning of a script for a certain remote computer and must not exceed 31 characters. The text of a section header will appear in RAS when you activate the script. The section header is enclosed in square brackets. For example:

```
[Route 66 Logon]
```

Comment Lines

Comment lines must have a semicolon (;) in column one and can appear anywhere in the file. Comment lines contain information for those who maintain the Switch.inf file. For example:

```
; This script was created by MariaG on September 29, 1996
```

Commands

Each line in a script is a command from your local computer to the remote computer or a response from the remote computer to your local computer. Each command or response is a stream of data or text. For example, the following command sends a username (MariaG) and a carriage return (the macro **<cr>**) to the remote computer.

COMMAND=MariaG<cr>

The commands and responses must be in the exact order the remote device expects them. Branching statements, such as GOTO or IF, are not supported.

The required sequence of commands and responses for a specific remote device should be in the documentation for the device or, if you are connecting to a commercial service, from the support staff of that service. If the exact sequence is not available, activate the generic script provided with RAS and modify it to match the logon sequence of the remote computer as described in the "Troubleshooting Scripts Using Device.log" section.

The COMMAND= statement can be used in two additional ways:

```
COMMAND=
NoResponse
```

This is the default behavior and causes an approximate two-second delay. This can be useful when the intermediate device requires a delay.

```
COMMAND= string
```

Note *string* is not followed by a carriage return (<cr>). This is useful when a device requires slow input. Instead of receiving the whole command string, the device requires characters to be sent one-by-one.

The following is an example in which the intermediary device is so slow that it is able to receive and process only one character of the command PPP at a time:

```
COMMAND=P
NoResponse

COMMAND=P
NoResponse

COMMAND=P
NoResponse
```

Response

A response is sent from the remote device or computer. To write an automatic script, you must know the responses you will receive from the remote device. If a gap of two or more seconds occurs between characters, the received text is sent as a response. This gap is the only cue that a response is over. For more information, see the following section, "Getting Through Large Blocks of Text and Two-Second Gaps."

Response Keywords

The keyword in a response line specifies what to do with the responses you receive from the remote computer:

OK=*remote computer response<macro>*
The script continues to the next line if the response or macro is encountered.

LOOP=*remote computer response<macro>*
The script returns to the previous line if the response or macro is encountered.

CONNECT=*remote computer response <macro>*
Used at the end of a successful modem script. Not generally useful for the Switch.inf file.

ERROR= *remote computer response <macro>*
Causes RAS to display a generic error message if the response is encountered. Useful for notifying the RAS user when the remote computer reports a specific error.

ERROR_DIAGNOSTICS= *remote computer response* **<diagnostics>**
Causes RAS to display the specific cause for an error returned by the device. Not all devices report specific errors. Use **ERROR=** if your device does not return specific errors that can be identified with Microsoft RAS diagnostics.

NoResponse
Used when no response will come from the remote device.

RAS on the local computer always expects a response from the remote device and will wait until a response is received unless a **NoResponse** statement follows the **COMMAND=** line. If there is no statement for a response following a **COMMAND=** line, the **COMMAND=** line will execute and stop the script at that point.

Macros

Macros are enclosed in angle brackets (<>) and perform a variety of special functions:

<cr>
Inserts a carriage return.

<lf>
Inserts a line feed.

<match> "*string*"
Reports a match if the string enclosed in quotation marks is found in the device response. Each character in the string is matched according to upper and lower case. For example, **<match>** "Smith" matches Jane Smith and John Smith III, but not SMITH.

<?>
Inserts a wildcard character, for example, **CO<?><?>2** matches COOL2 or COAT2, but not COOL3.

<hXX> (XX are hexadecimal digits)
Allows any hexadecimal character to appear in a string—including the zero byte, **<h00>**.

<ignore>
Ignores the rest of a response from the macro on.

<diagnostics>
Passes specific error information from a device to RAS. This enables RAS to display the specific error to RAS users. Otherwise, a nonspecific error message appears.

Authentication Macros

The following macros enable your username and password logon credentials to be automatically passed to the remote computer.

<username>
The username entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

<password>
The password entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

▶ **Your logon creditials will fail (and the Retry Authentication dialog box will appear) if both of the following occur**

- You call into a system that has an intermediary security device. (This situation would generally not apply if you are using RAS to call an Internet provider.)
- After the security device has logged you on successfully, you try to log on to a Windows NT RAS server.

  The dialog box appears because the RAS Authentication dialog box username and password boxes are used by the two new username and password macros as well as by Windows NT RAS servers.

  For example, if the logon information for an intermediary security device that is plugged in between the Windows NT RAS server and its modem is username: "BB318" and password: "34554377", but on the Windows NT RAS server it is username: "BB318" and password: "treehouse", then your logon to the intermediary device will succeed, but your logon to the Windows NT RAS server will fail.

  Logon will fail because the security device password of "34554377" is different from the Windows NT domain password. Windows NT will prompt you with the Retry Authentication dialog box to obtain your proper Windows NT logon credentials, in this case the password.

▶ **To eliminate the Retry Authentication dialog box**

- Ask your administrator to make your username and password identical on both systems. (Because this solution defeats the purpose of the security device, it is not recommended.)
- Do not use the shared dialog box for the intermediary device logon credentials: Enter the username and password in clear text into the Switch.inf file according to the [Generic login for YourLoginHere] script provided in Switch.inf. To keep your clear-text password confidential you must use Windows NT file system (NTFS) file permissions to prevent other users from accessing this file.

Stepping Through an Example Script

This section describes each part of the generic script provided in the Switch.inf file included with RAS.

Every script must start with a command to the remote computer, followed by one or more response lines. This initial command might be simply to wait for the remote computer to initialize and send its logon banner. The default initial command is to wait two seconds for the logon banner. It would look like this in the Switch.inf file:

COMMAND=

If the response, (the logon banner from the remote computer) is the following:

```
Welcome to Gibraltar Net. Please enter your login:
```

then the corresponding response line in the Switch.inf file should be:

OK=<match>"Please enter your login:"

This line indicates that everything is correct if the remote computer sends the string "Please enter your login:". You respond by sending a command with the characters in your username and the carriage return.

COMMAND=MariaG<cr>

If the response from the remote computer is the following:

```
Please enter your password:
```

then the corresponding response line in the Switch.inf file should be:

OK=<match>"Please enter your password:"

To send your password, you would send the command:

COMMAND=mUs3naB<cr>

On many PPP computers, this script would automatically log you on.

Automating Log On to SLIP Computers

If your SLIP provider assigns you the same IP address every time you call, you can fully automate your SLIP connection by entering that address in the **SLIP TCP/IP Settings** dialog box.

If you are assigned a different IP address every time you call, then even though you can automate much of the logon sequence, you must manually enter your IP address in the SLIP terminal window.

Getting Through Large Blocks of Text and Two Second Gaps

If the remote computer has a two-second gap in the data stream reponse to your computer, RAS assumes that the gap is the end of the response. These gaps can occur anywhere—even between words—and can only be detected using Device.log. For more information, see the "Troubleshooting Scripts Using Device.log" section later in this chapter.

If you write a script that seems to fail for no reason, consult Device.log to see if a response ends in the middle of a word. If it does, your script must account for the two-second gap. A simple way to do this is to include the following command:

COMMAND=<cr>

You can skip to the end of large blocks of text that contain multiple gaps by using the **LOOP=** keyword and by matching text at the end of a block. For example,

COMMAND=<cr>OK=<match>"Enter the service to start:"LOOP=<ignore>

In this example, RAS sends a null command (waits two seconds). RAS then waits for the message "Enter the service to start:". If this is a long block of text, RAS does not find the string, so RAS then moves to the **LOOP** command. The **LOOP** command causes RAS to return to the line above, and RAS waits for the words "Enter the service to start:" in the second response. In this manner, you can loop though long blocks of text until you reach the text of the desired prompt.

Commands and Carriage Returns

Usually, you must include **<cr>**, which indicates a carriage return, at the end of a command. The carriage return causes the remote computer to process the command immediately. If you do not include **<cr>**, the remote computer might not recognize the command.

In other situations, **<cr>** cannot be used because the remote computer accepts the command without a carriage return and requires time to process the command. This situation mainly applies when you are sending a series of commands without expecting a response.

Activating Switch.inf Scripts

After you have created a script in Switch.inf, you can configure a RAS entry to execute the script.

▷ **To activate a script in Windows NT**

1. In Dial-Up Networking, select the entry to which you want to connect.
2. Click **More** and choose **Edit entry and modem settings.**
3. In the **Script** tab, select the **Run this script** option and select the name of the script. The section header in Switch.inf appears as the name of the script.

   You can also edit your script by clicking **Edit scripts.**
4. Click **OK** and then click **Dial.**

When you dial this entry, the selected script will execute and complete all comunication with the remote device before or after RAS dials the remote host.

Troubleshooting Scripts Using Device.log

Windows NT enables you to log all information passed between RAS, the modem, and the remote device, including errors reported by the remote device. This allows you to find errors that prevent your scripts from working.

The Device.log file is created by enabling logging in the registry. After you enable logging, the Device.log file is in the *systemroot*\SYSTEM32\RAS folder.

▶ To create the Device.log file

1. Hang up any connections, and then exit from Dial-Up Networking.
2. Start the Registry Editor by running the REGEDT32.EXE program.
3. Go to HKEY_LOCAL_MACHINE, and then access the following key:\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
4. Change the value of the Logging parameter to 1. When changed, the parameter should look like this:

   Logging:REG_DWORD:0x1
5. Close the Registry Editor.

Logging begins when you restart Remote Access or start the Remote Access Server service (if your computer is receiving calls). You do not need to shutdown and restart Windows NT.

After you dial a number and connect, a script will start. If an error is encountered during script execution, execution halts. You should exit RAS, and then determine the problem by using any text editor to view Device.log. The following topic is an example of an incomplete script that failed when a connection was attempted and the Device.log file that was created.

Note The traces from all calls will be appended to Device.log as long as RAS or the Remote Access Server service are not stopped and restarted. So, if you need to save a Device.log file with useful information for later review or troubleshooting, make a copy of the file, giving the file another name before you restart RAS or the Remote Access Server service.

Example of an Incomplete Switch.inf Script

The following script is incomplete for the service to which the user tried to connect. This script was used with Device.log to discover that the remote computer expected additional commands from the script. See the sample Device.log for the complete output that was generated.

```
[Gibraltar Net Login for MariaG]; FIRST COMMAND TO INITIALIZE REMOTE
COMPUTERCOMMAND=; Skip to login prompt. That is, loop through blocks of
text ; separated by 2-second gaps until the login prompt is
encountered.OK=<match>"Login:"LOOP=<ignore>; Provide username to remote
computerCOMMAND=MariaG<cr>; Since no 2-second gap is present,
immediately match "Password:"OK=<match>"Password:"; Provide password to
remote computerCOMMAND=mUs3naB
```

Sample Device.log

This is the Device.log file created by using the sample generic script. Note that Device.log comment lines in all uppercase letters are writer comments added after the file was created to help you understand the contents of the file.

```
Remote Access Service Device Log  08/23/1996  13:52:21-----------------
-------------------------------------------; THIS SECTION IS THE
COMMUNICATION BETWEEN RAS AND THE MODEMPort:COM1 Command to
Device:AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55
Port:COM1 Echo from Device :AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55
Port:COM1 Response from Device:OKPort:COM1 Command to
Device:AT\Q3\N7%C0M1
Port:COM1 Echo from Device :AT\Q3\N7%C0M1
Port:COM1 Response from Device:OK

; COMMAND TO DIAL REMOTE COMPUTER AND SUCCESSFUL CONNECTION
Port:COM1 Command to Device:ATDT1 206 555 5500
Port:COM1 Echo from Device :ATDT1 206 555 5500
Port:COM1 Response from Device:CONNECT 14400/RELPort:COM1 Connect
BPS:19200Port:COM1 Carrier BPS:14400
; INITIAL NULL COMMAND SENT TO DEVICE
Port:COM1 Command to Device:Port:COM1 Response from
Device:_[2J_[HWelcome to Gibraltar Net, a service of: Trey Computing,
Inc.Problems logging in?  Call us at 555-5500 between 8:00am and 8:00pm
Mon-Sat.NOTE: Your software must support VT100 (or higher) terminal
emulation!      Port:COM1 Response from Device:P
; THE LINE ABOVE INDICATES A TWO-SECOND GAP IN THE MIDDLE ; OF THE WORD
"PLEASE" IF YOUR SCRIPT FAILED AND DEVICE.LOG ENDED ; AFTER THE RESPONSE
ABOVE, YOU WOULD ACCOUNT FOR THIS ; TWO-SECOND GAP IN YOUR SCRIPT BY
USING A NULL COMMAND= LINE OR THE ; OK=response AND LOOP=<match>
COMBINATION.
Port:COM1 Response from Device:lease turn OFF your Caps Lock if it is on
now.Please enter your login name and password at the prompts below.  -
Log in as "guest" to take a look around the system.  - Log in as "new"
to create an account for yourself.Login:
; SEND YOUR USERNAME AS A COMMAND
Port:COM1 Command to Device:MariaG
Port:COM1 Echo from Device :MariaG
Port:COM1 Response from Device:Password:
; SEND YOUR PASSWORD AS A COMMAND
Port:COM1 Command to Device: mUs3naB
Port:COM1 Echo from Device : mUs3naB

; THE LOGIN SEQUENCE CONTINUES ON THE REMOTE COMPUTER
; BUT THE SCRIPT DOES NOT CONTINUE FROM HERE.
; THE AUTOMATED LOG IN WOULD FAIL AT THIS POINT.
Port:COM1 Response from Device:
```

This script would be complete for many remote computers, but the remote computer sent more responses and expected a command to start a service. To complete the script you must know the remainder of the responses from the remote computer. If you logged on manually using RAS Terminal and found the remainder of the logon sequence looked like this:

```
Gibraltar Net offers you several network services:Service
-------------------------------------------------------------------
SHellUPloadDOwnloadPAsswordPPPSLIPPlease enter a service:
```

you would complete the script with these lines:

COMMAND=<cr>
OK=<match>"Please enter a service:"
LOOP=<ignore>

If you added the lines above to your script, restarted RAS and redialed, you would successfully connect.

If the generic script in RAS does not work, these guidelines should help you modify the generic script to work for your connections. First copy the generic script to the end of Switch.ing, then modify the copy to work with your connections.

Using Scripts with Other Microsoft RAS Clients

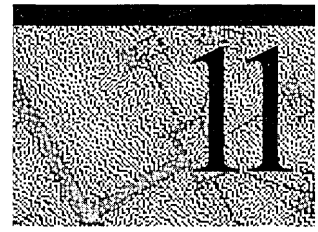
Microsoft RAS version 1.0 (which runs on LAN Manager) cannot invoke RAS Terminal or use scripts in .inf files.

Microsoft RAS version 1.1a (which runs on LAN Manager) supports Pad.inf only. Note that the syntax used in the Pad.inf file differs slightly from subsequent versions of Microsoft RAS.

Microsoft RAS for Windows for Workgroups version 3.11 and Windows NT version 3.1 or later support RAS Terminal and scripts in Switch.inf and Pad.inf.

CHAPTER 11

Point-to-Point Tunneling Protocol (PPTP)



A RAS server is usually connected to a PSTN, ISDN, or X.25 network, allowing remote users to access a server through these networks. RAS now allows remote users access through the Internet by using the new Point-to-Point Tunneling Protocol (PPTP).

PPTP is a new networking protocol that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet by dialing into an Internet Service Provider (ISP) or by connecting directly to the Internet. PPTP offers the following advantages:

Lower Transmission Costs PPTP uses the Internet as a connection instead of a long-distance telephone number or 800 service. This can greatly reduce transmission costs.

Lower Hardware Costs PPTP enables modems and ISDN cards to be separated from the RAS server. Instead, they can be located at a modem pool or at a communications server (resulting in less hardware for an administrator to purchase and manage).

Lower Administrative Overhead With PPTP, network administrators centrally manage and secure their remote access networks at the RAS server. They need to manage only user accounts instead of supporting complex hardware configurations.

Enhanced Security Above all, the PPTP connection over the Internet is encrypted and secure, and it works with any protocol (including, IP, IPX, and NetBEUI).

Applications for PPTP

PPTP provides a way to route PPP packets over an IP network. Since PPTP allows multiprotocol encapsulation, you can send any type of packet over the network. For example you can send IPX packets over the Internet.

PPTP treats your existing corporate network as a PSTN, ISDN, or X.25 network. This virtual WAN is supported through public carriers, such as the Internet.

Compare PPTP to the other WAN protocols: When you use PSTN, ISDN, or X.25, a remote access client establishes a PPP connection with a RAS server over a switched network. After the connection is established, PPP packets are sent over the switched connection to the RAS servers to be routed to the destination LAN.

In contrast, when you use PPTP instead of using a switched connection to send packets over the WAN, a transport protocol such as TCP/IP is used to send the PPP packets to the RAS server over the virtual WAN.

The end benefit for both the user and the corporation is a savings in transmission costs by using the Internet rather than long distance dial-up connections.

The following three sections describe how PPTP can be used: for outsourcing a dial-up network, for client connections directly through the Internet , and for client connections through an ISP.

PPTP in Outsourced Dial-Up Networks

Communications hardware available for supporting dial-up needs can be complicated and not well integrated. For a large enterprise, putting together a Windows NT RAS server requires modems, serial controllers, and many cables. Furthermore, many solutions do not provide a single integrated way to efficiently support V.34 and ISDN dial-up lines.

Many corporations would like to outsource dial-up access to their corporate backbone networks in a manner that is cost effective, hassle free, protocol independent, secure, and that requires no changes to the existing network addressing. Virtual WAN support using PPTP is one way a service provider can meet the needs of corporations.

By separating modem pools from a RAS server, PPTP allows you to outsource dial up services or geographically separate the RAS server from the hardware within a corporation. For example, a telephone company can manage modems and telephone lines so that user account management can be centralized at the RAS server. An end user would then make a local call to the telephone company which connects to a Windows NT RAS sever using a WAN link. The client then has access to the corporate network.

This type of solution leverages existing proven PPP authentication, encryption, and compression technologies.

See figure 11.1 for an example: The RAS client does not need to have the PPTP protocol; the client simply makes a PPP connection to the modem pool or communications server. Note that the communication server or modem pool must implement PPTP for communication with the RAS server.

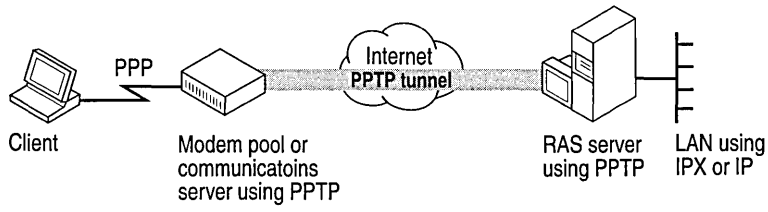


Figure 11.1 An outsourced dial-up network using PPTP

Secure Access to Corporate Networks over the Internet (Virtual Private Networks)

A RAS client that has PPTP as its WAN driver can access resources on a remote LAN by connecting to a Windows NT RAS server through the Internet. There are two ways to do this: By connecting directly to the Internet or by dialing an ISP as shown in the following examples.

In the first, a client directly connected on the Internet dials the number for the RAS server. PPTP on the client makes a tunnel through the Internet and connects to the PPTP enabled RAS server. After authentication, the client can access the corporate network, as shown in figure 11.2.

Note Connecting directly to the Internet means direct IP access without going through an ISP. (For example, some hotels allow you to use an Ethernet cable to gain a direct connection to the Internet.)

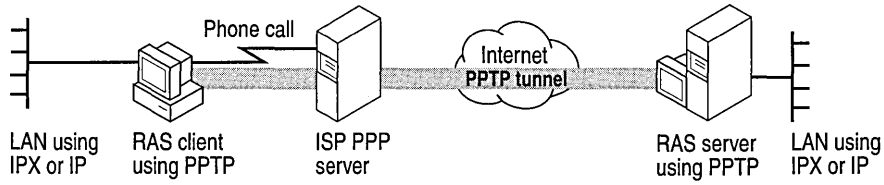


Figure 11.2 RAS client connected directly to the Internet

In the second example, the same functionality is achieved by calling an ISP instead of being directly connected to the Internet. The client first makes a call to the ISP. After that connection is established, the client makes another call to the RAS sever that establishes the PPTP tunnel. See figure 11.3 for an example.

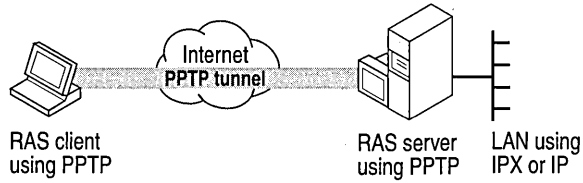


Figure 11.3 RAS client dialing into an ISP

Security Considerations

Data sent across the PPTP tunnel is encapsulated in PPP packets. Because RAS supports encryption, the data will be encrypted. RAS supports bulk data encryption using RSA RC4 and a 40-bit session key that is negotiated at PPP connect time between the RAS client and the Windows NT RAS server.

PPTP uses the Password Authentication Protocol and the Challenge Handshake Authentication Protocol encryption algorithms.

In addition to supporting encrypted PPP links across the Internet, a PPTP-based solution also enables the Internet to become a network backbone for carrying IPX and NetBEUI remote-access traffic. PPTP can transfer IPX traffic because it encapsulates and encrypts PPP packets so that they can ride TCP/IP. Thus, a solution does not depend only on TCP/IP LANs.

Installing PPTP

You must have the PPTP protocol installed on the RAS server—and on the client or communications server—for PPTP tunneling to succeed.

▶ **To install the PPTP protocol**

1. In Control Panel, double-click the Network icon, then click the **Protocols** tab.
2. Click **Add** and select **Point to Point Tunneling Protocol**.

   When prompted for the path to the distribution files, provide the path and click **OK**.

3. Enter the number of connections you want available to PPTP (i.e. Virtual Private Networks).

   RAS setup will start and add the PPTP protocol to RAS. Choose the port on which you want to install the PPTP protocol and click **OK**.

4. You must restart your computer for the PPTP configuration to take effect.

Protecting a RAS Server from Internet Attacks

If you select PPTP filtering, you effectively disable the selected network adapter for all other protocols. Only PPTP packets will be allowed in.

You might want to do this when you have a multihomed computer with one network adapter (with PPTP filtering enabled) connected to the Internet and another network adapter connected to the internal corporate network. Clients outside the corporate network can use PPTP to connect to the computer from across the Internet and gain secure access to the corporate network. Thus, the only traffic that can access the corporate network is PPTP packets from clients who have been authenticated using RAS authentication. Figure 11.4 illustrates this concept.

Note The RAS client can either be connected to the Internet directly or to a service provider. It is not necessary to be connected to both to use PPTP.

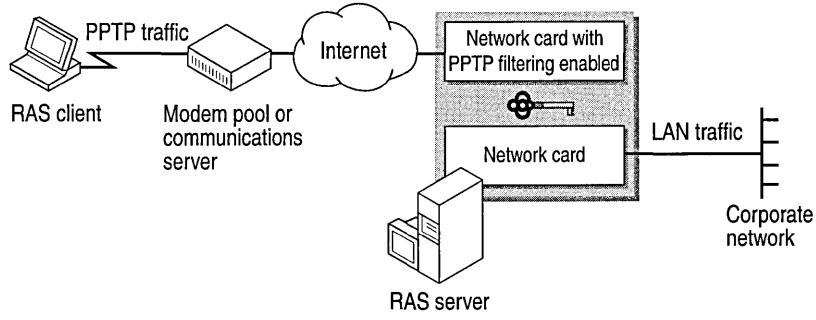


Figure 11.4 PPTP filtering between the Internet and the corporate network

▶ **To enable PPTP filtering**

1. In Control Panel, double-click the Network icon, then click the **Protocols** tab.
2. Select **TCP/IP Protocol**, and click **Properties**.

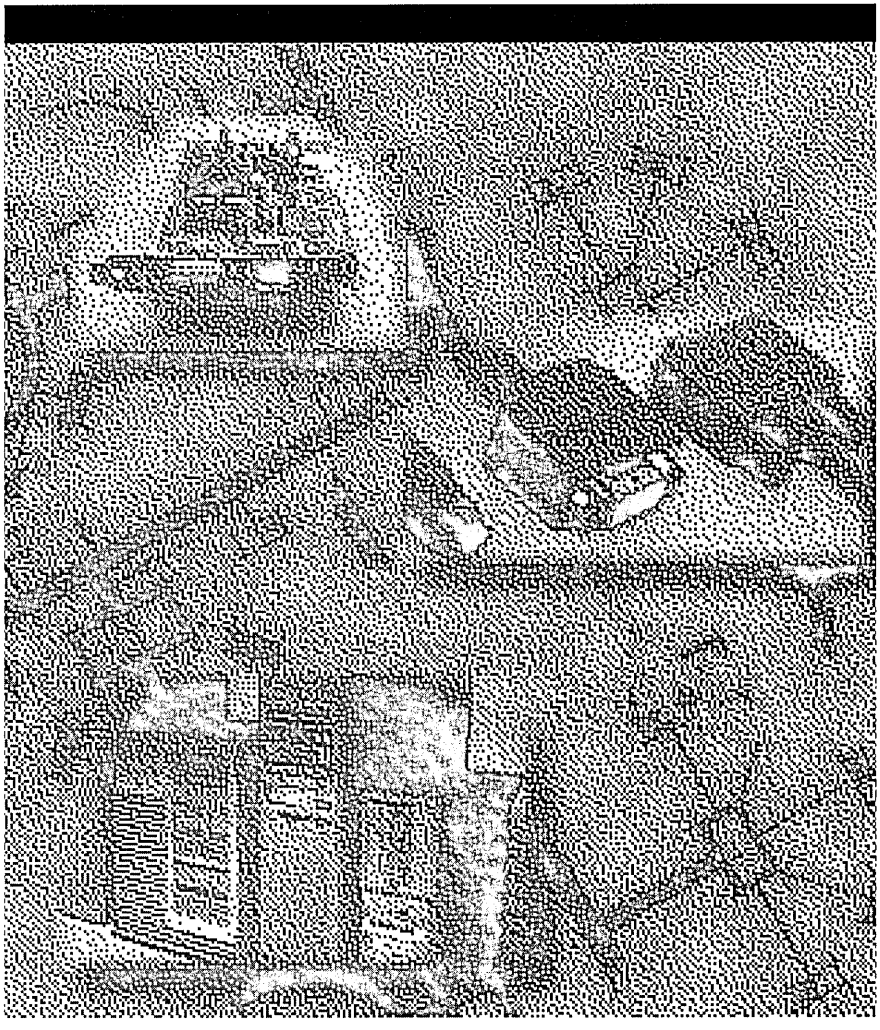
3. On the **IP Address** tab, click **Advanced**.
4. In the **Adapter** box, select the network adapter for which you want to specify PPTP filtering. The PPTP filtering settings in this dialog box are defined only for the selected network adapter.
5. To enable PPTP filtering, select **Enable PPTP Filtering**.

The settings take effect after you restart the computer.

For more information about advanced TCP/IP configuration, see the topic "To Configure Advanced TCP/IP Options" in the TCP/IP online Help file.

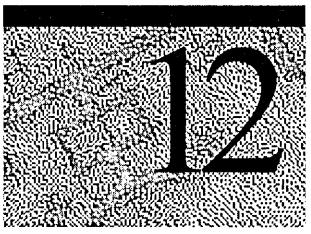
PART 4

Services for NetWare Networks



CHAPTER 12

Overview of NetWare Compatibility Features



Windows NT Server and Windows NT Workstation provide several features and services that enable Windows NT computers to coexist and interoperate with Novell® NetWare® networks and servers. Some of these services are included in Windows NT Server and Windows NT Workstation; others are available as separate products.

- *The NetWare Link IPX/SPX Compatible Transport* (NWLink) is the Windows NT implementation of the IPX/SPX protocol. NWLink supports connectivity between computers running Windows NT and computers running NetWare and compatible systems. NWLink can also be used as a protocol connecting multiple Window NT computers. NWLink is included with both Windows NT Server and Windows NT Workstation.
- *Client Service for NetWare*, included with Windows NT Workstation, enables workstations to make direct connections to file and printer resources at NetWare servers running NetWare 2.x or later. Client Service for NetWare supports NetWare 4.x servers running either Novell Directory Services (NDS) or bindery emulation. Login script support is also included.

  For more information on Client Service for NetWare, see the Windows NT Workstation online Help.
- *Gateway Service for NetWare*, included with Windows NT Server, enables a computer running Windows NT Server to connect to NetWare servers, just as Client Service for NetWare enables workstations to connect to NetWare servers. In addition, you can use Gateway Service for NetWare to create gateways to NetWare resources. Creating a gateway enables computers running only Microsoft client software to access NetWare resources through the gateway.

  For more information on Gateway Service for NetWare, see the following chapter, "Gateway Service for NetWare."

- *Migration Tool for NetWare*, included with Windows NT Server, enables you to easily transfer user and group accounts, volumes, folders, and files from a NetWare server to a computer running Windows NT Server. If the server you are migrating to runs File and Print Services for NetWare, you can also migrate users' logon scripts.

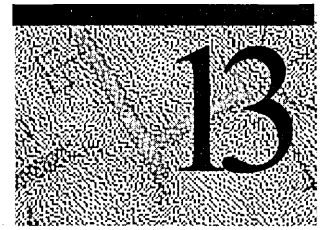
  For more information on Migration Tool for NetWare, see Chapter 3, "Migration Tool for NetWare."

- *File and Print Services for NetWare* (FPNW) is a separate product. It enables a computer running Windows NT Server to provide file and print services directly to NetWare and compatible client computers. The server appears just like any other NetWare server to the NetWare clients, and the clients can access volumes, files, and printers at the server. No changes or additions to the NetWare client software are necessary.

- *Directory Service Manager for NetWare*, also available separately, extends Windows NT Server directory service features to NetWare servers. It enables you to add NetWare servers to Windows NT Server domains and to manage a single set of user and group accounts that are valid at multiple servers running either Windows NT Server or NetWare. Users then have just one user account, with one password, to gain access to these servers.

CHAPTER 13

Gateway Service for NetWare



With Gateway Service for NetWare (GSNW), you can create a gateway through which Microsoft client computers without NetWare client software can access NetWare file and print resources. You can make gateways for resources located on NetWare Directory Service (NDS) trees as well as for resources on servers running NetWare 2.*x* or later with bindery security. These resources include volumes, directories, dirmaps, printers, and print queues.

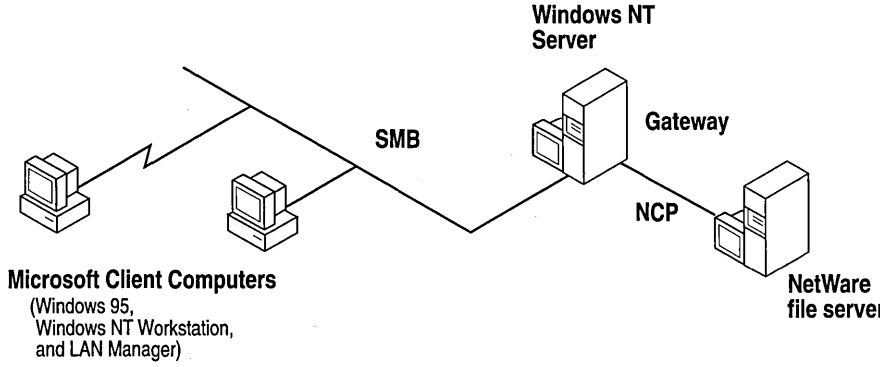
GSNW also enables users working locally at the Windows NT Server computer to directly access NetWare file and print resources, both on NDS trees and on servers with bindery security.

GSNW depends on and works with another NetWare compatibility feature of Windows NT Server: the *NWLink protocol.* NWLink is an implementation of the internetworking packet exchange (IPX) and sequenced packet exchange (SPX) transport protocols used by the NetWare network.

The Microsoft implementations of the IPX, SPX, and Novell NetBIOS protocols can seamlessly coexist with other protocols on the same network adapter card.

How a Gateway Works

GSNW acts as a bridge between the server message block (SMB) protocol used by the Windows NT network and the NetWare core protocol (NCP) used by the NetWare network. When a gateway is enabled, network clients running Microsoft client software can access NetWare files and printers without having to run NetWare client software locally. The following figure shows an example of a file gateway configuration:



File Gateway Example

For file access, the gateway server redirects one of its own drives to the NetWare volume and then shares that drive to other Microsoft clients. The file gateway uses a NetWare account on the Windows NT Server computer to create a validated connection to the NetWare server. This connection appears on the Windows NT Server computer as a redirected drive. When you share the redirected drive, it becomes like any other shared resource on the Windows NT Server computer.

For example, suppose you want to create a gateway from the computer Airedale (running GSNW) to the NetWare NDS folder \\Nw4\Server1\Org_Unit.Org\Data volume on the NetWare server NW4. When activating the gateway, you specify \\Nw4\Server1\Org_Unit.Org\Data as the NetWare resource, and you might specify Nw_Data as the share name for Microsoft clients. Microsoft clients would then refer to this resource as \\Airedale\Nw_Data.

After the gateway connection is established, it is disconnected only if the computer is turned off or if the Windows NT Server administrator disconnects the shared resource or disables the gateway. Logging off the Windows NT Server computer does not, by itself, disconnect the gateway.

Note Because requests from Microsoft networking clients are being processed through the gateway, access is slower than direct access from the client to the NetWare network. Clients that require frequent access to NetWare resources should run Windows NT Workstation with the Client Service for NetWare or Windows 95 with its NetWare client software, to achieve higher performance.

Installing Gateway Service for NetWare

GSNW is not installed by default when you install Windows NT Server: You install it from the Windows NT Server CD-ROM. (The NWLink transport protocol is also installed if it is not already on the server.)

Important Before installing the Gateway Service, remove any existing third-party network service or client software, including Novell NetWare client software.

You must be logged on as a member of the Administrators group to install and configure the Gateway Service.

▶ **To install the Gateway Service**

1. Click **Start**, then click **Settings**, then click **Control Panel**.
2. Double-click the Network icon.
3. Click the Services tab.
4. Click **Add**.
5. Select **Gateway (and Client) Services for NetWare** from the list, then click **Add**.
6. In the resulting dialog box, type the path to your Windows NT Server CD-ROM in the box, and then click **OK**.
7. When the file copying is complete, reboot the computer.

An icon labeled *GSNW* is added to Control Panel.

By default, the NetWare network is placed first in the network search order. For more information on the network search order, see Help.

Specifying a Default Tree and Context or Preferred Server

When you first log on after GSNW is installed, you are prompted to set your default tree and context or your preferred server. The tree and context define the position of the user object of the user name you use to log in to an NDS tree. A preferred server is the NetWare server to which you are automatically connected when you log on, if your network does not use NDS.

You can have either a default tree and context or a preferred server, but not both. (In NDS environments, a default tree and context are the common choice.) If you select a default tree and context, you can still access NetWare servers that use bindery security.

To change your tree and context later, use the GSNW icon in Control Panel.

Creating a Gateway

Before you can create a gateway on a Windows NT Server computer:

- You must have a user account on the NetWare network with the necessary rights for the resources you want to access.
- The NetWare server must have a group named Ntgateway with the necessary rights for the resources you want to access.
- The NetWare user account you use must be a member of the Ntgateway group.

The NetWare user account you use to enable gateways can be either an NDS account or a bindery account. If the server will have gateways to both NDS resources and resources on servers running bindery security, the user account must be a bindery account. (This account can connect to NDS resources through bindery emulation). If you create gateways only to NDS resources, the account can be an NDS account.

Creating a gateway is a two-step process:

1. First you *enable* gateways on the server running Windows NT Server. When you enable a gateway, you must type the name and password of the user account that has access to the NetWare server and is a member of the Ntgateway group on that NetWare server.

   You need to do this only once for each server that will act as a gateway.

2. For each volume or print queue to which you want to create a gateway, you *activate* a gateway. When you activate a gateway, you specify the NetWare resource and a share name that Microsoft client users will use to connect to the resource.

To activate a gateway for a volume, use the GSNW icon in Control Panel. To activate a gateway for a print queue, use the Add Printers wizard.

If you are activating a gateway to an NDS resource, and the gateway user account is a bindery user account, you should specify the resource using the bindery context name. If you are using a NDS user account, and you do not plan on also creating gateways to bindery resources, than you can specify the NDS resource name.

Security for gateway resources is provided on two levels:

- On the computer running Windows NT Server and acting as a gateway, you can set share-level permissions for each resource made available through the gateway.
- On the NetWare file server, the NetWare administrator can assign trustee rights to the user account used for the gateway or to the Ntgateway group. These rights will be enforced for all Microsoft client users who access the resource through the gateway. There is no auditing of gateway access.

Connecting Directly to NetWare Resources

In addition to providing gateway technology, GSNW enables users working locally at the server to access NetWare resources directly, just as Client Service for NetWare provides this service to Windows NT Workstation users. The information in this section applies to users working locally at a server, accessing NetWare resources directly—not to Microsoft clients accessing resources through a gateway. (This information *does* apply to users of Client Service for NetWare on Windows NT Workstation.)

NDS trees (as well as NetWare servers running bindery security) appear in the NetWare or Compatible Network list in the Explorer. Double-click a tree name to expand it, and then double-click any container object to expand its contents and structure.

To map a local drive to a volume on the NDS tree, select the volume, then on the **File** menu click **Map Network Drive**. You can connect to and assign a local drive letter to any volume, folder, or dirmap anywhere in the tree hierarchy (for which you have credentials).

To connect to an NDS printer, use the Add Printer wizard, just as you would to connect to any network printer.

If you have a default tree and context, once you have logged on you do not need to log on again or supply another password to access any volume in your default tree. Accessing another tree prompts you to supply a full context (including user name) for that tree.

For more information on connecting to network resources using Explorer, see Help.

Changing the NetWare Password

Users who use either GSNW or Client Service for NetWare to directly access NetWare resources can change their passwords on NDS trees on the network. To do this, use the standard Windows NT Server password changing procedure: Press CTRL+ALT+DEL, and then specify **NetWare or Compatible Network** in the **Domain** box of the **Change Password** dialog box).

To change the password on NetWare servers running bindery security, use the **setpass** command on the NetWare server. (Or, if the network runs *Microsoft Directory Service Manager for NetWare*, you can use a single command to change both Windows NT Server and NetWare bindery passwords.)

Logon Scripts

When a user running either GSNW or Client Service for NetWare to directly access NetWare resources first makes a connection to a particular NetWare server, the user's logon script (if any) runs. Users who connect to NetWare resources through a gateway do not have a logon script run, however.

Managing NetWare File Attributes

NetWare file attributes are not exactly the same as those on Windows NT Server. The following file rights mappings are applied when a NetWare file is opened through GSNW:

Windows NT file attributes	NetWare file attributes
A (Archive)	A
S (System)	Sy
H (Hidden)	H
R (Read Only)	Ro, Di (Delete Inhibit), Ri (Rename Inhibit)

GSNW does not support the following NetWare file attributes: RW (Read Write), S (Shareable), T (Transactional), P (Purge), Ra (Read Audit), Wa (Write Audit), and Ci (Copy Inhibit).

When you copy a file from a Microsoft networking client to the NetWare file server by means of GSNW, the Ro, A, Sy, and H file attributes are preserved.

When you use a computer running GSNW to directly access NetWare servers, you can use the NetWare utilities, such as **filer** and **rights**, to set attributes that are not supported by the Windows NT-to-NetWare file rights mapping. For more information about other supported utilities, see the next section.

Running NetWare Utilities and NetWare-Aware Applications

With Windows NT Server and GSNW, you can run many standard NetWare utilities from the command prompt. For some administrative functions, you must use Windows NT Server management tools. In addition, GSNW supports many NetWare-aware applications.

The following sections list the supported NetWare utilities and explain the Windows NT Server administrative utilities you can use to manage the NetWare network. It also lists supported NetWare-aware applications and describes the files you must have in order to run them.

Supported NetWare Utilities

Windows NT supports many NetWare utilities, enabling you to manage the NetWare network from a computer running Windows NT Workstation or Windows NT Server. Some additional files supplied either with Windows NT Server or with NetWare might be required by some utilities. For detailed information, see "Requirements for Running NetWare-Aware Applications," later in this chapter.

Windows NT supports the following MS-DOS–based NetWare utilities:

chkvol	**help**	**rconsole**	**settts**
colorpal	**listdir**	**remove**	**slist**
dspace	**map**	**revoke**	**syscon**
flag	**ncopy**	**rights**	**tlist**
flagdir	**ndir**	**security**	**userlist**
fconsole	**pconsole**	**send**	**volinfo**
filer	**psc**	**session**	**whoami**
grant	**pstat**	**setpass**	

Note If you run a utility (such as **rconsole** on 3.1*x* NetWare servers) outside of the Sys:Public directory, the utility might ask for the Sys$Msg.Dat file, which is located in the Sys:Public directory. To avoid this message, add Sys:Public to your path.

NetWare Utility Behavior Supplied by Windows NT Commands

The Windows NT **net use** command or Explorer perform the same functions as the NetWare **attach**, **login**, and **logout** utilities.

The Windows NT **net view** command performs the same function as the NetWare **slist** utility.

The **net use** command is similar to the **capture** command for printing when MS-DOS–based and Windows-based applications must print to a specific port. In addition, you can use the Add Printer wizard to connect to NetWare print queues.

You can use the **net use** command to connect to volumes and printers in NDS trees, as well as on other NetWare servers.

For more detailed command syntax, see Help.

NetWare-Aware Applications

Many NetWare-aware applications run on Windows NT Server and GSNW as if they were running on a NetWare client computer. However, not all NetWare-aware applications are supported, and of those that are, many require special files supplied with either NetWare or with Windows NT Server.

Supported NetWare-Aware Applications

The NetWare-aware applications shown in the following table are supported. They were tested on x86, MIPS, Digital Alpha, and PowerPC platforms. Most of these applications require the use of the Nwipxspx.dll, Netware.drv, and Nwnetapi.dll files; other prerequisites for each application are listed in the table. Following the table are descriptions of the services and files required for these applications to be supported.

MS-DOS–Based NetWare-Aware Applications

Application	Version	Prerequisites
DCA™ IRMA™ LAN for MS-DOS to Novell's SAA	2.1.0	None
Paradox for MS-DOS	4.0	None
Btrieve® requester (Brequest.exe)	6.10a	TSR
NetWare 3270 LAN Workstation for MS-DOS	3.0	Runs only on x86 platform

Windows–Based NetWare-Aware Applications

Application	Version	Prerequisites
Attachmate Extra! for Windows	4.0	TSR
DCA™ IRMA™ LAN for Windows	2.12	None
Btrieve® requester (BREQUEST.EXE)	6.10a	TSR
Gupta SQLBase® for NetWare systems	5.1.3	Btrieve support Must be connected to a NetWare server prior to loading
Lotus Notes®, SPX connectivity option	3.2	Must be connected to a NetWare server prior to loading
Lotus CCMail for Windows	2.0	
Wall Data Rumba for Windows	3.2	Must add Wdnovtsr.exe to your Autoexec.nt file
NetWare 3270 LAN Workstation for Windows	1.2	Runs only on x86 platform

Requirements for Running NetWare-Aware Applications

The following files and services might be required in order for MS-DOS–based NetWare utilities and NetWare-aware applications to be supported.

Note The Novell VLM Interface is not supported. (For example, NWADMIN will not run on a computer running GSNW.)

Nwipxspx.dll

Many 16-bit NetWare-aware applications (including many listed in the preceding tables) require Nwipxspx.dll from Novell. If you have previously used the application with another Microsoft Windows-based operating system and are using the same computer for Windows NT, Nwipxspx.dll exists on your system. If you start the application and the application cannot find this file, check your path by typing **path** at the command prompt. Verify that a copy of the Nwipxspx.dll exists. If it does not, obtain a copy from Novell, and copy it to the *\systemroot*\system32 directory.

If you are running these applications on the MIPS, Digital Alpha, or PowerPC platforms, you must obtain Nwipxspx.dll from Novell. Copy Nwipxspx.dll to the *\systemroot*\System32 directory.

If you need to copy Nwipxspx.dll to your Windows NT Server computer or modify your path statement, you must log off and then log on for the changes to take effect.

Netware.drv, Nwnetapi.dll, and Nwcalls.dll

NetWare-aware applications that use the NetWare application programming interface (API) to send and receive NetWare core protocol (NCP) packets might require Netware.drv and either Nwnetapi.dll or, for more recent versions of NetWare, Nwcalls.dll.

Netware.drv is installed in the *\systemroot*\system32 directory when you install the Gateway Service. If you have previously used a NetWare-aware application on the same computer using another Microsoft Windows-based operating system, Nwnetapi.dll or Nwcalls.dll is probably already installed on your computer. If your application cannot find Nwnetapi.dll or Nwcalls.dll, be sure the appropriate file is installed on your computer and is in your computer's search path. If you are running the application on the Digital Alpha or MIPS platform or you can't locate one of these .DLL files on your computer, contact Novell to obtain a copy of the appropriate file, and then install it in your *\systemroot*\system32 directory. If you cannot load your NetWare-aware application with the version of Netware.drv installed with the Gateway Service, replace Netware.drv with the corresponding file supplied by Novell, dated 10/27/92 with a file size of 126,144 bytes.

If you copied any of these files to your Windows NT Server computer or modified your Path statement during the current Windows NT work session, you must log off and then log on for the changes to take effect.

Special Considerations for Individual NetWare-Aware Applications

If you do not have a default tree and context or preferred server and you have not connected to any NetWare server, you must first create a connection to a NetWare server. For more information about connecting to NetWare servers, see "Connecting Directly to NetWare Resources" earlier in this chapter.

Btrieve

If you are running MS-DOS–based or 16-bit Windows-based applications that require the Btrieve requester, Brequest.exe, you must modify the Autoexec.nt file located in *\systemroot*\system32 so that the applications can find the Btrieve requester. Find the location of Brequest.exe on your computer and append location information in the Autoexec.nt file. The line you should add to Autoexec.nt depends on the computer you are running.

For example, if Brequest.exe is located in the C:\Btrieve directory, add the following line to Autoexec.nt on Windows NT Server:

c:\btrieve\brequest.exe

On Windows NT Workstation, add this line:

lh c:\btrieve\brequest.exe

Then log off and log on for the change to take effect.

Attachmate Extra! Extended for MS-DOS

If Extra! batch files are run from a console window, make the first line of the batch files **command /c** so that the Extra! hot keys work after Extra! has initialized.

Attachmate Extra! for Windows IPX/SPX Connectivity

Attachmate Extra! for Windows requires IPXINTFC, a terminate-and-stay-resident (TSR) utility. This TSR must be loaded by Autoexec.nt prior to the DOSX TSR being loaded.

For example, suppose Attachmate Extra! for Windows has been installed in the C:\Extrawin subdirectory. In Autoexec.nt, make sure the following three lines appear in the order shown:

```
lh c:\extrawin\ipxintfc
REM Install DPMI support
lh winnt\system32\dosx
```

Log off and log on to Windows NT for the changes to take effect.

Troubleshooting the Gateway Service

This section describes how to troubleshoot various problems that can arise while installing, starting, and running GSNW. Problems are organized into the following categories:.

- Startup problems
- Access problems
- Application and print problems
- Other network problems

Startup Problems

Many common startup problems are caused by improper installation of the network adapter card or of the Gateway Service itself. Be sure the network card is installed and configured correctly and that existing installations of NetWare redirectors (such as Novell's NetWare Services for Windows NT) have been removed.

To correct the configuration of your network card or to remove a NetWare redirector, use the Network icon in Control Panel.

Gateway Service Doesn't Start

If the Gateway Service does not start, one of its required services or protocols might be unavailable. First try to start it manually (using the Services icon in Control Panel). If that fails, troubleshoot the problem by using Event Viewer to look at the system log. Look for one of the messages described in the following table:

Messages Found in the Event Details Dialog Box

Source and Message	Recommended action
Service Control Manager Gateway Service for NetWareterminated with the following error: The system cannot find the specified file.	The Gateway Service was not installed properly. Use the Network icon in Control Panel to remove and reinstall the Gateway Service
Service Control Manager The NWLink service depends on the NWLinksys services which failed to start because of the following error: The system cannot find the file specified.	The NWLink IPX/SPX Compatible Transport Protocol was not installed properly. Use the Network icon in Control Panel to reinstall NWLink.
NWLinksys Error binding to adapter card *cardname*.	Your adapter card might be malfunctioning, or its settings might be incorrect. If your adapter card is not malfunctioning and the NWLink protocol is bound to the correct card, use the Network icon in Control Panel to verify the adapter card settings.

Gateway Service Starts, But Servers Can't Be Found

You might be unable to see NetWare servers because the network frame type is set incorrectly. View the network adapter load line in the NetWare server's Autoexec.ncf file to verify that you are using the correct frame type for the server. For example, suppose a server's network adapter load line is

```
load 3C503 FRAME=ETHERNET_802.3 NAME=ETH
```

In this case, the server is bound to a 3Com® 503 ethernet adapter that will accept the raw 802.3 frame format.

Use the Network icon in Control Panel to see the frame type set for your adapter card. If the frame type is "Auto Detected" and NWLink detects any frames of type 802.2 or no frames at all, it sets the frame type to 802.2. If the network adapter card receives frames of type 802.2 but your NetWare network uses some other frame type, you will have to set it manually. For instructions on setting the frame type manually, see online Help.

Access Denied While Creating Gateway

If access is denied when you try to configure a Windows NT Server computer as a file or print gateway, the NetWare user account you have used to enable the gateway might not be a member of the Ntgateway group, or your account or the Ntgateway group might have insufficient trustee rights. For information on setting up the Ntgateway group and assigning trustee rights on the NetWare server, see your NetWare documentation.

Application and Print Problems

To make sure a NetWare application is supported in this release, see the list of supported NetWare-aware applications in "NetWare-Aware Applications," earlier in this chapter. Also verify that any required files mentioned in that section are installed in a directory in the search path of your Windows NT computer.

The default environment for 16-bit programs is too small to accommodate the mapping table created by the NetWare **map** utility. You must designate Command.com as the permanent command interpreter for the Command Prompt window and reset the default environment size allocated to the window. An environment of 4096 bytes is large enough to accommodate the NetWare utility, the mapping table, and the command interpreter.

To make these changes to the environment, enter the following line in Config.nt:

shell=%systemroot%\system32\command.com /e:4096

This line causes Command.com to be the command interpreter for the window as long as it remains open or until you issue another **shell** command, and it permanently allocates 4096 bytes to 16-bit programs you run in the window.

Other Network Problems

This section briefly describes other network problems that could affect your ability to install or run the Gateway Service. If network problems persist, use Event Viewer to review the system log information generated during startup.

Duplicate Computer Names

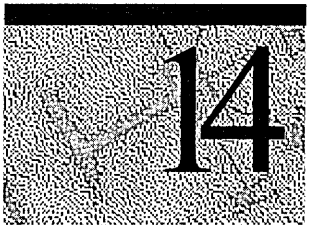
Each computer on a network must have a unique name. If you specify a computer name that is the same as another computer on the network or the same as a workgroup or a domain, the network will not start when you start your computer.

Services or Subsystems Do Not Start

If services or subsystems do not start properly, use the Services or Devices icons in Control Panel to check their status. You can try to start services using the Services icon and start a device with the Devices icon.

CHAPTER 14

Migration Tool for NetWare



The Windows NT Server Migration Tool for NetWare enables you to migrate NetWare servers to computers running Windows NT Server. The Migration Tool transfers user and group accounts, volumes, folders, and files. In addition, if the server you are migrating to runs File and Print Services for NetWare (FPNW), you can transfer users' logon scripts. (FPNW is a separate product that enables Windows NT Server to provide file and print sharing directly to NetWare clients.)

The Migration Tool enables you to

- Preserve most user account information.
- Control the transfer of user and group names.
- Set passwords for transferred accounts.
- Control the transfer of account restrictions and administrative rights.
- Select the folders and files to transfer.
- Select a destination for transferred folders and files.
- Preserve effective rights (the NetWare equivalent of permissions) on folders and files.
- Perform trial migrations, to test how current settings will actually transfer information.
- Generate comprehensive log files, detailing what happened during migration.

Software Requirements

- The Migration Tool can be used to migrate information only to computers that run Windows NT Server and function as primary domain controllers or backup domain controllers.
- You can run the Migration Tool from the server to which you are migrating, or remotely from another computer running Windows NT Server or Windows NT Workstation. (To copy the Migration Tool to a workstation, copy the nwconv.exe, nwconv.hlp, logview.exe, and logview.hlp files from a server's *systemroot*\SYSTEM32 folder.
- Both NetWare Link IPX/SPX Compatible Transport (NWLink) and Gateway Service for NetWare must be installed on the server used to run the Migration Tool and on servers being migrated to.
- It is best to migrate to servers that have the Windows NT file system (NTFS) installed. Only files and folders transferred to NTFS can preserve permissions (trustee rights) from the NetWare server.

Planning a Migration

Before performing a migration, become familiar with the differences between Windows NT Server and NetWare, and plan the migration.

When planning a migration, consider the following issues:

- How current NetWare clients access computers running Windows NT Server
- How servers should be organized into domains
- Which order to migrate NetWare servers in (if you are migrating more than one)

By running a trial migration you can make informed migration decisions. In a trial, the Migration Tool creates a set of log files that reflect how users and groups and volumes will be transferred. By reviewing the log files, you can adjust migration options as desired. For more information, see "Running a Trial," later in this chapter.

Providing Access to Windows NT Server

If you plan to add Windows NT Server to provide file and print services, and if existing workstations on your network are running NetWare client software, you must decide how to provide connectivity to Windows NT Server:

- To take full advantage of Windows NT Server features, upgrade workstations to Microsoft client software such as Windows NT Workstation or Windows 95. Such software preserves a workstation's connectivity to NetWare servers at the same time it supports all through Windows NT Server features.
- Alternatively, install FPNW on the computer you are migrating to. This enables the server to provide file and printer sharing directly to NetWare clients, with no changes necessary at the clients.

Organizing Servers Into Domains

If you plan to migrate many NetWare servers to Windows NT Server in several departments, consider how to best organize the network using one or more *domains*. The domain organization offered by Windows NT Server provides users complete access to the network with a single logon. It also eases the chore of account management because all accounts can be located centrally and each user needs only one account for complete network access. For more information on Windows NT domains, see "Comparing Network Models," later in this chapter and the *Windows NT Server Concepts and Planning Guide*.

To decide how computers running Windows NT Server should be organized, inventory your current network resources and how they are used. Consider both servers and client workstations. (A simple chart showing both the existing organization and the organization to which you are moving might prove helpful.)

For example, suppose a department relies on several servers that users in other departments rarely access, and that all clients in the department are running Windows 3.1. The best course might be to upgrade all clients to Windows 95, migrate the servers to Windows NT Server, and organize them as a single domain.

Planning the Order of Server Migration

When you have determined which NetWare servers to transfer, plan the order in which to migrate them.

When you transfer accounts from multiple NetWare servers to a Windows NT Server domain, you consolidate user and group accounts. It's usually easiest to first migrate the server that contains the greatest number of user and group accounts. Then, as you migrate additional servers, use the Migration Tool to control how duplicate user and group accounts are handled.

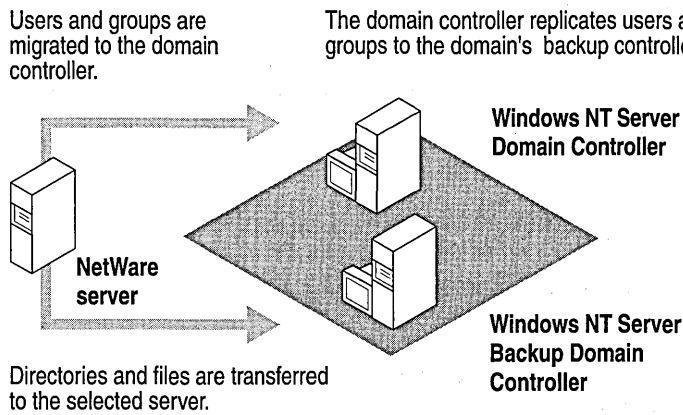
Similarly, if volumes on NetWare servers have the same name and you are transferring the volumes to a single Windows NT Server computer, you should plan how you want the volumes organized on the Windows NT Server computer. By default, the Migration Tool merges all volumes of the same name as a single shared folder, but you can also transfer each volume to a different share, or transfer each volume to a different folder of the share.

Comparing Network Models

On Windows NT Server networks, servers can share account information when they are organized into one or more domains. (A *domain* is a collection of servers that share a common user account database and security policy.) In a domain, one server—the *primary domain controller* (PDC)—stores all accounts and replicates changes to the backup domain controllers in the domain.

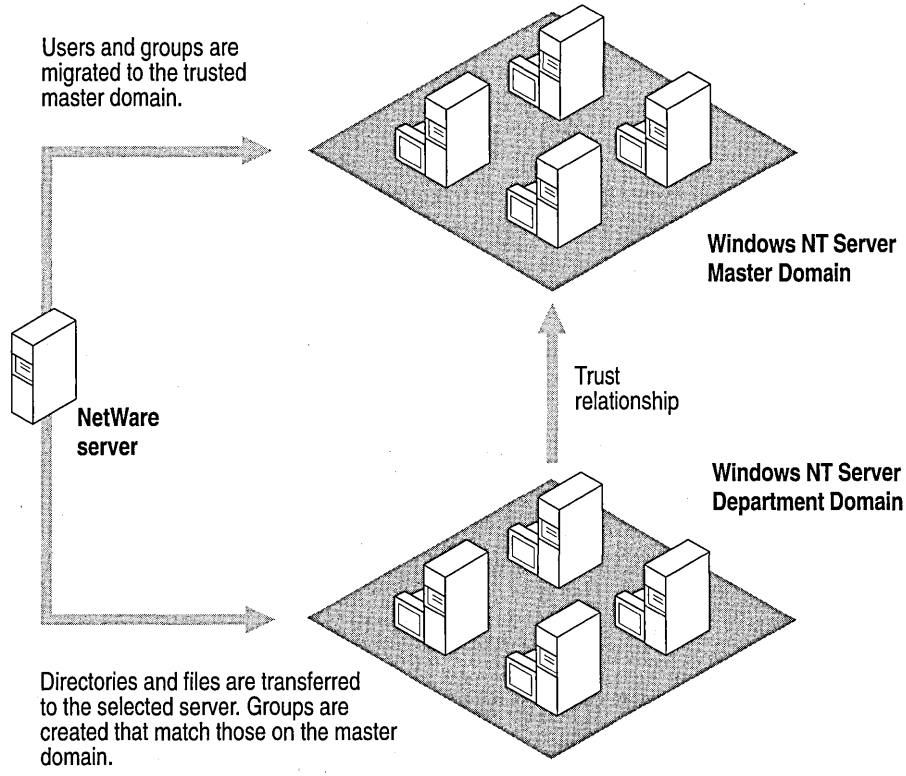
Domain organization allows a group of computers to behave as though they were a single server. Users can reach all domain resources with a single username and password. Account administration on a domain is easy because changes are made only once, and they affect all servers in the domain. For the purposes of migration planning, you can think of a domain as an expansion of the NetWare bindery to a larger organizational unit.

When you transfer user and group accounts from a NetWare server to a computer running Windows NT Server, the Migration Tool automatically creates the accounts on the PDC of the server's domain. At the end of the migration process, accounts are replicated automatically to the backup domain controllers in the domain.



For larger networks, you can link domains by establishing trust relationships between them. Once linked by trust, accounts in one domain can be used in another. For centralized administration, you can create a *master domain*, a single domain where all user accounts and global group accounts are stored. You can then use trust relationships to link each of the domains on the network to the master domain. When users log on and are authenticated by the master domain, resources throughout the network are available to them, yet all account information remains centralized for easy administration.

So that you can transfer user and group accounts from a NetWare server to a Windows NT Server master domain, the Migration Tool allows you to specify the domain to which accounts are transferred.



For more information on network security and domains in Windows NT networking, see the *Windows NT Server Concepts and Planning Guide.*

Comparing User Accounts

User accounts on NetWare and Windows NT Server contain the same basic information: a username, a password, and the user's full name. Accounts also perform the same function: They establish a user's identity on the network. Both network operating systems support a range of restrictions that allow you to control user accounts and enable you to put user accounts into groups.

Account Restrictions

On NetWare, most default account restrictions are set using the Supervisor Options and can be changed for individual user accounts. On Windows NT Server, some account restrictions are set individually for each user account, whereas others—called *account policies*—have a single setting that is enforced for all accounts in the domain.

When the Migration Tool transfers user accounts, restrictions that can be modified for each Windows NT Server user account are transferred individually from each NetWare user account. For setting Windows NT Server account policies, you have two options:

- To transfer these settings from the NetWare server's Supervisor account (the default).
- To *not* transfer these settings from the NetWare server and, instead, use the Windows NT Server existing account policies.

The following tables summarizes NetWare account restrictions, their Windows NT Server equivalents, and how they are transferred. The first table is for migrations to Windows NT Server computers that do not run FPNW, and the second shows the additional account restrictions migrated to servers that do run FPNW.

Transferring Account Restrictions to a Server Not Running File and Print Services for NetWare

NetWare Account Restriction	Windows NT Equivalent	How Transferred
Expiration Date	Expiration Date	By individual user account
Account Disabled	Account Disabled	By individual user account
Limit Concurrent Connections	None	Not transferred
Require Password	Permit Blank Password	As policy for all accounts
Minimum Password Length	Minimum Password Length	As policy for all accounts

(continued)

Transferring Account Restrictions to a Server Not Running File and Print Services for NetWare

Force Periodic Password Changes	Password Never Expires	By individual user account
NetWare Account Restriction	Windows NT Equivalent	How Transferred
Days Between Forced Changes	Maximum Password Age	As policy for all accounts
Grace Logins	None	Not transferred
Allow User to Change Password	User Cannot Change Password	By individual user account
Require Unique Passwords	Password Uniqueness	As policy for all accounts
Station Restrictions	None	Not transferred
Time Restrictions	Logon Hours	By individual user account
Intruder Detection/Lockout	Account Lockout	As policy for all accounts
User Disk Volume Restrictions	None	Not transferred

Additional Account Restrictions Transferred to Servers Running File and Print Services for NetWare

NetWare Account Restriction	**Windows NT (With FPNW) Equivalent**	**How Transferred**
Limit Concurrent Connections	Limit Concurrent Connections	By individual user account
Grace Logins	Grace Logins	By individual user account
Station Restrictions	Station Restrictions	Not transferred
Login Scripts	Login Scripts	By individual user account

The following sections provide further details on how some account restrictions are transferred and describes the defaults, if any, on each system.

Expiration Date
: Both NetWare and Windows NT Server support expiration dates after which the account cannot log on. Note that the User Manager for Domains tool in Windows NT Server shows the last day an account is valid, whereas NetWare utilities show the first day the account is expired.

Note In this release, NetWare accounts with expiration dates later than January 1, 2000, are given expiration dates of February 6, 2006 when migrated to Windows NT Server. Accounts with no expiration dates, or with expiration dates of December 31, 1999 or earlier, are not affected.

Limit Concurrent Connections
: NetWare supports limiting a user's concurrent network connections. Windows NT Server itself does not support this restriction, so this information is transferred only if the server being migrated to runs FPNW.

Require Password
: On Windows NT Server, a password is not required when the account policy allows blank passwords

Minimum Password Length
: The NetWare default is 5 characters; the Windows NT Server default is 6.

Force Periodic Password Changes
: The NetWare default is 40 days; the Windows NT Server default is 42 days.

Grace Logins
: The number of times a user can log on after his or her password has expired. Windows NT Server itself does not support this feature, so this information is transferred only if the server being migrated to runs FPNW.

Require Unique Passwords
: The number of different passwords required before the system allows reuse of one. NetWare requires 8 different passwords. The Windows NT Server default is 5 and can be set from 1 to 8.

Station Restrictions
: *Station restrictions* limit the NetWare client computers from which a user can log in. Computers are specified according to their network and node addresses. Windows NT Server itself does not support these NetWare client restrictions. FPNW provides a way for you to set station restrictions on users, but existing station restrictions are not transferred by the Migration Tool.

  Windows NT Server supports a similar feature for restricting users to certain Microsoft client computers.

Time Restrictions

Time restrictions specify the hours during which a user can log in to the network. On NetWare, time restrictions are set in half-hour blocks. On Windows NT Server, they are set in hour blocks. The Migration Tool adjusts blocks set at the half hour to the whole hour when transferring time restrictions. For example, if the NetWare restriction allows a user to log on between 7:30 A.M. and 7:30 P.M., the user will be able to log on between 7:00 P.M. and 8:00 P.M. on Windows NT Server.

Intruder Detection/Lockout

When intruder detection and lockout is in effect, the specified number of unsuccessful logon attempts are allowed before the account is locked for the specified amount of time. By default, NetWare allows 7 attempts before locking the account; Windows NT Server (if intruder lockout is enabled) allows 5 attempts.

Comparing Administrative Accounts

On a NetWare network, the Supervisor account has complete control over the network, and you can grant limited administrative privileges to other users and groups by adding them to the lists of managers and operators. Similarly, on a Windows NT Server network, the administrator and members of the Administrators group have complete control of the network, and you can grant limited administrative privileges to users and groups by adding them to other built-in administrative groups.

For more information on the use of administrative groups in Windows NT Server, see the *Windows NT Server Concepts and Planning Guide.*

Supervisor

On a computer running Windows NT Server, members of the Administrators group are functionally similar to the NetWare Supervisor. To grant a user full administrative privileges, add the user to the Administrators group.

By default, when transferring user accounts, the Migration Tool does not add accounts that have Supervisor rights to the Administrators group. However, you can choose to do so.

Workgroup Manager and User Account Manager

Because user account administration is centralized on a Windows NT Server domain, there is no need to delegate account administration to individual users who have administrative power on a particular server. When transferring accounts, the Migration Tool does not grant any kind of Windows NT Server administrative rights to accounts that were Workgroup or User Account Managers.

The closest Windows NT Server equivalent to the NetWare Workgroup Manager and User Account Manager is the Account Operators group. Account Operators can create, delete, and manage user and group accounts (except administrative accounts and groups).

File Server Console Operator

The closest Windows NT Server equivalent to the NetWare Console Operator is the Server Operators group. However, because Server Operators have greater power than Console Operators, the Migration Tool does not transfer NetWare Console Operators to the Windows NT Server Operators group.

In addition to being able to shut down the server, broadcast messages, see connection information, and set the system date and time, Server Operators can also back up and restore files and folders, lock and unlock the server, and share and stop sharing folders. Unlike Console Operators, whose control can be restricted to a single server, Server Operators have abilities on every server in the domain.

Print Server Operator and Print Queue Operator

The NetWare Print Server and Print Queue Operators are equivalent to the Windows NT Server Print Operators group. On a Windows NT Server network, the functionality represented by NetWare printers and print queues is integrated and administered from the Printers folder. Windows NT Server Print Operators can perform all of the tasks of NetWare Print Server and Print Queue Operators, including the ability to change queues and printer forms as well as manipulate the jobs within a queue.

The Migration Tool automatically adds users and groups who are Print Server Operators to the Windows NT Server Print Operators group. However, because adding Print Queue Operators to the Windows NT Server Print Operators group would grant them more authority than they currently have, the Migration Tool does not transfer users who are only Print Queue Operators to any Windows NT Server group.

Comparing Folder and File Security

When you use the Migration Tool to transfer folders and files from a NetWare server to a Windows NT Server computer, their effective rights are translated to the equivalent Windows NT Server permissions. Windows NT Server security is supported through the NTFS file system. To preserve security, you must transfer files to an NTFS volume.

Supervisors on NetWare and Administrators on Windows NT Server have complete access to all folders and files; note, however, the Administrator does not automatically have *immediate* access. The owner of a folder or file (most often the user who created the folder or file) controls its use. The owner can set permissions that deny access to the Administrator. However, an Administrator always has the right to take ownership: This protects the system.Transferred ownership cannot be returned; users who check the ownership of their folders and files can see whether an administrator has taken control of them.

For more information on Windows NT Server folder and file security, see the *Windows NT Server Concepts and Planning Guide.*

Folder Rights

The effective rights for folders are mapped to the following Windows NT Server permissions:

Folder Rights

NetWare Folder Rights	Windows NT Server Folder Permissions
Supervisory (S)	(All) (All)
Read (R)	(RX) (RX)
Write (W)	(RWXD) (RWXD)
Create (C)	(WX) (not specified)
Erase (E)	(RWXD) (RWXD)
Modify (M)	(RWXD) (RWXD)
File Scan (F)	(RX) (not specified)
Access Control (A)	(P) (P)

File Rights

Windows NT Server does not support the Create (C) and File Scan (F) rights for files. These rights are ignored when files are transferred.

After being transferred from NetWare to Windows NT Server, a file is owned by the Windows NT Server group Administrators.

The effective rights for files are mapped to the following Windows NT Server permissions:

File Access Rights

NetWare File Rights	Windows NT Server File Permissions
Supervisory (S)	(All)
Read (R)	(RX)
Write (W)	(RWXD)
Erase (E)	(RWXD)
Modify (M)	(RWXD)
File Scan (R)	Does not map.
Access Control (A)	(P)

Comparing File Attributes

The Migration Tool maps NetWare file attributes to their Windows NT Server equivalents when transferring files. Note that the following NetWare file attributes are not supported by Windows NT Server and are ignored: Copy Inhibit (C), Delete Inhibit (D), Execute Only (X), Indexed (I), Purge (P), Rename Inhibit (R), Read Audit (Ra), Shareable (Sh), Transactional (T), and Write Audit (Wa). The following table shows how the supported NetWare file attributes map to Windows NT Server file attributes:

File Attributes

NetWare File Attributes	Windows NT Server File Attributes
Read Only (Ro)	Read Only (R)
Archive Needed (A)	Archive (A)
System (SY)	System (S)
Hidden (H)	Hidden (H)
Read Write (Rw)	None — files without the R attribute can be read and written to.

Performing a Migration

To migrate a NetWare server to a computer running Windows NT Server, follow these general steps. The following sections of this manual provide more general information about these steps and the use of the Migration Tool.

For more detailed step-by-step procedures, see Running a Migration in the online Help.

1. After starting the Migration Tool, select the NetWare server(s) you want to migrate from and the computer(s) running Windows NT Server to migrate to.
2. Click **User Options** to specify how users and groups will be transferred from the NetWare server to Windows NT Server.
3. Click **File Options** to specify which volumes (if any) on the NetWare server to transfer files and folders from. For each volume you migrate, you can select which folders and files to actually transfer to Windows NT Server.
4. Click **Trial Migration** to generate log files that show exactly how the NetWare server(s) would be migrated, given the current settings. Examine these logs to make sure that the computer running Windows NT Server will receive the users, groups, files, and other information in the way you expect.
5. If necessary, adjust some settings in **User Options** and **File Options**, then click **Trial Migration** again until the logs show the information you want.
6. Click **Start Migration** to perform the migration.

You do not have to complete all these steps at one time. All settings—including the list of servers and the migration options specified for groups, users, folders, and files—are saved when you exit the Migration Tool before running a migration. The next time you start the utility, the Migration Tool restores settings. You can also save a list of servers and migration options in a configuration file (with a .cnf extension).

Starting the Migration Tool

When you start the Migration Tool for the first time, the **Select Servers For Migration** dialog box appears. From it, choose the NetWare servers and Windows NT Server computers you want to use. Migration options for users, groups, folders, and files are set to their defaults.

To select a NetWare server to migrate, you must have Supervisor rights on the server. You should not have any drive mappings to the NetWare server from the computer you are running the Migration Tool from. To transfer data to a computer running Windows NT Server, you must be a member of the server's Administrators group.

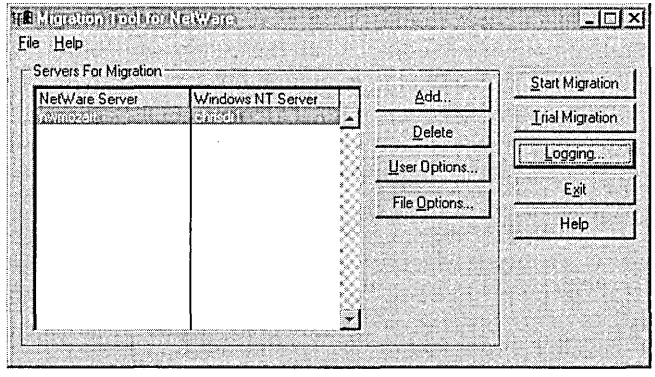
If you quit the Migration Tool before running a migration, the current list of servers and the migration settings are saved until the next time you start the utility.

Note To run the Migration Tool and to access NetWare servers, the Windows NT Server computer must be running the NWLink IPX/SPX Compatible Transport and the Gateway Service for NetWare.

▶ **To start the Migration Tool**

1. From the **Start** menu, click **Run**.
2. In the **Open** box, type **nwconv**, and click **OK**.

   If this is the first time you have started the Migration Tool since running a migration, the **Select Servers For Migration** dialog box appears. From it, select the servers you want to migrate. To see the Migration Tool's main window, either select a pair of servers or cancel the **Select Servers For Migration** dialog box.



Selecting Servers for Migration

You can select one or more NetWare servers to migrate and one or more Windows NT Server computers to accept the data from the NetWare servers. For example, you might want to reproduce the configuration of a single NetWare server by transferring the data from it to a similarly configured Windows NT Server computer, or you might want to replace more than one NetWare server with a single Windows NT Server computer.

Selecting servers is a two-step process:

1. Click **Add** to add server names to the list in the Migration Tool main window.
2. For each specific migration, select a pair of a NetWare server and a computer running Windows NT Server in the **Servers For Migration** area of the Migration Tool main window. The migration you perform applies only to the servers selected in this area.

Note To select a NetWare server to migrate, you must be logged on to the server as a Supervisor. To transfer data to a Windows NT Server computer, you must be a member of the Administrators group.

Specifying How to Migrate Users and Groups

This table summarizes the available migration options, which are described more fully in the text following the table.

Options for Transferring Users and Groups

Default options	Other options
Transfer groups and users	Transfer folders and files only
Assign null passwords to transferred accounts, allowing them to log on without a password	Set password for each account to the account's username
	Set password for all accounts to a specified password
	Use a mapping file to specify a password for each account
Allow transferred users continued use of the password assigned to them	Force users to change the password when they log in
Do not overwrite existing Windows NT Server user accounts when there is a name conflict, but log the conflict	Do not overwrite existing user accounts and do not log conflicts
	Overwrite existing user accounts and log conflicts
	Create a new user account when there is a conflict by adding a prefix to the username and log the conflict
	Use a mapping file to transfer conflicting accounts to new user accounts

(continued)

Options for Transferring Users and Groups

Default options	Other options
Do not overwrite existing group accounts and do not log conflicts	Do not overwrite existing group accounts and log conflicts
	Create a new group account when there is a conflict by adding a prefix to the group name and log the conflict
	Use a mapping file to transfer conflicting accounts to new group accounts
Transfer NetWare account restrictions for passwords and intruder lockout	Use Windows NT Server account restrictions
Do not transfer accounts with Supervisor rights to the Windows NT Server Administrators group	Transfer accounts with Supervisor rights to the Windows NT Server Administrators group
Transfer user and group accounts to the domain of the selected Windows NT Server computer	Transfer user and group accounts to a trusted master domain

Setting Password Options

Because passwords from a NetWare server are encrypted, they cannot be transferred. (The Migration Tool cannot read them.) To set the new passwords, use one of the following methods:

- Assign all accounts a null password (users will be able to log on without specifying a password).
- Set each account's password to be the same as its user name.
- Specify a single password to assign to all transferred accounts.
- Use a *mapping file*, which lists each account being migrated and specifies the new password for each account. For more information on creating and using a mapping file, see "Mapping Accounts," later in this chapter.

You also specify whether migrated users must change their passwords the next time they log on. (By default, they must.)

Handling Username Conflicts

By default, when you transfer users from NetWare to Windows NT Server, users with names that already exist on the Windows NT Server domain are not transferred. This ensures that existing Windows NT Server accounts are not changed. Conflicts are recorded in the Error.log file.

Instead of using the default, you can choose one of the following responses to conflicts:

- Transfer no account information. (If you have transferred accounts from one of several NetWare servers having identical accounts, you might want to select this option when you are transferring accounts from the additional servers.)
- Overwrite existing Windows NT Server account information. (If you choose this option, remember that passwords and other account information for current users on the Windows NT Server domain will be changed.)
- Create a new account on the Windows NT server or domain by adding a prefix to the current username.

If you want complete control over transferring usernames, you can also use a mapping file. For more information, see "Mapping Accounts," later in this chapter.

Handling Group Name Conflicts

Because both NetWare and Windows NT Server groups are used primarily to organize user accounts, no information needs to be transferred with the group name. Consequently, by default, when the Migration Tool transfers a group name that already exists on the Windows NT Server domain, it simply adds the listed user accounts from the NetWare server to the existing Windows NT Server group and does not log an error.

Instead of using the default, you can handle group name conflicts in the following ways:

- Record them in the Error.log file (and still add the users from the NetWare group to the existing Windows NT Server group).
- Add a prefix to the current group name, thereby creating a new group name on the Windows NT Server domain. User accounts from the NetWare group are added to the new group.

  Use this option when you are transferring groups from multiple NetWare servers to a single Windows NT Server domain and there are identical group names on the NetWare servers whose accounts you do not want to merge into one group. For example, if you are migrating all servers in the Sales department to a single domain and the servers use identical group names for different groups of users, you can specify a different prefix for group name conflicts for each server you migrate. You could specify NAT- when migrating the server used by National Sales and INTER- when migrating the server used by International Sales, creating new groups on the Windows NT Server domain called NAT-SALES and INTER-SALES.

If you want complete control over transferring group names, you can also use a mapping file. For more information, see "Mapping Accounts," later in this chapter.

Transferring Account Restrictions

By default, when you transfer user accounts from NetWare to Windows NT Server, the account restrictions of the NetWare Supervisor account are transferred and become the security policy on the Windows NT Server domain. Alternatively, you can choose not to transfer account restrictions and instead, retain the existing policy settings of the domain.

The following NetWare account policy settings are affected:

- Require Password
- Minimum Password Length
- Require Password Change
- Password Reuse
- Intruder Lockout

Transferring Administrative Rights

By default, groups and users with Supervisor rights are transferred to Windows NT Server without administrative privileges. Alternatively, you can add them to the Administrators group on Windows NT Server. Such users have power equivalent to NetWare Supervisors.

For more information on Windows NT Server and NetWare administrative accounts, see "Comparing Administrative Accounts," earlier in this chapter.

Mapping Accounts

Rather than setting general options for names and passwords in the **User and Group Options** dialog box, you can use a mapping file to specify how account information is transferred to a server running Windows NT Server.

You can either create a mapping file before you start a migration, or you can use the Migration Tool to create the mapping file while setting migration options. Using the Migration Tool to create the file is easier; the required section headings and the names of all user and group accounts from the NetWare server are automatically put into the file. After you use the Migration Tool to create the mapping file, you can edit the file.

To create a mapping file using Migration Tool, click **Create** in the **User and Group Options** dialog box. You can then edit the file you have created, specifying a new name and password for each user you are transferring and a new name for each group. Entries not getting a new name are transferred without change. The Migration Tool prompts you to edit the file as soon as it has been created; however, you can edit it at any time using a text editor such as Notepad.

The mapping file format consists of two sections, headed by **[users]** and **[groups]** lines. Each user or group being moved has one line. Each line in the user section has the following format:

old_username, *new_username*, [*password*]

The *old_username* is the current username of the user on the NetWare server. The *new_username* is the user's new name, and *password* is the new password to assign to the user. If you omit a password, the user's new password will be set to null.

For example, to migrate the user account currently named Patricia, rename it to PSmith, and give it a password of Orange, you would put the following line in the [users] section of the mapping file:

```
patricia, psmith, orange
```

To keep the current username of Patricia, you would use

```
patricia, patricia, orange
```

Within the group section, each line lists only the old and new group name:

old_groupname, *new_groupname*

To not propagate a user and group to the domain, simply remove that name from the mapping file.

Remember, usernames must be unique on the server and within the server's domain. Usernames can be up to 20 characters in length and can contain any upper or lowercase characters except the following:

" / \ [ ] : ; | = , + ? < >

Passwords can be up to 14 characters in length. Windows NT Server distinguishes between uppercase and lowercase characters in passwords.

Transferring Accounts to a Windows NT Server Master Domain

Suppose you have a Windows NT Server network where all user accounts are kept in a single master domain, and other domains on the network contain only resources. When you migrate a server running NetWare to Windows NT Server on this network, you can transfer user accounts and groups to the domain controller of the master domain, and transfer folders and files to a server in another domain. (This server would be the one listed in the **Servers For Migration** list in the Migration Tool.)

When you transfer groups to a master domain, they are created as global groups in the master domain and again as local groups on the server specified in the **Servers For Migration** list. The local group on the server contains the global group from the master domain. This allows you to easily add other global groups to the local group later.

Folders and files transferred to Windows NT Server are secured by setting permissions for the transferred users and local groups.

For more information on domains, and local and global groups, see the *Windows NT Server Concepts and Planning Guide.*

Migration Options for Folders and Files

The following table summarizes the options you can set for the transfer of volumes, folders, and files from the NetWare server to Windows NT Server. The following sections provide more details about these options.

Options for Transferring Files and Folders

Default options	Other options
Transfer files and folders	Transfer groups and users only
Transfer all NetWare volumes	Select volumes to transfer
Transfer to default destination shares	Change destination shares
Transfer all files and folders except NetWare system folders and files	Select folders and files to transfer
Do not transfer system files	Transfer system files in selected folders
Do not transfer hidden files	Transfer hidden files in selected folders

Selecting Volumes to Transfer

By default, all NetWare volumes are transferred. Alternatively, you can select specific NetWare volumes to transfer.

If you create a new volume on a NetWare server after you have selected which volumes, folders, and files to transfer, you must add it to the list manually.

Specifying a Destination Share

The Migration Tool transfers the contents of each NetWare volume to a Windows NT Server shared folder with the same name. Alternatively, you can specify a different shared folder as a destination. If the shared folder you specify does not exist, the Migration Tool creates it during migration.

Important Before you migrate folders and files to Windows NT Server, set the permissions for the Windows NT Server folder to which you are migrating. These permissions will be set on every level of folder that is transferred from the NetWare server. If you are migrating to an existing folder, set the permissions on that folder. Otherwise, set the permissions on the root of the volume.

When you transfer the contents of multiple NetWare servers to a single computer running Windows NT Server, the various NetWare servers might use the same volume names. In such a case you might want to specify a destination other than the default so that the files and folders from the various servers are not all merged into a single folder on the computer running Windows NT Server. For example, if all the servers contain a folder called PUBLIC, by default, all the files and folders from the PUBLIC folders are transferred to a single PUBLIC share. Instead, you can transfer each PUBLIC volume to a different share or to a different folder below the PUBLIC share.

Selecting Folders and Files to Transfer

By default, all files are transferred except files located on the NetWare administrative volumes (\SYSTEM, \LOGIN, \MAIL, and \ETC), and hidden and system files. Alternatively, you can select which folders and files to transfer.

If files are added to a NetWare volume after you have finished selecting folders and files, they will be transferred only if all the files in that folder are selected for transfer. In other cases, you must add them to the list of files for transfer.

Only as much of the folder structure as necessary is transferred. If, for example, you have not selected any first level folders for transfer, the first level of the folder structure is not transferred.

Transferring Hidden and System Files

By default, files with the Hidden (H) and System (SY) attributes are not transferred. Alternatively, you can select individual hidden and system files to transfer, or you can transfer all hidden and system files.

Migrating Logon Scripts

If you are migrating to a server that runs FPNW, use the Migration Tool to migrate users' logon scripts. Be sure to transfer files and folders, and include the NetWare server's MAIL folder in the list of folders being migrated.

The next time the user logs on to the server from a NetWare client, the logon script runs as the user's personal logon script. A system logon script is also available; it is the file Net$dat.log in the SYSVOL/PUBLIC folder.

Note Even if you transfer the contents of the MAIL folder to a server that does not run FPNW, the logon script files will be transferred. However, FPNW is required to preserve the user account information that calls the appropriate logon script.

Running a Trial Migration

Before running an actual migration, run a *trial migration* to make sure that users, groups, folders, and files will be transferred as desired. The Migration Tool tracks trial events as though an actual conversion were in progress, generating a set of log files that contain migration information. (Use the logview.exe utility to view and print them.)

Each time you run a trial or a migration, the Migration Tool creates a new set of files with a .LOG extension. The previous .LOG files are renamed using a number for the filename extension.

- Logfile.log contains information on users, groups, and files, including the information that currently exists on the NetWare server.
- Summary.log presents an overview including the names of servers that were migrated and the number of users, groups, and files that were transferred.
- Error.log shows information that the Migration Tool could not transfer, as well as information on system failures that prevented the migration (for example, a lack of disk space).

Review these files to see what information is on the server you are migrating and what trouble spots might affect the migration. Then, before running the migration, you can change options for users, groups, folders, and files so that information is transferred the way you want.

Reviewing the Log File

Logfile.log provides a complete record of the migration that includes both what was successfully transferred and what failed because of an error, including

- **Transfer Options**

  A record of the settings for user, group, and file transfer options.

- **Supervisor Defaults**

  A record of the defaults for the NetWare Supervisor account.

- **Group Information**

  A record of the NetWare groups added to Windows NT Server.

- **User Information**

  By default, the Migration Tool records account information first for the original NetWare account and then for the new Windows NT Server account. For NetWare accounts, this includes information on password and account restrictions as well as additional information such as allowed login times. A similar set of information is recorded for new Windows NT Server accounts.

  To show allowed login times, the log file presents a chart like the one below where asterisks indicate the blocks of time during which a user can log in:

```
Login Times:
 Midnight          AM          Noon          PM
    12 1  2  3  4  5  6  7  8  9  10 11 12 1  2  3  4  5  6  7  8  9  10 11
   +-----------------------------------------------------------------------+
Sun ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Mon ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Tue ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Wed ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Thu ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
Fri ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
```

- **File Information**

  By default, the Migration Tool lists the volumes copied and the number of files copied. You can also record a complete list of files and folders copied that includes information such as file size and date.

Reviewing the Summary File

Summary.log provides statistics for the migration, including

- Names of migrated servers
- Total running time for the migration

  (Note that the running time for a trial migration will be shorter than that for an actual migration, particularly when files are transferred.)

- Total number of users transferred per server
- Total number of groups transferred per server

- Total number of files transferred per server
- Total number of name conflicts
- Total number of errors

Reviewing the Error File

Error.log provides a list of any errors that occurred, including

- Names of user and group accounts that were not transferred successfully
- Network errors, such as the failure to access a server
- System errors, such as a lack of disk space for file transfers

Running a Migration

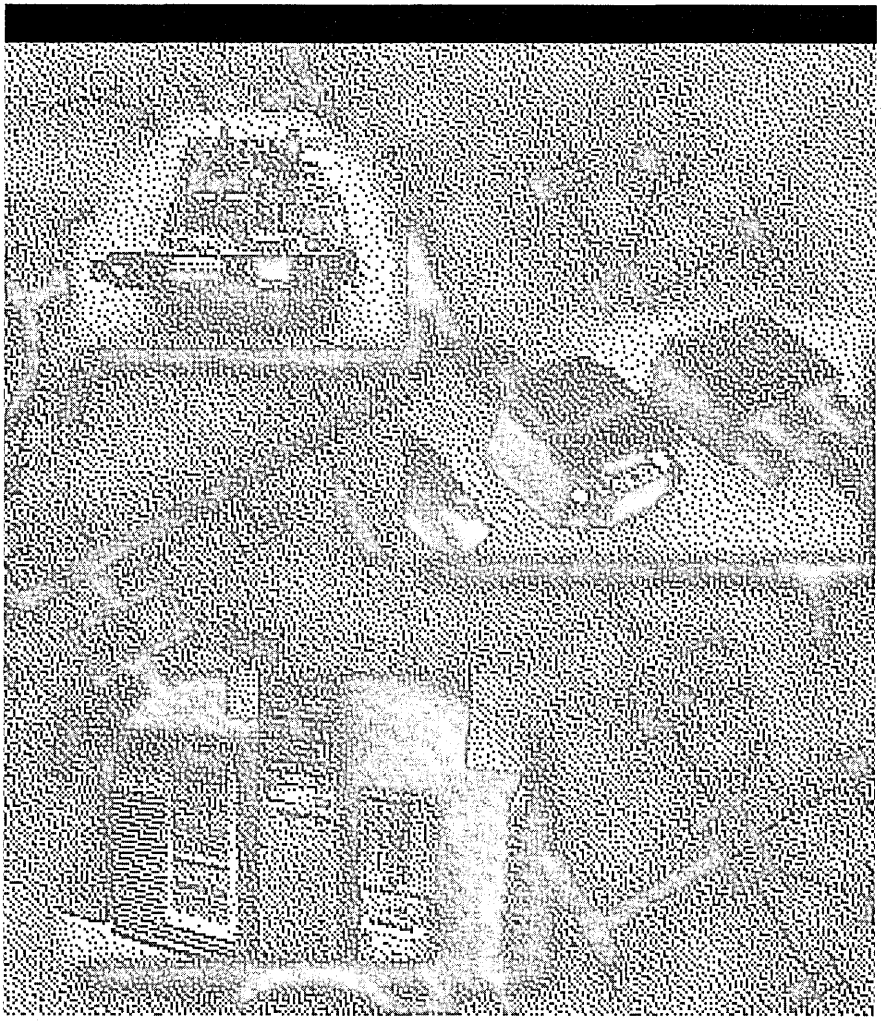
Before running a migration, run a trial migration as described in the previous section. This enables you to see and correct problems such as username conflicts before actually migrating servers.

Important Before running a migration, make sure that all other users have logged off the servers you are migrating and that files on the servers are closed.

To run the migration, click **Start Migration**. When the migration is complete, the Migration Tool displays the log files for review. If you have transferred user and group accounts to a domain, the domain's PDC replicates user and group account information to the backup domain controllers in the domain.

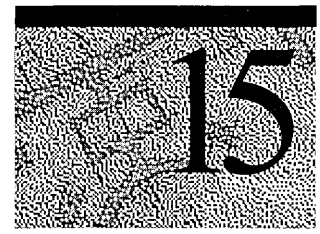
PART 5

Services for Macintosh



CHAPTER 15

Introduction to Services for Macintosh



Microsoft® Windows NT™ Server Services for Macintosh® (SFM) is a thoroughly integrated component of Microsoft Windows NT Server that makes it possible for PC and Apple® Macintosh clients to share files and printers.

You can set up SFM and other components (such as Microsoft Windows NT Server Remote Access Service) when you install Windows NT Server, or you can set them up later. After SFM is set up, a computer running Windows NT Server can also function as an AppleTalk® router. Routing capability is supported for AppleTalk Phase 2.

With SFM, Macintoshes need only the Macintosh operating system software to function as clients; no additional software is required. You can, however, set up the optional user authentication module, which is software that provides a secure logon to the Windows NT Server.

Features

Version 1.0 of LAN Manager SFM made it possible for a LAN Manager server to share files and printers with Macintosh clients. This meant that both PC and Macintosh clients could share resources on the same network. This version of SFM does that and more. Version 4.0 uses the capabilities of Windows NT Server, which include built-in networking services for multiple-domain networks of MS-DOS®–based, Windows™-based, and OS/2® clients. Version 4.0 includes these features:

- Enhanced performance because of better resource use.
- Secured logon, which provides added protection from network *sniffers*. (Sniffers can detect clear-text passwords.)
- Easy-to-use graphical administration tools that are fully integrated into the Windows NT Server File Manager, Print Manager, and Server Manager.
- Printing to non-PostScript® printers.
- Increased number of clients that can be simultaneously connected to the server.

- Compatibility with all computers that can run Windows NT Server, including 80386, 80486, MIPS®, Pentium™, Alpha™, and multiprocessor systems.
- Support of AppleTalk Phase 2, which is available for routers and networking protocols. (AppleTalk Phase 1 is not supported in this version of SFM.)

Note Macintosh Service functionality is still included in File Manager and is not part of the Explorer. After you install SFM, in the Start menu, click Run. In the **Open** box, type winfile and click **OK** to start File Manager. You can also add File Manager to any group in your Start menu by choosing Settings in the Start menu and then clicking **Taskbar**. In the **Start Menu Programs** tab, click **Add**, and type winfile.

What Services for Macintosh Can Do

Using SFM on your network gives you many benefits—including the following:

- File sharing

  For example, some people in your department use Microsoft Excel for Windows. Others prefer using Microsoft Excel for Macintosh. With SFM, these users can work on the same spreadsheet files.

- Printer sharing

  For example, your small network has only one PostScript printer. With SFM, both PC and Macintosh users can have access to the PostScript printer.

  Or your network has two printers for PC clients and two printers for Macintosh clients. However, PC users get frustrated when the PC printers are busy and the Macintosh printers are not, and vice versa. With SFM, all users can send print jobs to all printers, which means users have more choices for getting their work done. Moreover, you can control all of the print queues from a single location—your computer running Windows NT Server or Windows NT Workstation.

- Simplified administration

  For example, you have several Macintoshes that you'd like to put on the network. With SFM, you don't need a Macintosh server: Your computer running Windows NT Server can provide file sharing and file security for your Macintoshes and PCs. And by using your computer running Windows NT Server with Macintosh clients, you have only one list of users to maintain instead of two (one on a computer running Windows NT Server and one on a Macintosh server).

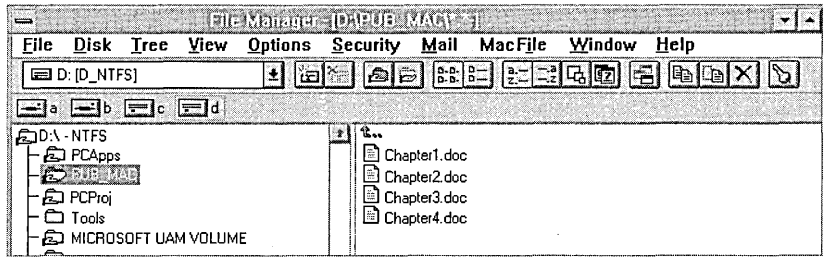
- AppleTalk routing support

  For example, suppose you want to connect an AppleTalk internet (a group of two or more AppleTalk physical networks). With SFM, you can attach networks with Macintosh clients to create an AppleTalk internet.

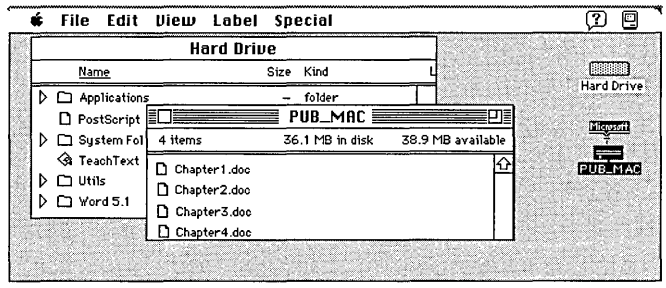
File Sharing

Even though the MS-DOS, OS/2, and Windows NT file systems differ greatly from that of the Macintosh operating system, both PC clients and Macintosh clients can use the same files stored on the server. SFM works in the background to make this possible.

For both Macintosh and PC users, files appear as they usually do: A PC user sees files located in a directory tree structure, and a Macintosh user sees files located in the familiar Macintosh folder structure.



Windows NT Server File Manager with a shared directory



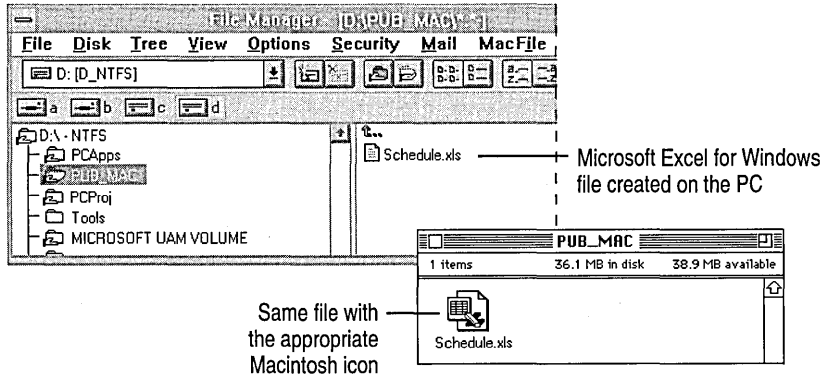
Macintosh Finder™ with the same directory designated as a Macintosh-accessible volume

Using Cross-Platform Applications on PCs and Macintoshes

For many applications that have versions for PCs and for Macintoshes, users of both versions can work on the same data file using SFM. When Macintosh users view directories on the server containing these data files, they see the files represented by the appropriate icon.

For example, a person using a PC version of Microsoft Excel can create a spreadsheet file, and then store it on the server in a shared directory that also is configured as a Macintosh-accessible volume. A Macintosh user who opens that folder sees the file represented by the Macintosh icon that represents a Microsoft Excel spreadsheet. The Macintosh user can double-click the file icon, and Microsoft Excel for Macintosh starts and opens the file. The Macintosh user can modify the file, and then save it. When the PC user opens the file, the modified version of the file appears.

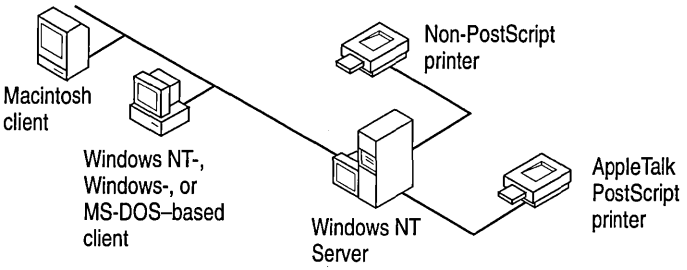
SFM uses *extension-type associations* to display PC files with the correct icon when the Macintosh user is viewing them in the Finder. For example, the Macintosh user sees a Microsoft Excel for Macintosh document icon for a Microsoft Excel for Windows file (a *.XLS file).



SFM comes with extension-type associations already defined for many applications. You can also add extension-type associations. For information and instructions on how to add more associations, see Chapter 19, "Configuring Services for Macintosh."

Printer Sharing

With SFM, Macintosh and PC users can send print jobs to any printer attached to a computer running Windows NT Server, as well as to PostScript printers that register themselves as a LaserWriter on the AppleTalk network.



SFM provides additional benefits for Macintosh users who use AppleTalk printers—it provides *spooling*. With spooling, Macintosh users can start other tasks as soon as they send a print job to the computer running Windows NT Server, where print jobs are stored until a printer becomes available. Without spooling, users must wait until the print job completes before doing anything else.

Simplified Administration

With *simplified administration* you have one set of users to maintain instead of separate user accounts on the Macintosh server and the computer running Windows NT Server. It also ensures a consistent file-level security for PC and Macintosh users.

SFM translates file permissions, which adds a level of security to your network. SFM translates Windows NT file permissions and Macintosh-style permissions (referred to as *access privileges* by Macintosh users). A Macintosh user sets permissions according to the Macintosh scheme; SFM translates these to Windows NT permissions. The reverse is also true: Windows NT permissions set by PC users are translated to Macintosh-style permissions for Macintosh users.

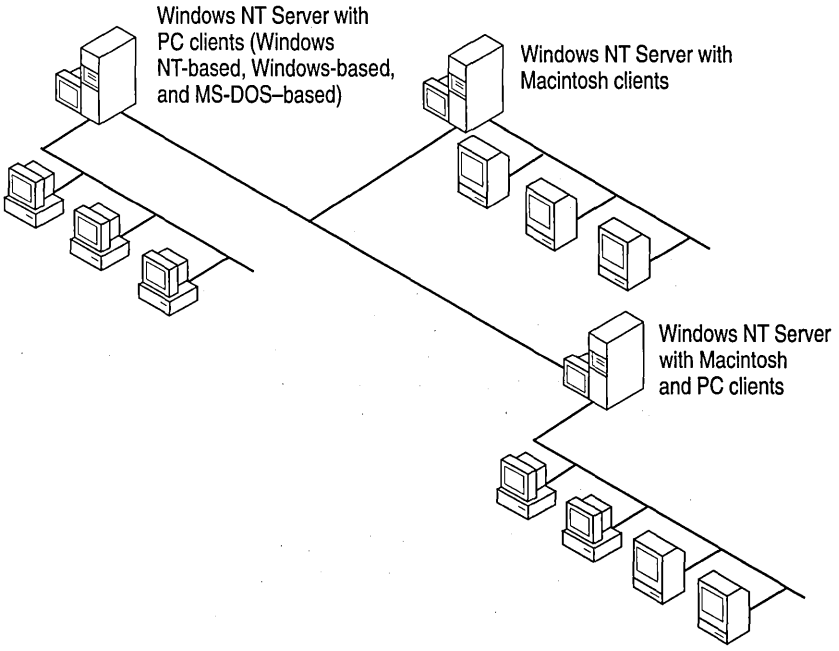
Both Administrators and Server Operators can administer SFM.

AppleTalk Routing Support

With SFM, the computer running Windows NT Server can also provide routing and seed routing support. An AppleTalk router broadcasts routing information, such as network addresses, and keeps track of and directs data packets on AppleTalk networks. Seed routers perform these functions and also seed the physical networks on which they reside. Seeding a network means establishing and initializing the network address information for that network.

You can install an unlimited number of network adapters to a computer running Windows NT Server to add to an AppleTalk *internet*, which is a group of two or more physical networks connected by one or more routers.

For more information about routing and internets, see Chapter 17, "Planning Your AppleTalk Network."



System Requirements

To set up SFM, you need a PC that is running Windows NT Server; to make full use of SFM, you need Macintosh clients. Requirements for each of these follow.

In addition, SFM supports version 6.*x* (or later) of the LaserWriter printer driver and versions 2.0 and 2.1 of the AppleTalk Filing Protocol.

Requirements for Computers Running Windows NT Server

Setting up SFM with Windows NT Server requires that your server meet specifications for both Windows NT Server and for SFM.

For information about the Windows NT Server requirements, refer to the *Windows NT Server System Guide.*

SFM requires these additions to the computer running Windows NT Server:

- 2 megabytes (MB) of extra hard disk space
- A Windows NT file system (NTFS) partition in order to create directories (Macintosh-accessible volumes) that can be used by Macintosh clients

Requirements for Macintosh Clients

All Macintosh computers that can use AppleShare® (the Apple networking software for the Macintosh) can use SFM. These include all Macintoshes except the Macintosh XL and Macintosh 128K. To use SFM, the Macintosh must have version 6.0.7 or later (including System 7™ or higher) of the Macintosh operating system.

The following are known Macintosh client limitations:

- For Macintosh clients older than version 7.5, the volume size must not exceed 2 GB.
- For version 7.5 or later Macintosh clients, the volume size must not exceed 4 GB.

Note The AppleTalk Filing Protocol (AFP) has the following limitations: a maximum volume size of 4 GB, a maximum file size of 2 GB, and a maximum number of files and folders (65,536). For more information, see the Apple Tech Info Library.

SFM supports LocalTalk®, ethernet, token ring, and Fiber Distribution Data Interface (FDDI). Ethernet and token ring are commonly used when integrating Macintoshes into PC networks. For more information about these networks, see Chapter 17, "Planning Your AppleTalk Network."

Where to Go from Here

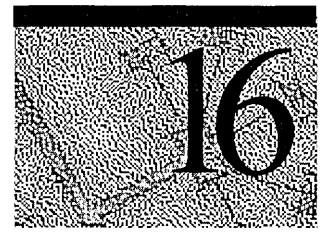
For more conceptual information about SFM, read Chapter 16, "How Services for Macintosh Works."

For instructions on setting up SFM and a discussion of how to plan your Apple internet setup, see Chapter 17, "Planning Your AppleTalk Network."

For step-by-step instructions that explain how to administer SFM after it is set up and how to set up files and printers to be shared by Macintosh and PC users, see Chapter 21, "Working with Macintosh-Accessible Volumes."

CHAPTER 16

How Services for Macintosh Works



The two main services for Services for Macintosh clients are File Server for Macintosh and Print Server for Macintosh. The file server enables Macintosh users to access files stored on the computer running Windows NT Server. The print server enables Macintosh users to print to any printer connected to the computer running Windows NT Server and to spool print jobs for AppleTalk printers such as the LaserWriter.

This chapter explains how these services work. It also explains how Macintosh users gain access to the computer running Windows NT Server and how security applies to Macintosh users. For instructions on how to administer and manage these services and the other tools added to Server Manager and Control Panel, see Chapter 21, "Working with Macintosh-Accessible Volumes."

How Files Are Shared

With SFM, both PC users and Macintosh users can easily share files stored on the server. Shared files appear as expected to PC users and to Macintosh users. For example, when an MS-DOS user views these shared files, the filenames follow the MS-DOS standard naming convention, whether or not they were created that way by a Macintosh user. When a Macintosh user views the files, they appear as Macintosh files, like files on the Macintosh client itself or on Macintosh servers running AppleShare.

How Shared Files Appear to Users

On a computer running SFM, files are stored in shared directories or in Macintosh volumes. For a file to be accessible to PC clients, it must be in a shared directory (or in a subdirectory of a shared directory). Each server can have one or more shared directories. Each shared directory on a server is assigned a unique *share name*, which is sometimes referred to simply as a *share*.

With SFM, Macintosh users cannot automatically gain access to all shares. To make a directory—and consequently its subdirectories (which may or may not be shared on the Windows NT system network)—available to Macintosh users, the administrator must designate the directory as a *Macintosh-accessible volume*.

Note Some PC users are familiar with the terms *volume* and *volume labels* as they relate to a hard disk partition. In this manual, however, a volume is either a directory designated as both a share and a Macintosh-accessible volume (meaning that both types of clients can gain access to the files in the volume) or a directory available only to Macintosh users on the network. There is one exception to this convention: when CD-ROM or Compact Disc Filing System (CDFS) volumes are mentioned.

Within a directory that is both a share and a Macintosh-accessible volume, networked PC users see directories and files. In fact, this is what is actually stored on the server's hard disk. To Macintosh users, the volume appears to contain Macintosh files and folders (the Macintosh equivalent of directories). When Macintosh users browse through the files available on the server, they see icons that represent each file and folder.

Macintosh files and folders can have Macintosh filenames, including long names and names containing spaces and other characters. They are not limited to the 8.3 naming convention of the file allocation table (FAT) file system used with the MS-DOS system and some OS/2 computers. The file server and the NTFS translate the names so that users can see them.

How SFM Stores Files

Understanding how Macintosh files work is helpful in understanding how SFM and Windows NT Server present files to both PC and Macintosh users.

Each Macintosh file has two parts, or *forks*: a *data fork* and a *resource fork*. The data fork contains the actual data of the file. The resource fork contains Macintosh operating system information about the file, such as code, menu, font, and icon definitions.

When a Macintosh file is shared on a computer running SFM, the two forks are saved in a single NTFS file.

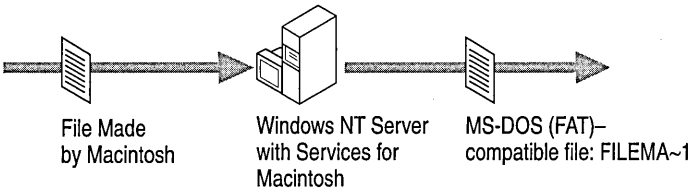
How Filenames Are Translated

There are two types of filename translations to consider when running SFM:

- How Macintosh filenames are maintained and presented to various users
- How the longer NTFS names (more than 32 characters) are presented to the Macintosh user

When a Macintosh user creates a file or a folder on the server and gives it a name, SFM checks it for illegal NTFS characters. If the filename contains illegal NTFS characters, File Server for Macintosh replaces the illegal characters. Otherwise, the original Macintosh name is the same as the NTFS name. Macintosh users see the name as it was created. Windows NT Server users will see the same name, with illegal characters—if any—replaced.

After the file server has replaced illegal NTFS characters, Windows NT Server takes over the file-translation process. Names that are too long for MS-DOS users are shortened to six characters, a tilde (~), and a unique number. Extensions are preserved. For more information about this process, refer to Appendix E, "How Filenames Are Translated," and to the *Windows NT Server Concepts and Planning Guide.*



For example, in a directory and volume called MACFILES, Windows NT Server and Macintosh users see a sample file as *File Made by Macintosh.* When MS-DOS users view the contents of the MACFILES directory, however, they see the short version of the filename: FILEMA~1. More examples follow:

- *Files Made By Macintosh (Old)* is translated to the following:

  ```
  FILEMA~2
  ```

  This prevents duplicate filenames if FILEMA~1 has already been created.
- MARCHSALES.Sales Report.XLS is translated to the following:

  ```
  MARCHS~1.XLS
  ```

  Notice that the extension (.XLS) has been retained. The last period in a name is recognized by NTFS as signaling the extension.

Windows NT users creating long NTFS filenames (up to 256 characters) should name files with 31 characters (the Macintosh limit) or fewer so that Macintosh users can readily decipher the filenames. If an NTFS name is longer than 31 characters, Macintosh users will also see the short name.

Here is a quick summary:

- A file created using the FAT file naming convention appears as created to NTFS users and Macintosh users alike.
- A file created using the 31-character limit of the Macintosh system appears as created to NTFS users. MS-DOS users see a short name.
- A file created using the NTFS 256-character limit appears as created to Macintosh users if it is 31 characters or less. Otherwise, it appears in the shortened form to both MS-DOS and Macintosh users.

Note Because MS-DOS users refer to files created by Macintosh users by the translated short names, you might want to instruct Macintosh users to give the FAT standard names (eight characters, and an optional period and three-character extension) to files and folders that will also be used by MS-DOS users. This prevents MS-DOS users from having to decipher short names.. (For files that only Macintosh users or Windows NT clients will use, Macintosh users can freely use long filenames and folder names.)

Configuring Macintosh-Accessible Volumes

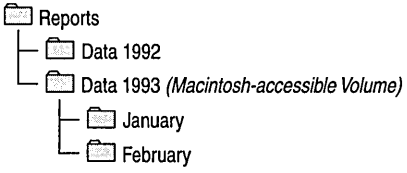
With Windows NT Server, you can share directories on the server in any combination. For example, you can share a single directory twice with two different share names, and you can share a directory with one share name and then share a subdirectory of that directory with another share name.

However, different rules apply when you use SFM to configure Macintosh-accessible volumes. You cannot configure two directories in the same directory tree as volumes.

This means that you cannot do the following when configuring Macintosh-accessible volumes:

- Configure a single directory twice as two different volumes.
- Configure a directory as a volume if it exists anywhere in the directory tree under another directory configured as a volume.
- Configure a directory as a volume if one of its subdirectories, or any subdirectory of one of its subdirectories, is configured as a volume.

For example, consider the directory tree shown in the following illustration. If you configure the DATA1993 directory as a Macintosh-accessible volume, you cannot configure the JANUARY, FEBRUARY, or REPORTS directories as Macintosh-accessible volumes.



The only other directory that can be designated a volume is Data 1992.

All Macintosh-accessible volumes must be on an NTFS partition or a CDFS volume. (The CDFS volumes are, by design, read-only.) The number of volumes visible to the user is determined by the length of the volume names, which must all fit in a buffer in order to be displayed. (The size of the buffer is determined by an underlying AppleTalk protocol.) Volume names can have a maximum of 27 characters. Try to strike a balance between clearly naming volumes so that users can identify them easily and keeping the names short so that all of the volume names can be displayed.

Note To determine the number of Macintosh-accessible volume names that can be displayed, use this formula:

$N * (M+2) <= 4624$

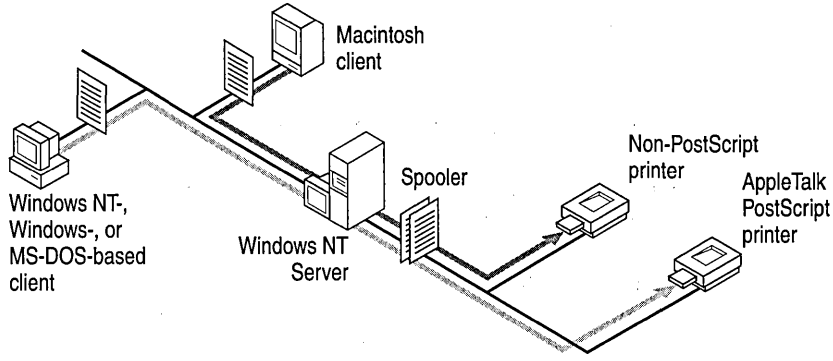
where N is the number of volumes and M is the average length of the names in bytes.

Printing

With SFM, users gain three major printing benefits:

- Macintosh users can print PostScript jobs to non-PostScript printers directly connected to the computer running Windows NT Server. To the Macintosh user, these printers appear like the standard LaserWriter.

- PC users can send print jobs to PostScript printers on the AppleTalk network. PC users can also check print jobs from their clients.
- Macintosh and PC print jobs are spooled before they go to the printer. So, Macintosh and PC users can both send jobs to the printer and then continue working at their computers. This means that users don't have to wait for their jobs to print before using their computers to do other tasks or wait for a printer to be available.



Capturing AppleTalk Printers

When you set up a printer on the AppleTalk network to be used with SFM, you can specify whether SFM will *capture* the printer—that is, prevent the printer from accepting print jobs from any source other than the print server. Capturing, in essence, gives Windows NT Server administrators complete control over the printer.

If a printer will be used exclusively by Windows NT Server, Microsoft recommends that you capture it. Doing so ensures that users don't accidentally bypass the print server and send print jobs directly to the printer or reset the printer, which might cause spooler problems. You'll also avoid "LaserPrep Wars." (For more information on avoiding LaserPrep Wars, see the next section.)

Note that if a source other than the print server prints jobs on the printer, you should not capture the printer. For example, you would not capture printers if you were using Apple LaserShare™ (which provides spooled printing for Macintosh clients) or if you were using a minicomputer that sends print jobs from minicomputer users to the printer.

If a printer is not captured, and both Windows NT Server and another source send jobs to the printer, no jobs will be interrupted; however, while the printer is printing a job from one source, it will appear busy to the other sources.

For information on capturing AppleTalk printers, see Chapter 21, "Working with Macintosh-Accessible Volumes."

Avoiding LaserPrep Wars

With some AppleTalk networks, a condition known as *LaserPrep Wars* causes slow printing performance. SFM solves this problem.

LaserPrep Wars occur when a network has Macintosh clients that use two or more versions of Chooser Packs, which include a PostScript preparation file (also called a LaserPrep file) and a PostScript driver. A printer can use only one version of the LaserPrep file at a time. When a Macintosh user sends a print job to the printer, the Macintosh checks for the printer's version of the LaserPrep file; if the printer currently has a different version than the Macintosh client uses, the Macintosh client sends its version of the LaserPrep file along with the print job, and it instructs the printer to load that file as the printer's resident LaserPrep file. Because Macintoshes with different LaserPrep file versions send print jobs to a printer, different versions of the LaserPrep file are loaded and unloaded on the printer.

Performance problems result because the printer must load and unload versions of the LaserPrep file and then print a startup page each time a different LaserPrep file becomes resident. This can also reduce the life cycle of the printer.

For example, suppose a Macintosh user whose client uses Chooser Pack version 6.0 sends a document to the printer. The LaserPrep version 6.0 file is made resident on the printer. Then, if the next document sent to the printer comes from a client using Chooser Pack version 7.0, the printer must reset, load LaserPrep 7.0, and print a new startup page before printing the document.

SFM solves the LaserPrep Wars problem by sending the LaserPrep file with each job. This extra effort actually improves overall performance: The printer never has to spend time making a LaserPrep resident or printing a startup page.

Note that for printers on an AppleTalk network, LaserPrep Wars are guaranteed to be avoided only if the printer is captured. If the printer is not captured, users who send print jobs directly to the printer, bypassing the print server, can initiate LaserPrep Wars.

LaserPrep Wars are always prevented when printers are attached directly to a computer running Windows NT Server that is set up with SFM.

Network Security

With Windows NT Server and SFM, network security is enforced for Macintosh users in the same way it is enforced for PC users. SFM translates user identification, authentication (passwords), and permissions so that the integrity of the server is maintained regardless of the type of client used. The following sections explain how network security applies to Macintosh users and cover the following topics:

- Windows NT Server user-account restrictions for Macintosh users
- Password protection, including guest logons from Macintosh clients
- Translation of Windows NT Server file permissions to Macintosh-style permissions
- Macintosh-accessible volume passwords

Windows NT Server Accounts for Macintosh Clients

SFM uses the same user accounts database as Windows NT Server. Therefore, if you already have Windows NT Server accounts created for the people who will be using Macintoshes on the network, you don't need to create additional accounts. You must create accounts only for users who don't already have accounts on the computer running Windows NT Server and SFM.

One aspect of Windows NT Server user accounts, the user's *primary group*, applies only to SFM. The user's primary group is the group the user works with most, and it should be the group with which the user has the most resource needs in common. When a user creates a folder on a server, the user becomes the owner. The owner's primary group is set as the group associated with the folder. The administrator or owner can change the group associated with the folder.

Passwords

Macintosh users are logged on to a computer running Windows NT Server in one of three possible scenarios:

- As a guest
- As a user with a clear-text password
- As a user with an encrypted password

Guest Logons

Using SFM, you can set up *guest logons*, which allow users without accounts to log on to the server using a Macintosh. You can specify what access to resources guest logon users have; administrators typically grant guest users fewer permissions than users who have accounts on the server. If the guest logon option is enabled, the server always approves the logon request without requiring a password.

For information on setting up guest logons, see Chapter 22, "Managing the File Server."

Clear-text Passwords

Clear-text password protection is part of the AppleShare client software on Macintoshes. It provides less security than encrypted password protection because the passwords are sent over computer lines and can be detected by *sniffers*—network monitors that can look for passwords. Moreover, the AppleShare passwords can be no more than eight characters in length. Clear-text password protection is offered for Macintosh users who use the standard AppleShare client software or System 7 File Sharing.

Encrypted Passwords

An encrypted, or encoded, password is more secure than a clear-text password. Windows NT Server encodes passwords and stores them so that they cannot be directly stolen from the client itself. Encrypted passwords can be up to 14 characters in length. SFM offers encrypted passwords to Macintosh clients.

For more information about security, see Chapter 21, "Working with Macintosh-Accessible Volumes" and the *Windows NT Server Concepts and Planning Guide.*

Permissions

Access to network files and directories is controlled with *permissions*. With the Windows NT security system, you specify which users can use which shares, directories, and files, and how they can be used. The Macintosh-style permissions differ in that they can be set for folders (directories) only—not files.

The set of permissions available for PC users differs from the set of permissions available for the Macintosh. SFM automatically translates permissionsso that permissions are enforced for both PC and Macintosh users.

The Windows NT Server Administrator account always has full permissions on SFM volumes.

Types of Permissions

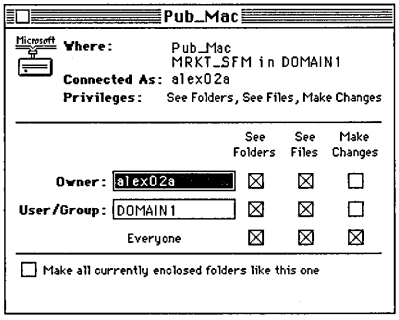
PC users and administrators use Windows NT permissions. Macintosh users set Macintosh-style permissions on the folders they create.

In Windows NT, new files and new subdirectories inherit permissions from the directory in which they are created.

Macintosh files inherit the permissions set on folders. Any Windows NT permission specified for a file will be recognized by the File Server for Macintosh, even though the Macintosh user won't see any indication in the Finder that these permissions exist. The Macintosh has the following four types of permissions for a folder:

- *See Files*, which lets a user see what files are in the folder and read those files
- *See Folders*, which lets a user see what folders are contained in the folder
- *Make Changes*, which lets a user modify the contents of files in the folder, rename files, move files, create new files, and delete existing files
- *Cannot Move, Rename, Or Delete*, which prohibits these actions on a folder

A Macintosh user cannot give these permissions to multiple users and groups. Instead, permissions can be assigned to three categories of user, as shown in the following screen:



- **Owner** The user who created the folder.
- **User/Group** Similar to the Windows NT Server group associated with the folder. Every folder on a server can have one group associated with it at any one time. The group can be a special group like *users* or *administrators*, or it can be any other group on the server.
- **Everyone** All other users of the server, including user accounts with guest access.

The Macintosh security scheme is based on the idea that every folder on a server falls into one of three types: *private information* (accessible only by the owner of the folder); *group information* (accessible by a single workgroup); and *public information* (accessible by everyone).

For example, consider a folder containing information that all members of a certain group should see, but that only one person can change. The person allowed to change the information should be the *Owner* of the folder and should have See Files, See Folders, and Make Changes permissions. The workgroup that uses the folder should be the *Group* associated with the folder and should have only See Files and See Folders permissions. Because no one else needs to see the folder's contents, the *Everyone* category should not be selected.

Although a folder's owner will often be a member of the group associated with the folder, this need not be the case.

With both Macintosh-style and Windows NT Server-style permissions, users' access to folders can be defined differently for each directory and subdirectory within a directory tree. For example, you could give a user See Files, See Folders, and Make Changes permissions for one folder, only the See Files permission for a subfolder of that folder, and no permissions at all for another subfolder.

How File-Level Permissions Are Handled

With Windows NT Server, PC users can assign permissions separately for each file within a directory. The Macintosh, however, does not support file-level permissions. When a file has file-level permissions, those permissions apply to Macintosh users only if the permissions are more restrictive than those assigned for the directory that contains the file.

For example, if a Macintosh user has See Files, See Folders, and Make Changes permissions for a directory (which appears as a folder), the user can read and make changes to files in the directory. However, if that user has only Read permission for any particular file in that directory, the user can only read that file. Because of the Read file-level permission, the user cannot make changes to the file.

Translating Permissions

SFM translates permissions so that those set by a PC user are translated into the equivalent Macintosh permissions, and vice versa. When a PC user sets permissions for a directory, or when a Macintosh user sets permissions for a folder, permissions are translated according to the following table:

Directory and File Permissions Translation

Windows NT permissions	Macintosh permissions
Read	See Files, See Folders (or both)
Write, Delete	Make Changes

The following guidelines apply:

- When a PC user sets Read permissions on a directory or file, users will have both See Files and See Folders permissions when using a Macintosh.
- When a PC user sets Write and Delete permissions on a directory or file, users will have Make Changes permission when using a Macintosh.
- When a Macintosh user sets See Files or See Folders (or both) permissions, the user will have Read permissions when using a PC.
- When a Macintosh user sets the Make Changes permission, the user will have Write and Delete permissions when using a PC.

Note Permissions set within the Macintosh behave differently than those set from within Windows NT Server, including Macintosh-style permissions. From the Macintosh, a right assigned to everyone overrides more restrictive rights set on the owner or a group. From Windows NT, permissions assigned to everyone do not override permissions set on the owner or group.

Setting Permissions from a Macintosh or a PC

A folder's owner can set permissions for the folder. Both the folder's owner and the server administrators can also use a PC to set Windows NT permissions for folders on the server. The folder's owner can set permissions for the directory (folder) from a PC because the owner of every directory (folder) has the Windows NT P (Change Permission) permission for that folder.

And after SFM is started, Administrators can also use File Manager to set Macintosh-style permissions for any directory within a Macintosh-accessible volume, including the volume root directory.

Volume Passwords

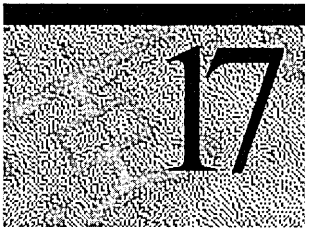
SFM provides an extra level of security through Macintosh-accessible *volume passwords*. A volume password is a password you assign to a Macintosh-accessible volume when configuring it. Any Macintosh user who wants to use the volume must type the volume password. PC users do not need to know the volume password to access the directory that corresponds to the Macintosh-accessible volume. Volume passwords are case-sensitive.

Volume passwords are optional; when you create a new Macintosh-accessible volume, the default is to have no volume password.

Note Because of a constraint with the System 6 and 7 Finder, you cannot automatically mount a volume with a volume password at startup or by double-clicking an alias. You also cannot automatically mount a volume if the user originally connected to the volume with Microsoft Authentication. For more information on Authentication, see Chapter 18, "Setting up Services for Macintosh."

CHAPTER 17

Planning Your AppleTalk Network



Before you set up Services for Macintosh (SFM) on a computer running Windows NT Server, it's a good idea to create a plan for your network. In such a network—one that includes both PCs and Macintoshes—a major consideration is how to plan the physical setup of the network, including the *network media.* (Network media are different types of local area networks, each of which uses different cabling, topology, and network cards. Examples are ethernet, token ring, LocalTalk, and FDDI.) If your network has multiple media types, you must find a way to make them work together.

Note The basic concepts of AppleTalk networking are important to master. Because few of these concepts are involved in PC networking, they might be unfamiliar. For more information about AppleTalk networks, see "AppleTalk Networks" and "Planning Your AppleTalk Internet," later in this chapter. Also refer to the *Windows NT Server Concepts and Planning Guide* for information on planning a network.

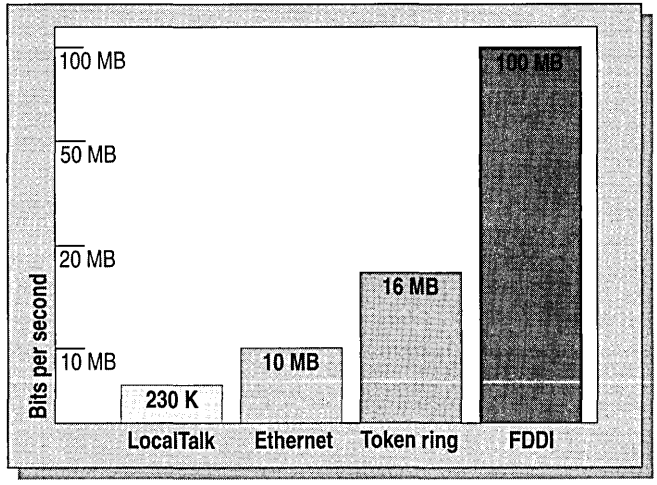
Planning the Physical Setup

As you plan how to physically connect your PCs and Macintoshes, the first thing to consider is network media. Each network media type has its own method of cabling and network topology, and each requires different network hardware.

Windows NT Server supports four types of media:

- Ethernet
- Token ring
- LocalTalk
- FDDI

Ethernet and token ring are common network media in PC networking. LocalTalk is used in AppleTalk networking. FDDI, although not as common, is based on token ring and is designed to be used with fiber-optic cabling. Every Macintosh includes hardware and software that enables it to be a client on a LocalTalk network.



Media Speeds

To set up a computer running Windows NT Server to communicate with both PCs and Macintoshes, you might need to install two (or more) network cards in the server: one card (such as ethernet) for communication with the PCs and another card (such as LocalTalk) for communication with Macintoshes. If the Macintoshes are also using ethernet (or EtherTalk®) cards, you'll need only one network card.

The following section describes how to connect your network.

Example

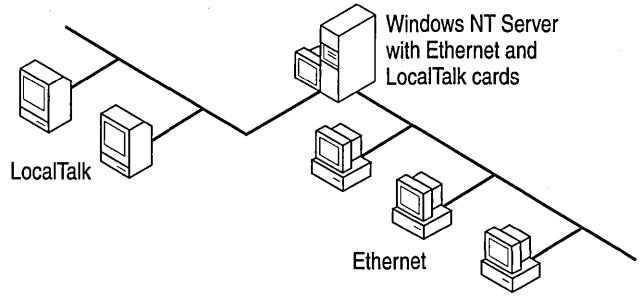
Suppose your server and PC clients use ethernet, and your Macintoshes aren't currently attached to any network. (They have only their built-in LocalTalk hardware and software.) To enable the computers running Windows NT Server and the Macintoshes to communicate, choose one of these methods:

- Install a LocalTalk network adapter card on the server in addition to the ethernet card already installed.
- Install ethernet cards on each Macintosh.
- Install an ethernet/LocalTalk router.

Solution 1: Install a LocalTalk Card on the Computer Running Windows NT Server

You can install a LocalTalk network adapter card on the computer running Windows NT Server, in addition to an ethernet card. You can then set up the Macintoshes on a LocalTalk network attached to the server's new LocalTalk card. The server will communicate with the PC clients by means of ethernet and will communicate with the Macintoshes by means of LocalTalk.

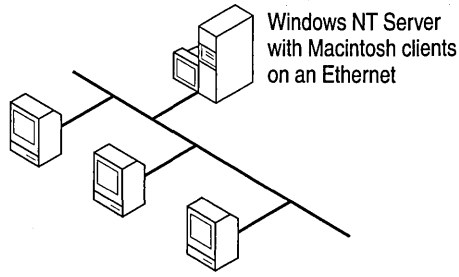
The following illustration shows such a network:



This solution is fairly inexpensive because it requires that you buy only one additional network adapter card. However, LocalTalk is not as fast as ethernet; consequently, network performance is not as good as it would be if all the clients used ethernet. Because you can have a limited number of Macintoshes on a LocalTalk network, this solution might be impractical if your network has a large number of Macintoshes.

Solution 2: Install Ethernet Cards on the Macintoshes

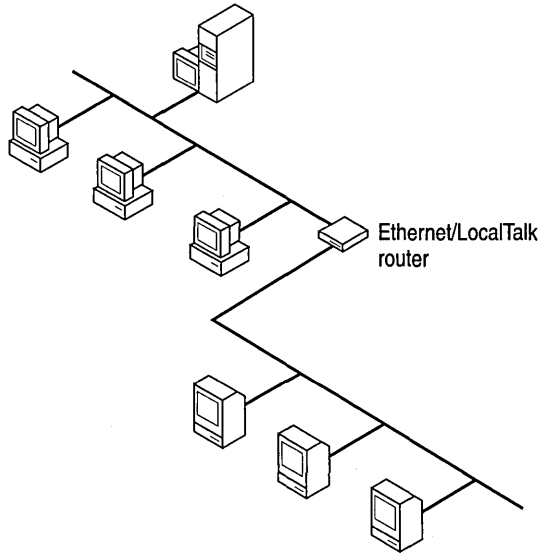
You can install ethernet network adapter cards on all the Macintoshes and attach them to your existing ethernet network. The server will use its existing ethernet card to communicate with both PC and Macintosh clients, which can all be attached to a single physical ethernet network. The following illustration shows a network using this solution:



Solution 3: Install an Ethernet/LocalTalk Router

You can install an ethernet/LocalTalk router, which translates data on the network between the two media. (These routers are made by several companies.) Windows NT Server running SFM can also act as a router between ethernet and LocalTalk. Windows NT Server, however, must have both an ethernet and LocalTalk card installed in it. (See the Note at the end of this section for more information on using the computer running Windows NT Server as a router.)

By using an ethernet/LocalTalk router, the server can still use its ethernet card, and you can put the Macintosh clients on a LocalTalk network and attach the router to both the ethernet and LocalTalk networks. All data transferred between the server and the Macintoshes passes through the router. To the server, all the Macintoshes appear to be on the ethernet network. The following illustration shows a network that uses an ethernet/LocalTalk router.



To use this ethernet/LocalTalk router, you must be able to bind the AppleTalk protocol on the server to an ethernet card on the server.

This is a low cost and useful solution if you want to make printers on the ethernet available to Macintosh clients. However, performance is degraded by using a router. A network with LocalTalk clients is not as fast as an all-ethernet network.

Note Because a computer running Windows NT Server can function as a router, it can also function as an ethernet/LocalTalk router—as long as it has both an ethernet network adapter card and a LocalTalk card. To connect one physical network of Macintoshes to several servers, you can install a LocalTalk card on one server, and that server can function as a router, enabling the Macintoshes to reach the other servers on the ethernet network.

Advanced Examples

Depending on which clients you have, the issues you face when deciding how to connect them can be more complex than those discussed previously. For example:

- Windows NT Server uses ethernet, but some of your Macintoshes use ethernet and others use LocalTalk.

  Solution: You can install a LocalTalk card on the computer running Windows NT Server to communicate with the Macintoshes that use LocalTalk, or you can install ethernet cards on all the Macintoshes, or you can use an ethernet/LocalTalk router.

- Windows NT Server uses ethernet, but some of your Macintoshes use ethernet and others use LocalTalk. You also have some Macintoshes that have token-ring network cards.

  Solution: Install a token-ring network card on the computer running Windows NT Server to communicate with these Macintoshes, in addition to whatever solution you choose in the previous example for the Macintoshes that use ethernet and LocalTalk.

These examples can be used to install FDDI rings as well.

AppleTalk Networks

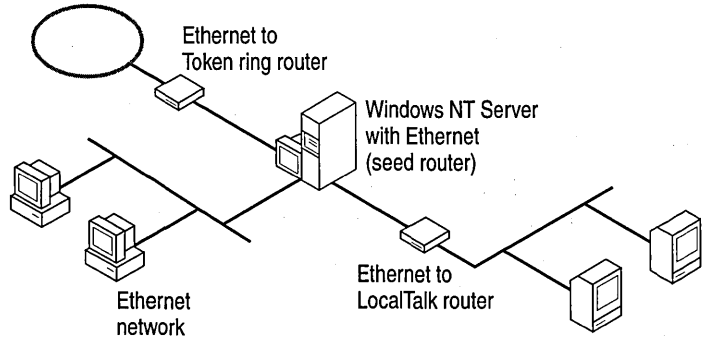
Because AppleTalk networks differ from PC networks, you must consider some special concepts and issues when you set up an AppleTalk network.

The first concept you need to understand is the *internet*. (Note that this is a different concept than the Transport Control Protocol/Internet Protocol [TCP/IP] Internet.) Most large AppleTalk networks are not single physical networks in which all computers are attached to the same network cabling system. Instead, they are internets, which are multiple smaller physical networks connected by *routers*. Routers maintain a map of the physical networks on the internet and forward data received from one physical network to other physical networks. Routers are necessary so that computers on different physical networks can communicate with one another. They also reduce network traffic on the internet by isolating the physical networks. In other words, routers only send data that is usable by a network.

Some routers on the network are *seed routers*. A seed router initializes and broadcasts routing information about one or more physical networks. This information tells routers where to send each packet of data. Each physical network must have one or more seed routers that broadcast the routing information for that network.

Not all routers must be seed routers. Routers that are not seed routers maintain a map of the physical networks on the internet and forward data to the correct physical network. Seed routers perform these functions too, but they also initialize the routing information, such as network numbers and zone lists, for one or more physical networks. (See "Determining Seed Router Placement on a Network" later in this chapter.)

A computer running Windows NT Server with SFM can function as a seed router or as a nonseed router. If it is a seed router, it must be the first server you start so that it can initialize the other routers and nodes with network information. If it is a nonseed router, it cannot be started until a seed router has initialized all ports. You can also use dedicated hardware routers (such as those made by Cayman Systems®, Shiva®, Solana, Hayes®, and others) on your network.



Phase 2 AppleTalk Networks

There are two types of AppleTalk networks: Phase 1 and Phase 2. You must use Phase 2 to run Windows NT Server and SFM (For more information, see Chapter 15, "Introduction to Services for Macintosh.")

Phase 2 includes these features:

Supported media types
: Token ring, LocalTalk, ethernet, FDDI.

Network numbers
: LocalTalk networks have a single network number; EtherTalk and TokenTalk® networks can be assigned a network range, allowing for more nodes on the network.

AppleTalk zones
: Each LocalTalk network must be in a single zone; each EtherTalk and TokenTalk network can have multiple zones, and individual nodes on a network can be configured to be in any one of the network's associated zones.

Number of *nodes* per network
: A node is any type of device on the network. Each client, printer, server, and router is a node on an AppleTalk network.

  LocalTalk networks can have as many as 254 nodes (but are actually limited to 32 or fewer nodes because of media capacity); EtherTalk and TokenTalk networks can have as many as 253 nodes for every number in the network range, for a maximum of 16.5 million nodes. (But don't specify this many nodes; network media cannot physically accommodate this large number of nodes.)

Note In this book, the terms *ethernet* and *token ring* are used in descriptions of network media. For discussions on the implementation of an AppleTalk network on ethernet or token ring, the respective Apple product names—EtherTalk and TokenTalk—are used. For more information, refer to an AppleTalk manual.

Routing Information

Routing information includes

- A network number or network range associated with each physical network
- The zone name or zone list associated with each physical network
- The default zone for the network (if the network has multiple zones)

The *network number* or *network range* is the address or range of addresses assigned to the network. A network number is unique and identifies a particular AppleTalk physical network. By keeping track of network numbers and network ranges, routers can send incoming data to the correct physical network. A network number can be any number from 1 through 65,279.

LocalTalk networks can have only a single network number; EtherTalk, TokenTalk and FDDI networks can have network ranges.

A *zone* is a logical grouping that simplifies browsing the network for resources, such as servers and printers. It is similar to a domain in Windows NT Server networking, as far as browsing is concerned. In LocalTalk networks, each physical network can be associated with only one zone. However, for EtherTalk, TokenTalk, or FDDI, you have more flexibility in assigning zones. Each EtherTalk, TokenTalk, or FDDI network can have one or more zones associated with it, and each zone can include servers and printers on one or more physical networks. This allows you to group servers and printers logically into zones so that users can easily locate and access the servers and printers, no matter what physical networks they are on.

Each Macintosh client on the network is assigned to a single zone. However, each client can access servers and printers in any zone on the network. Zones make accessing network resources simpler for users. When users use the Chooser to view the network, they see only the resources in a single zone at a time, preventing them from having to navigate through huge numbers of resources on large networks to find the resources that they need. You can put the clients, servers, and printers used by a single group into a single zone so that users will see only the resources they typically use but will still be able to access resources in other zones when required.

A zone list includes all the zones associated with that network. One of these zones is the network's *default zone*, to which the Macintosh clients on that network are assigned by default. Users can configure the client to be in a different zone, however.

Working with Seed Routers

When you install Windows NT Server and set up SFM, you must specify whether the Windows NT Server computer will seed each physical network to which it is attached. For example, a computer running Windows NT Server attached to three physical AppleTalk networks might serve as a seed router on two of the networks but not on the third.

For networks that the server will seed, specify the routing information. The Windows NT Server computer will then function as a seed router, seeding the routing information that you provided. If you specify that a server will not seed a network (that is, if you make it a nonseed router), the port will be seeded by another AppleTalk router attached to it.

Using Multiple Seed Routers on a Network

To make your network more reliable in case of system crashes and power outages, you can install multiple seed routers on the same physical network.

When you install multiple seed routers for a particular network, all the seed routers must seed the same information for that network. When the network starts, the first seed router that starts on the network becomes the actual seed router.

When a network starts, if the first seed router to start has different routing information than seed routers that start later, the information established by the first seed router is used. If a seed router that starts subsequently with different information is a server running Windows NT Server, the conflicting information is ignored, an event is written to Windows NT Server Event Viewer, and the server ceases to be a seed router. Non-Microsoft routers might behave differently.

For more information on configuring seed routers in a network, see online Help and the section "Configuring AppleTalk Routing" in Chapter 4, "Routing in Windows NT."

Planning Your AppleTalk Internet

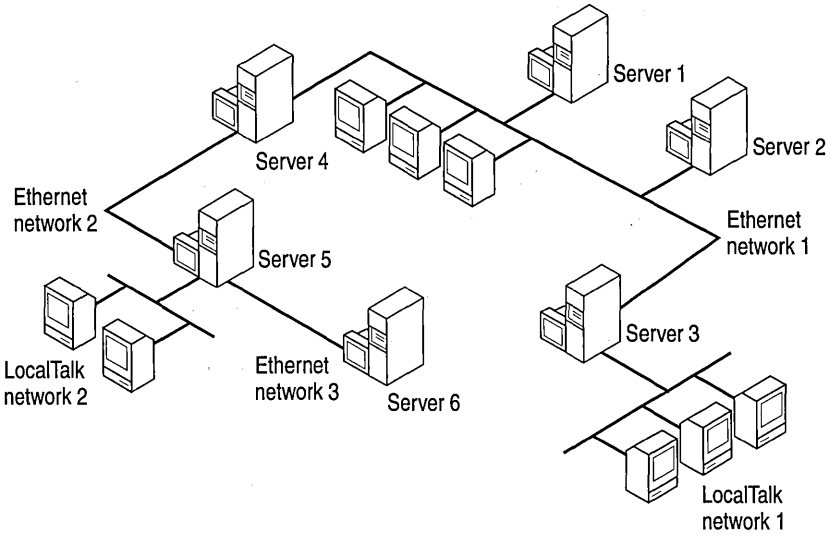
When you plan your AppleTalk internet, follow these guidelines:

- Determine which router will seed each network.
- Decide how to assign network numbers and network ranges.
- Decide how to assign zones.
- Create a router plan and router record.

These guidelines are explained in the following sections.

Determining Seed Router Placement on a Network

When planning a large internet, it is helpful to make a diagram of your AppleTalk internet, including the physical network layout and connecting points in the diagram. The following illustration shows an example of an AppleTalk internet. It includes clients only for visual clarity; you only need to diagram routers and servers. Diagramming the internet will help you determine which router will seed each physical network.



Example

Suppose you have an existing network with six computers running Windows NT Server (as shown in the previous illustration). You must determine which server will seed each network. Refer to the illustration as you read the following plan.

- The seed router for ethernet network #1 must be Server 1, Server 2, Server 3, or Server 4.
- The seed router for ethernet network #2 must be Server 4 or Server 5.
- The seed router for ethernet network #3 must be Server 5 or Server 6.
- The seed router for LocalTalk network #2 must be Server 5, because the router on Server 5 is the only one available for this network. Similarly, Server 3 must seed LocalTalk network #1.

Assigning Network Numbers and Network Ranges

Follow these guidelines when you decide how to assign network numbers and network ranges:

- Use network numbers that leave room for expansion.

  For example, LocalTalk #2 in the Router Seeding Plan Example table, later in this chapter, starts at 1280, leaving plenty of growth for LocalTalk #1, which starts at 1024.

- For a LocalTalk network, you can assign only a single network number. For each ethernet or token-ring network, you can assign a network range.

  Network numbers are essentially arbitrary. The important thing is for them to be unique and to not overlap (if in a range) with other ranges.

  If you plan to expand any LocalTalk networks for which you can currently assign only a network number, leave a range of unused numbers above the number you assign. You can use these numbers when you expand your network.

- Base your network ranges on the number of nodes you expect to have in the future on each network.

  Base the extent of a network range on the number of AppleTalk nodes expected on the physical network. The total number of possible AppleTalk nodes is 253 times the number of network numbers in the range. For example, a network range of 101 through 103 permits 759 nodes (3 * 253 = 759); a network range of 120 to 129 permits 2530 nodes (10 * 253 = 2530) on a network. Leave room for more nodes than are currently connected.

Assigning Zones

AppleTalk zones are identified by zone names. Follow these guidelines when you decide how to assign zone names:

- Assign a single zone name to each physical LocalTalk network. You can assign one or more zone names to each ethernet and token-ring network. An asterisk (*) cannot be a zone name.
- For each ethernet and token-ring network, decide which zone will be the default zone.
- The number of zones your internet has depends on the size of the internet you are planning. If your internet is small, a single zone can be adequate. But if you have a single Phase 2 ethernet or token-ring network that spans a large geographic area or contains large numbers of AppleTalk devices (such as printers and servers), use multiple zones to make it easier for users to find the devices they need.

Making a Router Plan

After you have diagrammed your network, make a router plan that shows the location and type of each seed router for the network. The following seed router examples are based on the preceding network diagram.

To make a router plan, determine:

- The expected number of AppleTalk devices on present and projected ethernet and token-ring networks.
- The quantity of network numbers sufficient to satisfy capacity requirements. (Up to *n* * 253 devices can be supported, where *n* is the number of network numbers in the range.)

Router Seeding Plan Example

Cable ID	Network range	Zone list	Seed device(s)[1]
Ethernet #1	16-25	**Finance**[2]	
		Accounts Payable	Server 1
		Accounts Receivable	Server 3
Ethernet #2	32-37	**Marketing**[2]	
		Marketing Exec	Server 5
Ethernet #3	768	**Engineering**[2]	Server 6
LocalTalk #1	1024	Finance	Server 3
LocalTalk #2	1280	Marketing	Server 5

1 Seed device information can indicate the server name, the type of dedicated hardware router, or the location, depending on your needs.

2 Indicates the network's default zone.

Creating a Router Record

To keep information about your internet for maintenance purposes, create a record from your router seeding plan. Include the following information:

- Router location
  - Physical location
  - If the router is a computer running Windows NT Server with SFM, record the computer name of the server
- Router type and version
- The physical networks connected to the router, with the following information for each:
  - Cabling identification
  - Network media type

- Network number(s)
- Zone name(s)
- Default zone
- Whether this router is a seed router for the networks attached to it

Note Third-party AppleTalk network management products for Macintosh clients can simplify internet administration. For example, the Apple Inter-Poll® network administrator's utility lets you see all AppleTalk devices (including routers) on an internet in real time, observe every SFM server, and sort devices by network number, device name, node, and so on. If you install the Apple Responder (part of the Inter-Poll product) on Macintosh clients running System 6.*x*, you can also view those clients with Inter-Poll. (The Responder is built into System 7.) Farallon™ Computing, Sonic System, and Caravelle also provide network management utilities that track network activity.

Preparing to Set Up Services for Macintosh

Before you set up SFM on any computer running Windows NT Server, take the router seeding plans and diagrams you have made, and prepare the information you will need when you install each server. For each server, create a table of information:

- Indicate the computer name and physical location of the server.
- For each network attached to the server, record network ID, network adapter card type, and whether the server will serve as a seed router for the network.
- If the server will be a seed router for any network, record the routing information that it will seed for each network, including the network number or network range, the zone name or zone list, and the default zone.
- If the server is on an ethernet or token-ring network that has multiple zones, record the zone (or zones) where you want Windows NT Server to appear to Macintosh users.

The following tables show examples, based on the preceding diagram and examples.

Server Planning Example

Windows NT Server computer name: \\server5

Physical location: Room 1350

Cable ID	Adapter	Seed	Routing information	Appears in zone
Ethernet #2	EtherLink® II	Yes	512-517 **Marketing**[1]	Marketing
LocalTalk #2	COPS[2]LTI ISA	Yes	1280 **Marketing**[1]	Marketing

Windows NT Server computer name: \\server6

Physical location: Engineering Lab

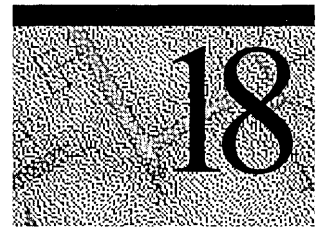
Cable ID	Adapter	Seed	Routing information	Appears in zone
Ethernet #3	EtherLink II	Yes	768 **Engineering**[1]	Engineering

1 Indicates the network's default zone.

2 Same as the DayStar Digital card.

CHAPTER 18

Setting Up Services for Macintosh



This chapter describes what happens when you set up Services for Macintosh (SFM) on a computer running Windows NT Server. It explains how to set up SFM directly from the distribution disk and over the network, as well as how to remove it from the server. This chapter also includes instructions for setting up the *encrypted password module*, also called user authentication module (UAM), that runs on Macintosh clients connected to the network.

Note Before setting up SFM, become familiar with concepts such as AppleTalk internets, AppleTalk Phase 2, routing and seed routing, network numbers and ranges, and zones. Also, make a plan for your AppleTalk internet. If you aren't familiar with AppleTalk networking concepts, or if you don't yet have an internet plan, read Chapter 17, "Planning Your AppleTalk Network," before proceeding.

Overview

You can set up SFM at the same time you install Windows NT Server, or you can set it up later. To set up SFM, use the Network icon in Control Panel and the Windows NT Server distribution disk.

If you remove SFM and later decide to set it up again, you must use the Windows NT Server distribution disk and installation program to copy the required SFM files to the server. Removing SFM deletes the distribution files (except Macintosh-accessible volumes) instead of disabling them.

Note You must be an administrator or have administrator permissions to use the Network icon in Control Panel.

When you set up SFM, the following are automatically started or enabled: AppleTalk Protocol, File Server for Macintosh, and Print Server for Macintosh.

- The AppleTalk Protocol is the layer of AppleTalk Phase 2 protocols that delivers data to its destination on the network. The AppleTalk Protocol can be configured through the Network icon in Control Panel. Configuration instructions for the AppleTalk Protocol appear in Chapter 19, "Configuring Services for Macintosh."
- File Server for Macintosh (also called *MacFile*) allows you to designate a directory as a Macintosh-accessible volume, ensures Macintosh filenames are legal NTFS names, and handles permissions. When set up, File Server for Macintosh commands appear in Windows NT Server File Manager and Server Manager under the MacFile menu. Instructions for configuring it appear in Chapter 19, "Configuring Services for Macintosh."
- Print Server for Macintosh (also called *MacPrint*) allows all network users to send print jobs to a spooler on the Windows NT Server and continue working; they need not wait for their print jobs to complete. Windows-based users can also review the print jobs in the Printers folder. See Chapter 20, "Setting Up Printers," for more information.

In addition, setting up SFM creates a Control Panel icon that gives you the same server administration capabilities as the MacFile menu (excluding volume management) for the local computer.

Setting Up from Windows NT Server

After Windows NT Server is installed, use the Network icon in Control Panel and the Windows NT Server distribution disk to set up SFM.

▷ **To set up Services for Macintosh**

1. In Control Panel click **Network**.
2. In the **Services** tab, click **Add**.
3. From the **Network Service** list, select **Services for Macintosh** and click **OK**.
4. Type the path to the Windows NT Server distribution files.

   Setup copies all SFM files and sets up the Registry.
5. In the **Network** dialog box, click **Close**.

   The **AppleTalk Protocol Configuration** dialog box appears. Use it to select a new zone, a different network, or to enable AppleTalk routing, as desired. See online Help for more information.
6. Click **OK**, or click **Cancel** if you do not want to change the configuration.

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

Setting Up from the Network

Setting up over the network can save time if you need to set up SFM on multiple Windows NT Server computers. SFM is set up over the network just as any other service: Simply type the path to the files. This path can be a network drive or a universal naming convention (UNC) name such as **\\server1\ntfiles**. For more information, refer to the *Windows NT Server Concepts and Planning Guide*.

Setting Up for Remote Administration

You can set up the administrative tools on any Windows NT computer so that you can administer SFM remotely from a Windows NT clients.

Refer to the *Windows NT Resource Kit* for information on setting up administrative tools on Windows NT computers.

Stopping and Removing Services for Macintosh

After you have set up SFM on a server, you can remove it at any time. For example, you might want to move your SFM installation to another server. When you remove SFM, all SFM files are deleted from the server's hard disk, except some program files that are in use. (The files in use will be reworked when the system is rebooted.)

Before you remove SFM, use the Devices icon in Control Panel to stop the services. If the services are running, removing will delete only the registry entries.

▷ **To stop the services**

1. In Control Panel click Devices.
2. From the **Device** list, select **AppleTalk Protocol** and click **Stop**.
3. Click **OK** to stop the AppleTalk Protocol and the Print and File Servers for Macintosh. After the devices have stopped, click **Close**.

   Now you're ready to remove SFM.

▷ **To remove Services for Macintosh**

1. In Control Panel click Network.
2. In the **Services tab**, select **Services for Macintosh** and click **Remove**.
3. Click **Yes** to confirm that you want to remove the SFM files from the computer running Windows NT Server.
4. Click **OK**.

The AppleTalk Protocol and the File and Print Servers for Macintosh will be deleted; services will be removed. Note that removal makes all volumes unavailable to the Macintosh users, but it does not delete them; in other words, the volumes will revert to directories.

Setting Up the Services for Macintosh Client Software

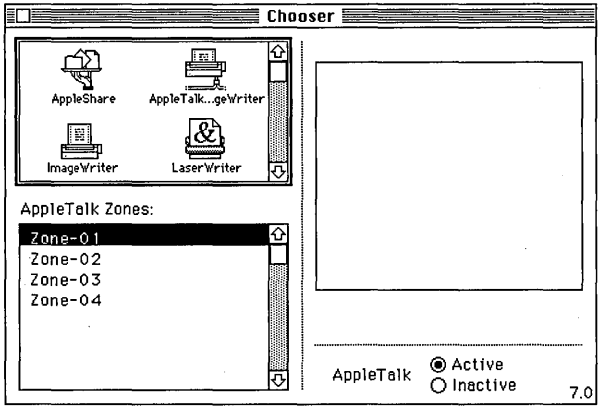
Microsoft authentication is an AppleShare extension that provides a more secure logon session to a computer running Windows NT Server. It encrypts passwords and stores them on the computer running Windows NT Server. You can either set up, or instruct Macintosh users to set up, the authentication file on their Macintoshes by means of the network.

With Microsoft authentication, users can also specify a domain when they log on or change their passwords. So, if they have an account in several domains, the right one will be used. (To do this, users type *domainname\username* in the Name box.)

▷ To gain access to the authentication files

1. From the **Macintosh Apple** menu, select the **Chooser.**

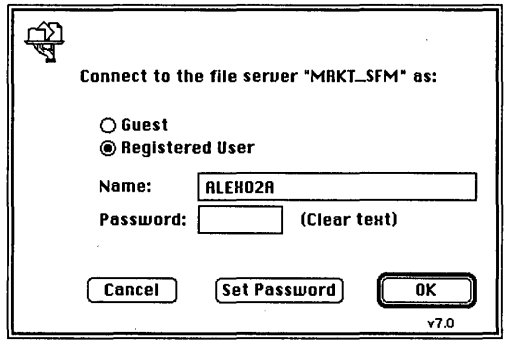
   The **Chooser** dialog box appears.



2. Select the AppleShare icon, and then the AppleTalk zone in which the computer running Windows NT Server resides.

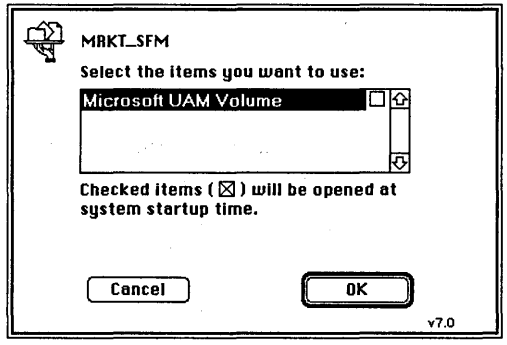
3. From the list of file servers, select the name of the Windows NT Server.
4. Click **OK**.

   A sign-in dialog box appears.



5. Choose the **Registered User** or **Guest** option button, as appropriate.
6. Click **OK**.

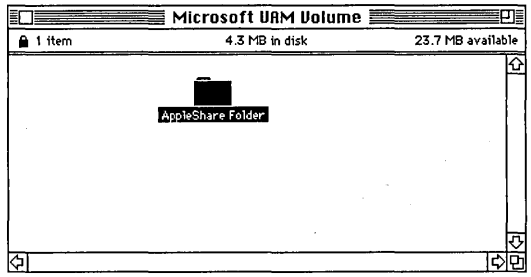
   A server dialog box appears.



7. Select the Microsoft UAM Volume.
8. Click **OK**.
9. Close the **Chooser** dialog box.

▶ To install the authentication files on the Macintosh client

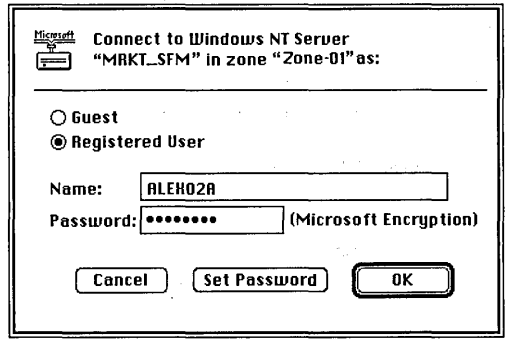
1. From the Macintosh Desktop, double-click the Microsoft UAM Volume to open it. The Microsoft UAM Volume window appears.



2. Select the AppleShare Folder and drag it to the System Folder on your hard disk.

Note If the Macintosh client already has an AppleShare Folder in the System Folder, a message will ask if you want to overwrite the folder. Do not overwrite it because it might contain other UAMs (such as the NetWare® UAM). To maintain the files in the original AppleShare Folder, simply open the AppleShare Folder in the Microsoft UAM Volume, and drop the MS UAM file into your existing AppleShare Folder in your System Folder.

Now, when the Macintosh user connects to the computer running Windows NT Server, authentication will be offered as shown in the following dialog box:



How this is done depends on the Macintosh system the user is running. If a Macintosh is running System 7.1 or later and the clear-ext and guest options are disabled at the server level, the user will be given only one choice: Microsoft Authentication. Earlier systems will show both choices: Microsoft Authentication and clear-text password protection in the form of the Apple standard UAMs, even if the cleartext and guest logon options have been disabled and are unavailable to clients.

Setting Up Buttons on the File Manager Toolbar

If you use SFM frequently, you might want to customize the File Manager toolbar to include SFM buttons. To make room for the SFM buttons, you might need to remove separators (spaces between the buttons) or other buttons.

The SFM buttons available for setup include the following commands: **Create Volume, Remove Volumes,** and **Permissions**, which are available on the MacFile menu in File Manager.

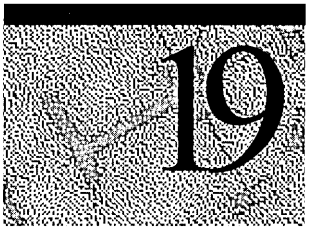
From File Manager, use the **Options** menu and the **Customize Toolbar** command to make changes to the Toolbar. For more information about customizing the Toolbar, refer to online Help.

Choosing a Zone After Setup

After setting up SFM and rebooting, you can choose a zone for SFM. For more information, refer to Chapter 19, "Configuring Services for Macintosh."

CHAPTER 19

Configuring Services for Macintosh



The AppleTalk Protocol is the component of Services for Macintosh that can be configured using the Network icon in Control Panel.

AppleTalk Protocol is a stack of protocols that Services for Macintosh uses to route information and configure zones. It works behind the scenes to ensure that computers on the network can talk to one another.

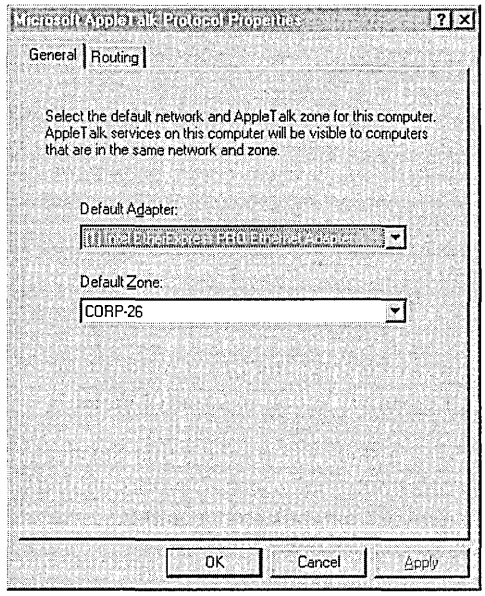
Starting the Configuration

You start configuration of the AppleTalk Protocol from the Network icon in Windows NT Server Control Panel.

▷ **To get started**

1. In Control Panel, click **Network**.
2. In the **Services** tab, select **Services For Macintosh** and click **Properties**.

The Microsoft AppleTalk Protocol Properties dialog box appears.



Configuring AppleTalk Protocol

You use the Microsoft AppleTalk Protocol Properties dialog box to select a default network from a list of adapter cards bound to the AppleTalk Protocol, and to enable routing and seeding of the network, which include configuring zones and setting network ranges.

Choosing a Network and Zone

Start with the Microsoft AppleTalk Protocol Properties dialog box (see "Starting the Configuration," earlier in this chapter) where you can see the default network and the other network adapters to which the AppleTalk Protocol is bound. You also use this dialog box to select the zone where the services will appear, to specify that the server act as an AppleTalk router, and to choose Advanced options for AppleTalk routing, such as seeding the network. Seeding the network means determining zones and the default network and setting network ranges.

▷ **To choose a network and zone**

1. In the **General** tab, in the **Default Adapter** box, select the network you want.

   The Network list shows the network adapter card drivers available on the computer running Windows NT Server.

   Note If the computer running Windows NT Server is to be used as a router, the LocalTalk network cannot be used as the default network.

2. In the **Default Zone** box, select the zone in which you want Services for Macintosh to appear.

   This is the zone in which the File Server for Macintosh and Windows NT Server printers will appear when Macintosh users select them in Chooser.

In the **Routing** tab, if you select the **Enable Routing** check box, the computer running Windows NT Server will become an AppleTalk router. This means that if the AppleTalk Protocol is bound to more than one network card, the computer running Windows NT Server will be seen from Macintoshes connected to all the bound networks. Otherwise, the computer running Windows NT Server can be used only from the Macintoshes connected to the default network, unless another router broadcasts the information for the other networks.

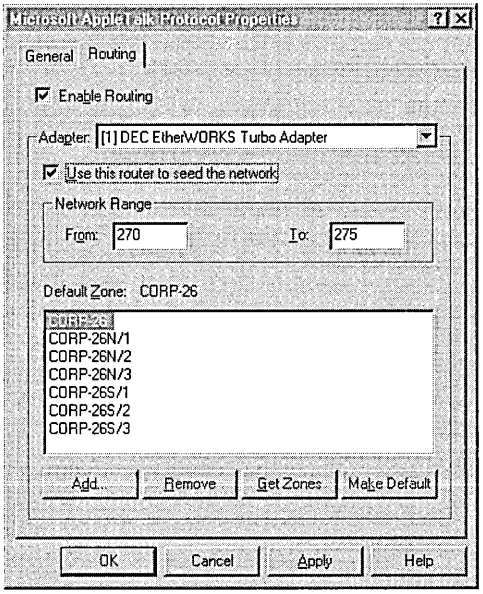
Seeding the Network

In the **Routing** tab, the **Adapter** box shows a list of network cards that correspond to the networks the Windows NT Server computer is attached to. Seeding can be enabled on any or all of the networks. To seed a specific network, choose the corresponding adapter and then select the use this router to seed the network check box.

Caution The seeding information must agree with all routing information on that network and internet. Otherwise, all routers on the internet could fail to function.

▷ To seed the network

1. In the **Routing** tab, select the **Enable Routing** check box.



2. If you want, select another network from the **Adapter** list.

   This list contains all network adapter cards to which the AppleTalk Protocol is bound. (To add and remove network adapters, use the Network icon and the Add and Remove buttons in the Adapter tab.)

3. Select the **Use this router to seed the network** check box.

Selecting to seed the network makes the present state of the Zone List and the Network Range options available.

▷ To have the server stop seeding a network

1. Clear the **Use this router to seed the network** check box..
2. Click **OK**.

Setting the Network Range

Setting the network range is part of seeding a network. Each AppleTalk network in an internet is assigned a range of numbers, and each node is identified to the network by one of those numbers, combined with a dynamically assigned AppleTalk node identification number. Because of this, no two networks on an internet should have overlapping ranges.

The value you specify for a network must range from 1 through 65,279. If you specify a range that overlaps another network range on the computer running Windows NT Server, you'll see a warning message. For more information about ranges, refer to Chapter 17, "Planning Your AppleTalk Network."

▷ **To set a network range**

1. In the **From** box, provide a number.
2. In the **To** box, provide a number.

   If the network adapter is for a LocalTalk network, you cannot type a value in the to range.

Setting Zone Information

Setting zone information is part of seeding a network. You can see the current list of zones, add and remove zones, and set the default zone. The default zone is the zone in which all AppleTalk devices will appear if a desired zone has not been specified for the device.

To set zone information, start with the Microsoft AppleTalk Protocol Properties dialog box. For an explanation of how to get to this dialog box, see "Starting the Configuration" and "Seeding the Network" earlier in this chapter.

▷ **To see the current state of the zones on a chosen network**

1. In the **Routing** tab, select a zone from the **Default Zone** list.
2. Click **Get Zones**.

   This gets the current zone information for the current network. If you want to see zones on another network, select one from the Default Networks list.

▷ **To add a zone to the network**

1. Click **Add**.
2. In the **New Zone** box, type the name of the new zone.

   The new zone is added to the Zone List.
3. Click **OK**.

▶ **To remove a zone or zones from the network**

1. Select a zone in the **Default Zone** list and click **Remove.**

   The zone or zones are removed from the Zone List. For others on the network to see the change, however, you must restart the AppleTalk Protocol, which is serving as a router.

2. Click **OK**.

▶ **To set a new default zone for the network**

1. In the **Default Zone** list, select a zone.
2. Click **Set Default**.

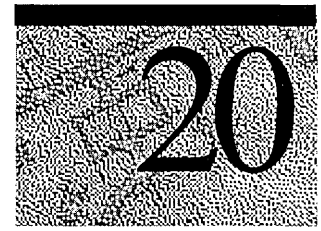
   You see the new default zone highlighted in the Zone list. For others on the network to see the change, however, you must restart the AppleTalk Protocol, which is serving as a router.

3. Click **OK**.

Note For the changes to take effect, you must stop the AppleTalk Protocol and restart it so that the information can be routed on the network.

CHAPTER 20

Setting Up Printers



Before setting up printers, it's important to understand the distinction between a printing device and a printer that you create using the Add Printer wizard:

- A printing device is the hardware that actually does the printing, such as a Hewlett-Packard® LaserJet®.
- A printer you create using Windows NT Server is a software interface between the document and the printing device. You create a printer using the Add Printer wizard, and each printer sends jobs to the printing device, according to the specified priority—for example, on a first-come, first-served basis.

These concepts and others are explained more fully in the *Windows NT Server Concepts and Planning Guide.*

Services for Macintosh Print Server

When Services for Macintosh (SFM) is set up, several AppleTalk services are integrated into Windows NT Server. The print server, called *Print Server for Macintosh,* is integrated into the Windows NT Server Printers folder. The print server makes printers connected to the computer running Windows NT Server available to Macintosh clients, and it makes AppleTalk PostScript printers (with LaserWriter drivers) available to PC clients.

When the print server receives print jobs from the print server, it sends them to a spooler, which is a portion of the hard disk. The spooler then sends the print job to the specified printing device—for example, to a printing device on the AppleTalk network. This enables Macintosh users, as well as PC users, to submit print jobs and continue working on their computers without waiting for the print job to complete.

The print server also translates all incoming PostScript files if the print request is to a non-PostScript printer attached to the computer running Windows NT Server. So, a Macintosh client (but not a Windows NT client) can send a PostScript job to any Windows NT Server printer.

Note This implementation of Postscript RIP for SFM supports 300 dpi and Postscript level 1.

Stopping and Restarting the Print Server

When you set up SFM, all services are automatically started, including the print server. You might want to stop and restart the print server if, for example, you must remove a printing device. You stop and restart the Print Server for Macintosh using the Services icon in Control Panel.

▷ **To stop and restart Print Server for Macintosh**

1. From Control Panel, choose the Services icon.
2. From the **Service** list, **select Print Server For Macintosh.**
3. Click **Stop** or **Start**, as appropriate.

   To change options at startup, click **Startup.**
4. Click **Close.**

Printing on a Network

The following list shows the three scenarios for printing on a network:

- PC clients send print requests to printers representing printing devices attached to a computer running Windows NT Server.
- Macintosh clients send print requests to printers representing printing devices on an AppleTalk network.
- Macintosh and PC clients send print requests to printers representing printing devices attached to a computer running Windows NT Server (for example, to a non-PostScript printing device such as the HP DeskJet® 500) and to printing devices on an AppleTalk network (for example, to a PostScript printing device such as the Apple LaserWriter).

Printing is very easy in each of these scenarios. PC users simply specify printers on a computer running Windows NT Server and send print jobs to them as usual, whether the printing device is attached to the server itself or located elsewhere on the network. Similarly, Macintosh users have the familiar Chooser interface to use for connecting to printers that are set up for both AppleTalk printing devices and those attached to a computer running Windows NT Server.

The first two scenarios are the common setup for networks serving either PC or Macintosh clients, respectively. Setup options for PCs and printers attached to a computer running Windows NT Server are explained in the *Windows NT Server Concepts and Planning Guide*. Macintosh network and printer options are explained in Macintosh software manuals. The last scenario is explained in this chapter.

Planning the Setup of Printing Devices

With SFM, installing and setting up printing devices and creating printers is no different than what you'd normally do using Windows NT Server, with one exception: The print server and file server must appear in the same zone. However, there are some performance issues worth considering.

In PC networks printing devices have traditionally attached to a server through serial or parallel ports, whereas printing devices used on Macintosh networks have traditionally attached to the network using a LocalTalk connection. With SFM, you can attach a printing device to a computer running Windows NT Server, or put it on the AppleTalk network. Either way, both types of clients can send print jobs to the printing device. (If on AppleTalk, the printer must be a PostScript printer that uses the LaserWriter driver.)

To obtain fastest performance, attach printing devices to the network rather than to a port. The following attachment options are listed in slowest to fastest order:

1. The printing device is connected to a serial port attached to the computer running Windows NT Server.

   (Some older models of the Apple LaserWriter can be attached only to a serial port, not to a parallel port.)
2. The printing device is connected to a parallel port attached to the computer running Windows NT Server.
3. The printing device is connected to the AppleTalk network through LocalTalk, which is the typical Macintosh network attachment.
4. The printing device is connected to AppleTalk through the token ring or ethernet media.

How you attach printing devices to AppleTalk depends on the type of network media you are using for your AppleTalk network. Most Macintosh-compatible printing devices have LocalTalk connections to AppleTalk. If your network is ethernet or token ring, you might need to do one of the following before adding a printing device to it:

- Install a LocalTalk/ethernet or LocalTalk/token-ring router on your network.
- Install a LocalTalk card in the server, and connect the printing device to it. The server will act as a router between the ethernet network and the LocalTalk network where the printing device is located.

The type of printing devices with built-in ethernet interfaces offer the best performance. These printing devices attach directly to the network and don't need to be physically close to the computer running Windows NT Server. Also, they print at faster network transmissions speeds than printers that rely on parallel or serial connections.

Creating a Printer on a Computer Running Windows NT Server

After you have physically attached a printing device to a computer running Windows NT Server (either directly or on a network), use the Add Printer wizard to create a printer that represents it. You can create more than one printer representing the same printing device.

For example, if you have a printing device in your office but also share it with others over the network, you might want to create two printers representing the printing device. You can create a printer for yourself that is not shared over the network and a second printer that is shared. Then it's easy to control the use of the shared printer. You can set permissions on the shared printer, ensuring that only members of your department can print to it. Or you can set a low priority for it, ensuring that documents you send to the printer will always print before documents sent by those who share it.

Another common example is to create a printer that spools to a printing device at night and another printer that spools to the same printing device during the day.

To create a printer, you must be logged on with sufficient permissions. Administrators, Server Operators, and Print Operators can create printers.

▷ **To create a printer**

1. From the **Start** menu, choose **Settings** and then choose **Printers.**
2. In the **Printers** dialog box, click **Add Printer.**
3. Follow the Add Printer wizard to choose the printer ports, printer driver, and printer name. You can also set printer properties such as location and scheduling information.

See the online Help during setup for more information.

Note The printer name can be up to 32 characters in length. This name will appear in the title bar of the printer window. By default, it is the name that network users (except MS-DOS users) will see when you share the printer.

Choose the **Share this printer** option during setup. In the Share Name box, specify the printer name that you want MS-DOS clients to see.

When you are selecting a destination, if the printing device is physically connected to the Windows NT Server computer, then select the appropriate port. If the printing device is on the network, click **Add Port.** Choose **AppleTalk Printing Devices** from the **Printer Ports** dialog box and click **OK.** From the **Available AppleTalk Printing Devices** dialog box, select a zone and a printer, and click **OK.**

Setting Up a User Account for Macintosh Print Jobs

After setting up SFM, you should create an account that will be used by all Macintosh clients when printing jobs to captured AppleTalk printing devices or to other devices on the computer running Windows NT Server. You should also configure Print Server for Macintosh to use this account.

After it is created, the user account (for example, MACUSERS) appears in the list of names that appears when you choose **Permissions** from the **Security** menu in Print Manager. You can give specific rights to this user account, just as you would any user account, including Print and No Access.

For more information about permissions, see Chapter 22, "Managing the File Server." For information on creating a user account and more specific information for configuring it to run with a service (such as Print Server for Macintosh), see the *Windows NT Server Concepts and Planning Guide*.

▶ **To configure the Print Server for Macintosh service to use a user account**

1. From Control Panel, choose the Services icon.
2. In the **Services** dialog box, select **Print Server For Macintosh.**
3. Click **Startup.**
4. In the **Print Server For Macintosh** dialog box, click **This Account** and type or choose the user account—for example, MACUSERS.
5. To require a password for Macintosh users of the computer running Windows NT Server, type a password in the Password box and confirm it.
6. Click **OK.**

Enabling Clients to Use Printers on the AppleTalk Network

With SFM, both PC and Macintosh clients can send print jobs to printing devices or spoolers on the AppleTalk network.

The printing device must appear as a LaserWriter in the Chooser, and there must be a Windows NT print driver for the printing device.

Macintosh clients use printers just as they normally do—through the Chooser. If an AppleTalk printer has been set up through Print Manager, it can be captured so that Macintosh clients cannot access it directly. This causes Macintosh print jobs go through the computer running Windows NT Server and be spooled along with print jobs from PC clients.

You can disable the capture setting. Doing so enables any Macintosh client to print to an AppleTalk printer directly. There are a few problems with this scenario, the most important being that the jobs will not be under the administrator's control.

▶ **To release or recapture an AppleTalk printing device**

1. In Printers, select an AppleTalk printing device.
2. From the File Menu, choose Properties.
3. In the **Ports** tab, click **Configure Port.**

   A dialog box appears, asking if you want to capture this AppleTalk printing device.
4. Choose Yes to capture it or No to release it.
5. Click **OK.**

When an AppleTalk printer is released, any Macintosh user on the AppleTalk network can use the device directly.

A printing device on AppleTalk can be captured when SFM is set up and a printer is created for it. It must remain captured so that all Macintosh clients send print jobs through the computer running Windows NT Server. If a printing device has been released for some reason, you can recapture it.

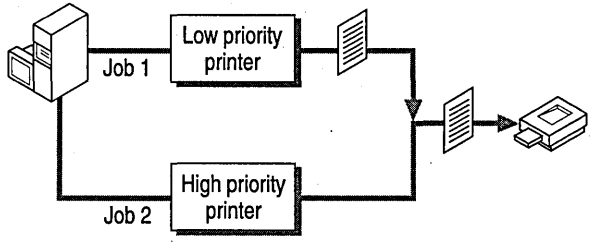
You can select another spooler instead of an actual device. Use this type of configuration with caution. It is possible to create an endless loop of print spooling with this method.

Advanced Topics

Whether printing devices are attached to the computer running Windows NT Server or are located elsewhere on the AppleTalk network, the Printers folder displays a list of print jobs for the respective printers you created to represent the devices. Each list, by default, presents jobs in first-come, first-served order. You can change the priority of jobs, however, and specify permissions for the printer and times for print jobs to run. For example, you can do the following:

- Set up multiple printers that all send print jobs to a single printing device. You might want to assign the printers a priority number (such as high-priority and low-priority), or assign times for the printer to spool its jobs (such as during business hours or only during the night).
- Set up a single printer that sends print jobs to a pool of printing devices. Doing this can make printing more efficient because print jobs are sent to the first available printing device in the pool.

An illustration of the first approach follows:



Creating Multiple Printers for a Single Printing Device

You might want to create multiple printers, all of which send print jobs to a single printing device. Each printer has a print-priority level associated with it. If you create two printers and associate them with a single printing device, jobs routed to the printer with the highest priority (lowest number) print first.

For PC users, it's a good idea to create a group that corresponds to each printer. For example, users in Group1 might have access rights to a priority-1 printer, users in Group2 might have access rights to a priority-2 printer, and so on. This allows you to prioritize print jobs according to the users submitting their jobs. (Refer to the *Windows NT Server Concepts and Planning Guide* for more information.)

For Macintosh users, however, one user account must be created for all incoming print jobs to the computer running Windows NT Server. Consequently, all Macintosh users sending print jobs through the computer running Windows NT Server will have the same access rights.

▶ **To specify priorities for printers sending jobs to a single printing device**

1. If necessary, create the two (or more) printers and share them, using procedures described earlier in this chapter and in the *Windows NT Server Concepts and Planning Guide*.
2. For each printer, from the **File** menu, choose **Properties**.
3. In the **Scheduling** tab, use the slide bar to select a priority in the **Priority** box.

   Higher priority jobs will print before lower priority jobs.
4. Click **OK**.

You can also create two printers that postpone the print jobs—for example, one that releases its queued jobs at night and another that release queued jobs during daytime hours. To do so, use the Scheduling tab to change the hours that each printer is available. For more information about setting up printers, refer to the *Windows NT Server Concepts and Planning Guide* and to online Help.

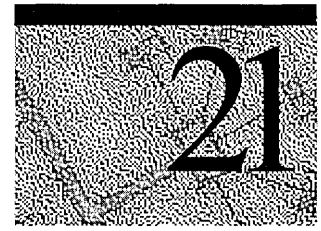
Creating Printing Pools

When you create a printer, you can associate it with more than one printing device in order to form a *printing pool.* A printing pool consists of two or more similar printing devices associated with one printer name. To set up a pool, you create a printer and assign it as many output ports as you have identical printing devices. Printing pools have the following characteristics:

- All devices in the pool share the same print property settings and act as a single unit. For example, stopping one device pauses them all.
- Print destinations can be of the same type or mixed (serial, parallel, and network).
- When a job arrives for the printing pool, the spooler on the computer running Windows NT Server checks the destinations to see which device is idle. The first port selected gets checked first, the second port second, and so on. If your pool consists of a different type of port, make sure you select the fastest port first (network, then parallel, and then serial).
- A printing pool can contain a mixture of printer interface types, but the printing devices must all use the same printer driver.

CHAPTER 21

Working with Macintosh-Accessible Volumes



A computer running Windows NT Server with Services for Macintosh (SFM) can store files so that both PC and Macintosh users can gain access to them. PC users (including users of the MS-DOS, OS/2, Windows, Windows for Workgroups, Windows NT Workstation, and Windows NT Server systems) look for shared files in a shared directory on the computer running Windows NT Server. Macintosh users look for shared files in the same directory; however, they see the directory as a volume, with familiar folders and files.

A Macintosh user shares a file with PC users by storing that file in a Macintosh-accessible volume on the computer running Windows NT Server. Likewise, a Macintosh user can mount a Macintosh-accessible volume on the desktop to use files stored in shared directories by PC users.

This chapter explains how to create a Macintosh-accessible volume so that files can be shared between Macintosh and PC clients.

Creating Volumes

All Macintosh-accessible volumes must be created on an NTFS partition or on a CDFS volume. If you specify a CDFS volume, the Macintosh-accessible volume will provide read-only access. (In this case, *CDFS volume* refers to a hard disk volume.)

Creating a Macintosh-Accessible Volume

Similar to creating a share (shared directory) for PC users, you can designate a directory as a Macintosh-accessible volume. If the directory is to be accessed by PC clients as well as Macintosh clients, make sure you share the directory using the **Share As** command on the **Disk** menu and designate it as a Macintosh-accessible volume. (Refer to the *Windows NT Server Concepts and Planning Guide* for more information on creating shares.) If you don't need to share the files with PC users, you can create a volume on a directory—that is, it doesn't have to be a shared directory.

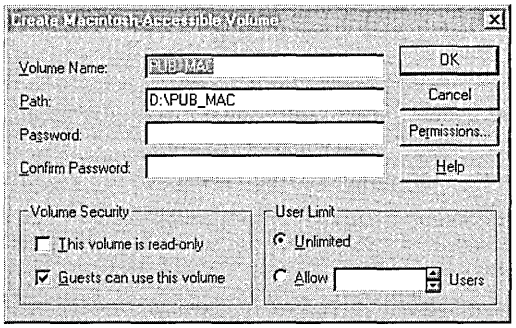
Note You cannot give a directory Macintosh-accessible volume status if it is a subdirectory of another directory that has Macintosh-accessible volume status. Refer to Chapter 16, "How Services for Macintosh Works," for more information.

You designate a directory as a Macintosh-accessible volume using the **Create Volume** command on the **MacFile** menu. From the **Create Volume** dialog box, you can quickly create the volume by accepting the default settings, or you can change the options.

▷ To create a Macintosh-accessible volume

1. From File Manager, select the directory that you want to designate as a Macintosh-accessible volume.
2. From the **MacFile** menu, choose **Create Volume**.

   The **Create Macintosh-Accessible Volume** dialog box appears.



The default setting for each option follows:

Option	Default Setting
Volume Name	Same as the directory name. The character limit is 27.
Path	Same as the directory path.
Password/Confirm Password	No password.
This volume is read-only	Off.
Guests can use this volume	On (Yes).
User Limit	Unlimited.
Permissions	Current directory permissions.

Using the default name and path has some advantages when a directory will be available as a share to PC users and as a volume for Macintosh users. Ease of communication between the two clients is simplified if the directory is referred to by the same name.

3. To accept the default options, click **OK**. Otherwise, continue to the next step.
4. In the **Volume Name** box, type a volume name that Macintosh users will see when they log on.
5. In the various boxes, specify a new path, password, security options, and user limits.

   These options are described later in this chapter, in "Modifying a Macintosh-Accessible Volume."
6. Click **Permissions** to set directory permissions for Macintosh users.

   The Macintosh-accessible volume automatically inherits the permissions of the corresponding directory, although you may change these. For further explanation of permissions, see "Setting Permissions for Volumes and Folders," later in this chapter.
7. Click **OK**.

Creating a Macintosh-Accessible Volume on a CDFS Volume

To create a Macintosh-accessible volume on a CDFS volume, you follow the same procedure you used to create one on an NTFS-partitioned drive. The only difference is that the CDFS disk is read-only. So, SFM will interpret all security options as See Files and See Folders (read-only).

Creating Folders in a Volume

From the computer running Windows NT Server, you can create subdirectories for a Macintosh-accessible volume or folders for Macintosh clients. The procedure for doing so is no different than the procedure for creating other directories or folders on the respective systems.

On the computer running Windows NT Server, the folders appear in the File Manager's directory tree as subdirectories of the directory. To create another subdirectory, you select the directory in which it will appear, and choose **Create Directory** from the **File** menu.

On the Macintosh, you create folders using the **New Folder** command on the **File** menu. You view and use folders in the Macintosh-accessible volume just as you would any other volume—by using the **View** menu to see the folders organized by Name, Date, Icon, Size, and so forth.

You cannot, however, designate the subdirectory or folder as another Macintosh-accessible volume when the directory is already designated as a Macintosh-accessible volume. For a quick review, see the illustration in the section "Configuring Macintosh-Accessible Volumes" in Chapter 16.

Setting Permissions for Volumes and Folders

Just as you set permissions on shared directories to control which PC users have access to the share, you control who can use Macintosh-accessible volumes by setting permissions. Permissions also control what kind of access is granted to users. For example, permissions dictate which users can make changes to a folder and which ones can read the content of the folder but not alter it in any way. Permissions for volumes and folders can be set in a number of ways.

From File Manager, you can set Windows NT-style permissions with the **Permissions** command on the **Security** menu. (You set permissions on a Macintosh-accessible volume or folder, just as you would on a shared directory.) Or you can use Macintosh-style permissions, available in the **Macintosh View Of Directory Permissions** dialog box. From File Manager, you can find this dialog boxes in three ways—when you choose **Permissions**, **Create Volumes**, or **View/Modify Volumes** from the **MacFile** menu.

This section explains how to set Macintosh-style permissions on Macintosh-accessible volumes and folders, using the **Macintosh View of Directory Permissions** dialog box. Information on setting Windows NT-style permissions is covered in the *Windows NT Server Concepts and Planning Guide*. For a more detailed discussion of Macintosh-style permissions and how they relate to Windows NT permissions, refer to Chapter 16, "How Services for Macintosh Works."

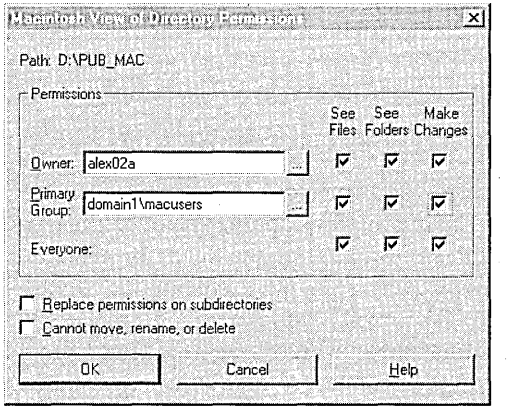
Note Macintosh files inherit the permissions set on folders; you cannot set permissions on files directly.

▶ To set Macintosh-style permissions on a Macintosh-accessible volume or folder

1. Using File Manager, select the directory you've designated as a Macintosh-accessible volume or a subdirectory that represents a folder in the volume.
2. From the **MacFile** menu, choose **Permissions**.

   Or, from the **View/Modify Macintosh-Accessible Volumes** dialog box, click **Permissions**.

   The **Macintosh View Of Directory Permissions** dialog box appears.



3. For Owner, Primary Group, or Everyone, choose the **See Files**, **See Folders**, or **Make Changes** permissions check boxes.

Use the following table to help you decide which permissions to set.

Directory Permissions

Permission	Description
See Files	Allows the owner, primary group, or everyone to see and open files in this folder
See Folders	Allows the owner, primary group, or everyone to see and open folders in this folder
Make Changes	Allows the owner, primary group, or everyone to add or delete files and folders, and save changes to files in this folder

4. Beneath the permissions, select the appropriate check boxes, which are described in the following table.

Directory Permissions Check Boxes

Check box	Description
Replace permissions on subdirectories	Copies the permissions you just set to all folders within this volume or folder
Cannot move, rename, or delete	Prevents the volume or folder from being moved, renamed, or deleted by Macintosh users

Changing the Owner or Primary Group

While setting permissions on a directory, you can change the owner and primary group to which the permissions apply. The owner is the same as the one you see when choosing **Permissions** from the **Security** menu in File Manager. The primary group, however, is unique to Macintosh clients. The owner's primary group is the group the owner works with most, and it should be the group with which the owner has the most resource needs in common. When an owner creates a folder on a computer running Windows NT Server, the owner's primary group is set as the group associated with the folder. The owner (or administrator) can change the primary group associated with the folder from either the computer running Windows NT Server or the Macintosh.

▶ **To change the owner of the directory**

1. From the **MacFile** menu in File Manager, choose **Permissions**.

   The **Macintosh View Directory Permissions** dialog box appears.

2. Choose the button to the right of the Owner list box.

   The **Owner** dialog box appears.

3. From the **Names** list, select a new owner and click **Add**.

   You can also browse for members of the selected domain (including trusted domains), and search the list of domain users for a specific user you want to select as owner.

4. Click **OK**.

▶ **To change the primary group of the directory**

1. From the **Macintosh View Of Directory Permissions** dialog box, choose the button to the right of the Primary Group list box. The **Primary Group** dialog box appears.
2. In the **Names** list, select a group, and click **Add**.

   You can also browse for groups in the selected domain (including trusted domains) and search the list of domain groups for a specific primary group.

Note In the **Owners** and **Primary Group** dialog boxes, you can also specify global groups as an owner and owners as primary groups.

To change the primary group of an owner (rather than a directory), refer to the User Manager for Domains.

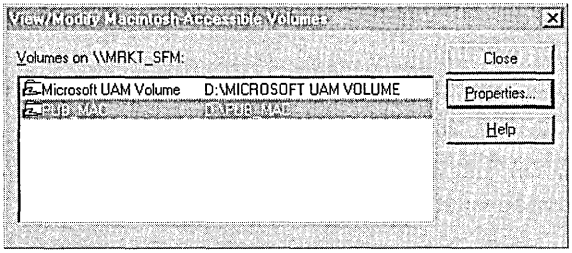
Modifying a Macintosh-Accessible Volume

You can change the properties of a Macintosh-accessible volume from the **MacFile** menu in File Manager. Properties include passwords, security options, and user limits, as well as permissions.

▶ To modify the properties of a Macintosh-accessible volume

1. From the **MacFile** menu, choose **View/Modify Volumes**.

   The **View/Modify Macintosh-Accessible Volumes** dialog box appears.



2. Select the Macintosh-accessible volume you want to change.
3. Click **Properties**.
4. In the **Properties of Macintosh-Accessible Volume** dialog box, make the changes to the options you want, as follows:

Macintosh-Accessible Volume Properties

Option/button	Description
Password	Enter the password for this volume. When Macintosh users try to mount this volume, they will be asked for this password.
Confirm password	Confirm the password you just entered.
This volume is read-only	This volume and all of its contents have read-only access. This option supersedes all directory permissions set with the Permissions button. In other words, if you give this volume read-only access, the permissions of directories with less restrictive access will not be honored.
Guests can use this volume	Guests can have access to this volume. If unchecked, guests do not see this volume.
Unlimited	Number of clients that can simultaneously access this volume is unlimited (limited only by the media).
Allow xxx Users	Number of clients that can simultaneously mount the volume on the respective desktops.
Permissions	Set access permissions on this volume. See "Setting Permissions for Volumes and Folders," earlier in this chapter.

Removing a Macintosh-Accessible Volume

If you want to make a volume unavailable to Macintosh users, you must remove it. Removing the volume does not delete the files contained in the volume, nor does it delete its status as a shared directory if it has been designated as a share for PC users. Removing only removes its status as a Macintosh-accessible volume.

▷ To remove a Macintosh-accessible volume

1. From File Manager, choose the **MacFile** menu.
2. Choose **Remove Volumes**.
3. In the Remove Macintosh-Accessible Volumes dialog box, select the volume, or volumes, you want to make inaccessible to Macintosh users.
4. Click **OK**.

   If Macintosh users are currently connected, you'll see a message that tells you who is using the volume. You can then use the **Send Message** command on the **MacFile** menu in Server Manager to send these users a warning that you intend to remove the volume. When no users are signed on, continue with the next step.

   Caution You can continue to remove the volume if users are still using it; however, the users are likely to lose data.

5. In the confirmation box, click **Yes**.

If you decide later to make the directory a Macintosh-accessible volume again, simply follow the steps in "Creating a Macintosh-Accessible Volume," earlier in this chapter.

To delete the contents of the shared directory, follow the instructions for deleting files in the *Windows NT Server Concepts and Planning Guide*.

Getting Help

Help is available when you are using the **MacFile** menu in File Manager.

▷ To get Services for Macintosh Help in File Manager

- From the **MacFile** menu, choose **Help**.

You can also choose the **Help** button in any dialog box you see after choosing commands from the **MacFile** menu.

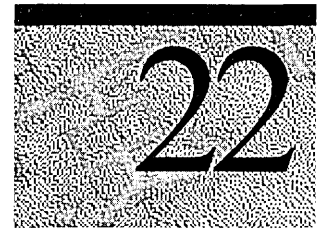
Using macfile to Work with Macintosh-Accessible Volumes

You can accomplish all of the volume configuration (and server administration) discussed in this chapter using the **macfile** command at the command prompt. The **macfile** command allows administrators to automate SFM volume, directory, file and server management by using batch programs.

For syntax of the **macfile** command, type **macfile /?** at the command prompt. For a complete reference to the **macfile** command, choose **Help** from the **MacFile** menu in File Manager.

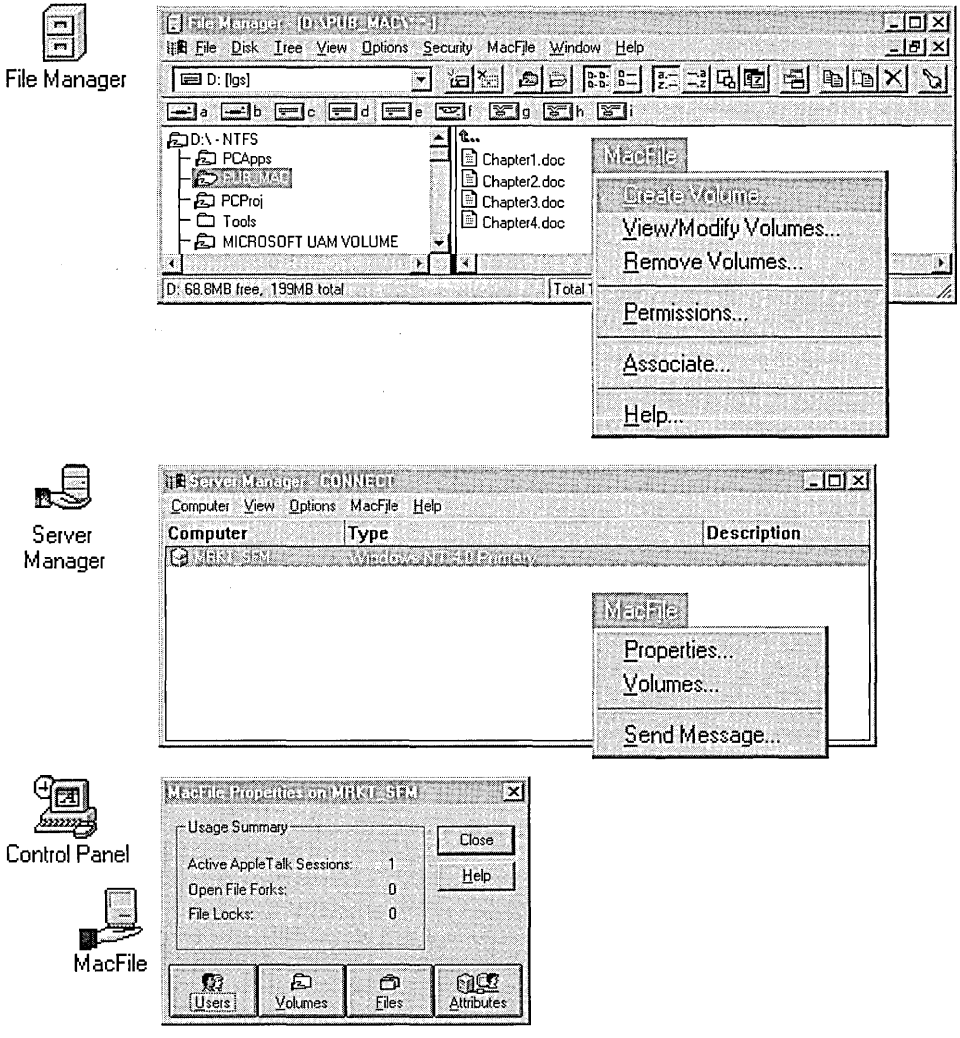
CHAPTER 22

Managing the File Server



You use User Manager to establish user accounts (including Macintosh user accounts), and you use Server Manager to set security options for the server and do other server-level tasks. When Services for Macintosh (SFM) is started, you use the **MacFile** menu in Server Manager to view the Macintosh users of the server and the Macintosh-accessible volumes. You can also send messages to Macintosh users of Windows NT Server, among other tasks.

Many tasks you perform from Server Manager are available from the MacFile icon in Control Panel. Individual volume options are available in the **MacFile** menu in File Manager and are described in Chapter 21, "Working with Macintosh-Accessible Volumes."



The File Server For Macintosh (MacFile) is available from different locations in Windows NT Server.

Setting Logon Security for Macintosh Users

To set security options for Macintosh users of SFM, use the **Properties** command on the **MacFile** menu in Server Manager. The commands available from the **MacFile** menu apply to Macintosh-accessible volumes on the computer running Windows NT Server and are described in the following procedure.

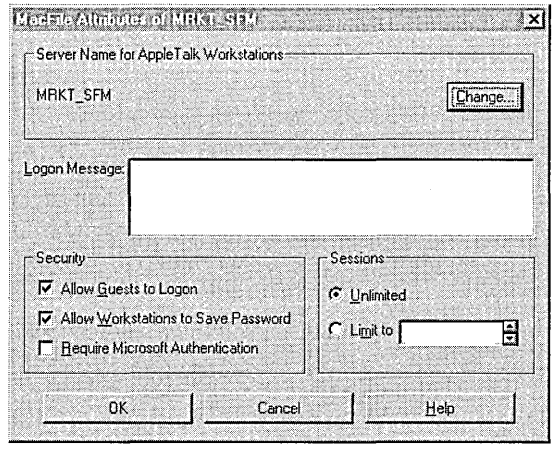
(For information on setting security for shared directories—which make files available to PC users—refer to the *Windows NT Server Concepts and Planning Guide*.)

▷ To set security options for all Macintosh-accessible volumes

1. In the **Start** menu, from the Administrative Tools folder, choose Server Manager.
2. From the **MacFile** menu, choose **Properties**.

   The **MacFile Properties** dialog box appears.
3. Click **Attributes.**

   The **MacFile Attributes** dialog box appears.



4. From the Security box, make the following selections as you prefer.

Security Options

Select this option	To do this
Allow Guests to Logon	Permit users who do not have a user account and password to log on to the computer running Windows NT Server from a Macintosh, which is connected to the AppleTalk network.
Allow Workstations to Save Password	Permit Macintosh users to save their passwords on their own workstations. That way, they won't be prompted for it each time they sign on to the computer running Windows NT Server. However, permitting this makes the computer running Windows NT Server less secure.
Require Microsoft Authentication	Specify that Macintosh users must use Microsoft Authentication rather than the Apple Standard UAM or other UAMs. If this option is chosen, Macintosh users either will not see the other UAM choices, or they will be unavailable for selection.

5. Click **OK**.

The security options available from the **Attributes** dialog box apply to all Macintosh-accessible volumes on the computer running Windows NT Server. (The individual volume permissions available in File Manager from the **MacFile** menu are explained in Chapter 21, "Working with Macintosh-Accessible Volumes.") For an explanation of Windows NT Server security issues, refer to the *Windows NT Server Concepts and Planning Guide*.

Changing the Server Name, Logon Message, and Session Limits

You can change the name of the server (the name that Macintosh users will see). You can also create a message that Macintosh users (of System 7.1) see when they log on to the computer running Windows NT Server. And you can specify the number of Macintosh clients that can simultaneously connect to the File Server For Macintosh on the computer running Windows NT Server.

▷ To change the name of the computer running Windows NT Server

1. From the **MacFile** menu in Server Manager, choose **Properties**.

   The **MacFile Properties** dialog box appears.

2. Click **Attributes.**

   The **MacFile Attributes** dialog box appears.

3. Click **Change.**
4. In the **Server Name For AppleTalk Workstations** dialog box, type a new name for the server.
5. Click **OK**.
6. In the Services icon in Control Panel, stop and restart File Server For Macintosh.

▷ To create a logon message for 7.1 System users

1. From the **MacFile** menu, choose **Properties**.

   The **MacFile Properties** dialog box appears.

2. Click **Attributes**.

   The **MacFile Attributes** dialog box appears.

3. In the Logon Message box, type a message that you want Macintosh users to see when they sign on to the computer running Windows NT Server.

   You can type four lines of text (the AppleTalk limit).

4. Click **OK**.

▷ To set session limits

1. From the **MacFile** menu in Server Manager, choose **Properties**.

   The **MacFile Properties** dialog box appears.

2. Click **Attributes**.

   The **MacFile Attributes** dialog box appears.

3. In the Session box, choose **unlimited** or specify a client limit by entering the number you want.

   The number you specify is the number of clients that can simultaneously gain access to the File Server For Macintosh. If you choose **unlimited**, the number of connections is limited only by the capabilities of the network media. However, performance improves when you limit the number of sessions.

4. Click **OK**.

Setting Up User Accounts for Macintosh Users

User accounts are created for Macintosh users just as they are created for other Windows NT Server users. A guest account is automatically created when you install Windows NT Server and, by default, both local guests and guests accessing the server through a client on the network (including a Macintosh) are allowed. This means that if users log on without a regular user account and password, they will be logged on as a guest.

Guests have some access to shared resources. Guests can do everything that those with a user account can do, except keep a local profile on their computers, lock their computers, and create, delete, and modify local groups on their computers.

The guest account cannot be deleted, but it can be disabled on Windows NT computers. If it is disabled, no network users, including Macintosh users, will be able to log on without a user account and password. To disable only Macintosh guests from the computer running Windows NT Server, follow the instructions in "Setting Logon Security for Macintosh Users," earlier in this chapter. For more information about the guest account, refer to the *Windows NT Server Concepts and Planning Guide*.

Stopping and Pausing Services

When you set up SFM, two services are automatically started: File Server For Macintosh and Print Server For Macintosh. (The AppleTalk Protocol is started as well.) At times, you might need to stop these services, as shown in the following table:

Service	Reason
Print Server For Macintosh (MacPrint)	Stop it to install another printer driver or to configure a printer; or to immediately see the result of deleting, creating, or changing a printer.
	Stop it to remove the Print Server for Macintosh service.
File Server For Macintosh (MacFile)	Stop it to change the server name that Macintosh users will see and to remove the MacFile Service.
	Pause it when you want to make changes to the server attributes but want to allow current users to continue working. If this service is paused, no new Macintosh users can log on to the computer running Windows NT Server.
AppleTalk Protocol	Stop it to change router parameters and the default networking zone, and to remove it (which automatically stops the file and print servers).

Use the **Services** command on the **Computer** menu in Server Manager to control the file and print servers. (You can use the Services icon in Control Panel to stop or start Print Server For Macintosh and to stop, start, pause, or continue File Server For Macintosh.)

Use the Devices icon in Control Panel to stop the AppleTalk Protocol and, consequently, both the file and print servers.

▶ **To stop, start, pause, or continue services**

1. From Server Manager, select the **Computer** menu.
2. Choose the **Services** command.
3. In the **Services** dialog box, find the service you want to change, and check its status.
4. Select either the File Server For Macintosh or Print Server For Macintosh.

   You cannot pause and continue the Print Server For Macintosh.
5. Click **Start, Stop, Pause**, or **Continue** as appropriate.

   To change the startup options (for example, to specify manual startup), click **Startup**. For a thorough explanation of this dialog box, refer to online Help.
6. Click **Close.**

Checking the Event Log

To check events on the computer running Windows NT Server, use Event Viewer, which is available in the Administrative Tools folder. If SFM is running, you can see events that involved the File or Print Server For Macintosh or the AppleTalk Protocol.

▶ **To check AppleTalk and MacFile events**

1. From the Administrative Tools folder, choose Event Viewer.
2. Review the Source list and look for MacFile, MacSrv, or AppleTalk events you want to monitor.

   Use the Event Viewer options for these services just as you would for other Windows NT Server events. For example, to see specific events, choose **Filter Events** from the **View** menu. (The Browser service must be started.)

▶ **To check printing events**

- From the **Log** menu, choose **Application**.

  You will see a list of events, including those generated by the AppleTalk Print Monitor and MacPrint.

Use the Event Viewer options for these services just as you would for other Windows NT Server events.

For more information about Event Viewer, refer to the *Windows NT Server Concepts and Planning Guide*.

Viewing a List of Macintosh-Accessible Volumes

Use the **MacFile** menu in Server Manager to view a list of all volumes available to Macintosh users on the computer running Windows NT Server. The **Volumes** command lists all directories that have been designated as Macintosh-accessible volumes and allows you to create and remove individual volumes, just as you can from the **MacFile** menu in File Manager.

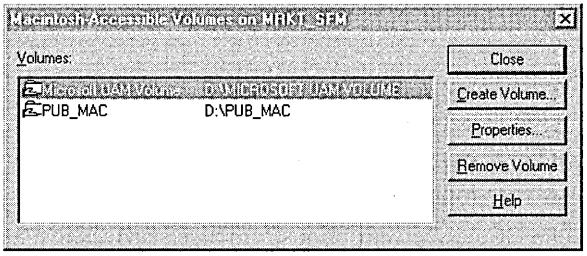
The **Volumes** button, which is available when you choose **Properties** from the **MacFile** menu, allows you to see which users are connected to individual volumes and to disconnect them. For more information, refer to "Disconnecting Macintosh Users and Volumes," later in this chapter.

▷ To view a list of Macintosh-accessible volumes

1. From the Administrative Tools folder, choose Server Manager.
2. From the **View** menu, choose **MacFile**.

   This choice limits the list of servers so that you can easily choose the computer running Windows NT Server and SFM.
3. From the **MacFile** menu, choose **Volumes**.

   The **Macintosh-Accessible Volumes** dialog box appears.



   This dialog box displays a list of Macintosh-accessible volumes on the computer running Windows NT Server. You can create or delete volumes here, or change the properties and permissions of the volumes. (Properties and permissions for volumes are explained in Chapter 21, "Working with Macintosh-Accessible Volumes.")

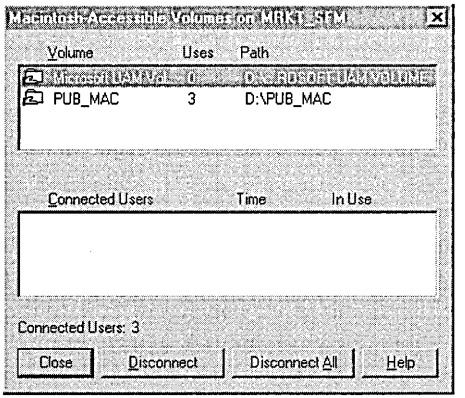
You can also view other information about the Macintosh-accessible volumes on the computer running Windows NT Server, including their paths and the names of users connected to them.

▷ **To see volume information**

1. From the Administrative Tools folder, choose Server Manager.
2. From the **MacFile** menu, choose **Properties**.

   The **MacFile Properties** dialog box appears.
3. Choose the **Volumes** button.

   The **Macintosh-Accessible Volumes** dialog box appears.



4. Select a Macintosh-accessible volume.

   You can see how many times the volume has been mounted by Macintosh users as well as the volume's directory path on the computer running Windows NT Server. You can also see how long users have been connected to the volume and whether there are open files on the volume.
5. Click **Close**.

Viewing Current Users of Volumes

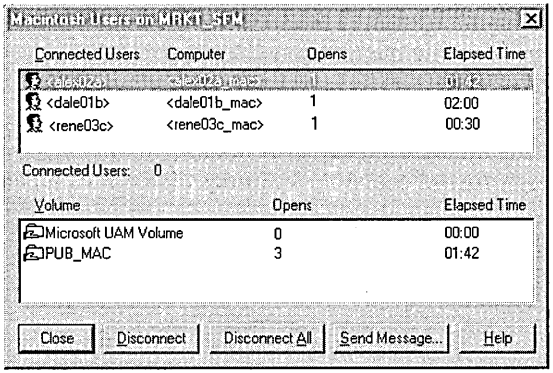
You can see the current list of users connected to selected Macintosh-accessible volumes.

▷ **To view connected users**

1. From the Administrative Tools folder, choose Server Manager.
2. From the **MacFile** menu, choose **Properties**.

   The **MacFile Properties** dialog box appears.
3. Choose the **Users** button.

The **Macintosh Users** dialog box appears.



4. Select a user.

   You see the Macintosh-accessible volumes that the user has mounted, the name of the Macintosh computer, how many volume file forks are open, and the amount of time that the user has been connected to the computer running Windows NT Server in hours and minutes. For more information about file forks, refer to the next section.

   Use the **Disconnect** and **Disconnect All** buttons to disconnect a user from all connected volumes or all users from all connected volumes. For more information, refer to "Disconnecting Macintosh Users and Volumes," later in this chapter.

5. Click **Close**.

Viewing Open File Forks

At times, you might want to view the resources (*file forks*) that Macintosh clients are using. (Remember that data is kept in a data fork and system information is kept in a resource fork.) By viewing open file forks, you can tell who has what forks open before you stop the File Server For Macintosh or disconnect a user.

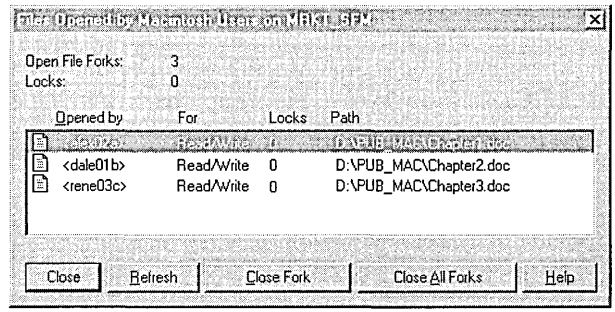
▶ To view open file forks

1. From the Administrative Tools folder, choose Server Manager.
2. From the **MacFile** menu, choose **Properties**.

   The **MacFile Properties** dialog box appears.

3. From the **MacFile Properties** dialog box, click **Files**.

The **Files Opened by Macintosh Users** dialog box appears.



This dialog box lists all the resource and data forks that are open on Macintosh clients connected to the computer running Windows NT Server. A summary of the options in this dialog box follows:

File Forks Opened by Macintosh Users Dialog Box

File fork option/button	Description
Open File Forks.	Summary count of all the open data and resource forks.
Locks. (Total lock count. *Locks* prevent multiple users from gaining access to the same fork at the same time.)	Total count of all the locks on file forks in Macintosh-accessible volumes.
Opened by.	Macintosh user who has opened the file fork.
For.	Permissions set (for example, Read/Write)
Locks (individual fork count).	Number of locks on the fork.
Path.	Directory path of the file.
Refresh.	Update the list box and recalculate counts of forks and locks.
Close Forks.	Close the selected file.
Close All Forks.	Close all Macintosh-accessible volume forks on the computer running Windows NT Server.

4. Choose one of the buttons described in the previous table.
5. Click **Close.**

Disconnecting Macintosh Users and Volumes

To disconnect users from volumes, choose **Properties** from the **MacFile** menu in Server Manager or choose the MacFile icon in Control Panel. The following instructions describe Server Manager approach, but you can use the basic instructions with the MacFile icon in Control Panel as well.

Note It's a good idea to send a message to users before disconnecting them or the volumes that they are using. Otherwise, they might lose data. Refer to the next section for more information.

▶ To disconnect users from Macintosh-accessible volumes

1. From the Administrative Tools folder, choose Server Manager.
2. From the **MacFile** menu, choose **Properties.**

   The **MacFile Properties** dialog box appears.
3. Use the following table to determine what you want to disconnect:

MacFile Disconnect Options

MacFile Propertiesdialog box	Disconnect button	Disconnect All button
Users button: When selected, displays the **Macintosh Users** dialog box with **Disconnect** and **Disconnect All** buttons.	Disconnects a selected user from all connected volumes.	Disconnects all users from all connected volumes.
Volumes button: When selected, displays the **Macintosh-Accessible Volumes** dialog box with **Disconnect** and **Disconnect All** buttons.	Disconnects selected users of a selected volume.	Disconnects all users from selected volumes.

4. Click **Users** or **Volumes.**
5. Select the user or volume you want to disconnect from the respective dialog boxes.
6. Click **Disconnect** or **Disconnect All**, as appropriate.
7. From the confirmation box that appears, click **Yes.**

Caution If you disconnect users or volumes, you could cause the loss of data. It's a good idea to send users a message before disconnecting.

Sending Messages to Connected Macintosh Users

SFM enables you to send messages to Macintosh clients that are connected to the computer running Windows NT Server. You can send messages to Macintosh users from two places:

- MacFile icon in Control Panel (choose the **Users** button).
- **MacFile** menu in Server Manager

The following instructions describe the **MacFile** menu approach; however, the basic instructions apply for the MacFile icon in Control Panel as well.

▶ To send a message to all connected Macintosh users

1. From the Administrative Tools folder, choose Server Manager.
2. From the list of computers, select a server that is running SFM.
3. From the **MacFile** menu, choose **Send Message**.

   The **Send Message** dialog box appears.
4. In the Message box, type the message you want to send to Macintosh users.

   You can type up to four lines, the AppleTalk limit, for example, "The server is going to be shut down in 10 minutes."
5. Click **OK**.

▶ To send a message to individual Macintosh users of the computer running Windows NT Server

1. From the **MacFile** menu, choose **Properties**.
2. Click **Users**. The **Macintosh Users** dialog box appears.
3. From the Connected Users box, select the user to whom you want to send the message.
4. Click **Send Message**.
5. Click **Selected MacFile**.
6. In the Message box, type the message you want to send.

   You can type up to four lines.
7. Click **OK**.

Setting Extension-Type Associations

With extension-type associations, users of both the PC and the Macintosh version of an application can easily work on the same data file. The extension-type associations provided with SFM tell the Finder which MS-DOS filename extensions correspond with which Macintosh file types and file creators. When a file on the server has a filename extension associated with a Macintosh file type and file creator, the Finder displays the appropriate icon for that file when a Macintosh user browses the files available on the server. And if a Macintosh user chooses the file, the appropriate application starts and opens the file.

The extension-type associations that follow are already defined. Others can be added to SFM. Refer to the **Association** command in the **MacFile** menu (from File Manager) to see a comprehensive list.

PC application/file format	Macintosh application	MS-DOS extension	Macintosh type	Macintosh creator
Adobe® Encapsulated PostScript	Adobe Illustrator® '88	EPS	EPSF	ARTZ
Aldus® PageMaker® for Windows version 2.0, Aldus PageMaker for OS/2 version 2.0	Aldus PageMaker for Macintosh version 2.0	PUB	PUBF	ALD2
Aldus PageMaker for Windows version 3.0	Aldus PageMaker for Macintosh version 3.0	PM3	ALB3	ALD3
Publication	Publication	PT3	ALT3	ALD3
Template	Template	TEM	ALT3	ALD3
Template	Template	TPL	ALT3	ALD3
Template	Template	TIF	TIFF	ALD3
TIFF graphics file	TIFF graphics file			
Aldus PageMaker for Windows version 4.0	Aldus PageMaker for Macintosh version 4.0	PM4	ALB4	ALD4
Publication	Publication	PT4	ALT4	ALD4
Template	Template	TEM	ALT4	ALD4
Template	Template	TPL	ALT4	ALD4
Template	Template	TIF	TIFF	ALD4
TIFF graphics file	TIFF graphics file			
Borland® dBASE®	Microsoft FoxBASE®/FoxBASE+® for Macintosh	DBF	F+DB	FOX+
Lotus® 1-2-3® for Windows version 2.0	Lotus 1-2-3 for Macintosh version 1.1	WK3	LWK3	L123

PC application/file format	Macintosh application	MS-DOS extension	Macintosh type	Macintosh creator
Microsoft Excel for Windows version 3.0, Microsoft Excel for OS/2 version 3.0	Microsoft Excel for Macintosh version 3.0			
Chart	Chart	XLC	XLC3	XCEL
Spreadsheet	Spreadsheet	XLS	XLS3	XCEL
Macro sheet	Macro sheet	XLM	XLM3	XCEL
Workspace	Workspace	XLW	XLW3	XCEL
Add-in macro file	Add-in macro file	LA	XLA	XCEL
Template file	Template file	XLT	SLM3	XCEL
Microsoft Excel for Windows version 4.0,Microsoft Excel for OS/2 version 4.0	Microsoft Excel for Macintosh version 4.0			
Chart	Chart	XLC	XLC4	XCEL
Spreadsheet	Spreadsheet	XLS	XLS4	XCEL
Macro sheet	Macro sheet	XLM	XLM4	XCEL
Workspace	Workspace	XLW	XLW4	XCEL
Add-in macro file	Add-in macro file	XLA	XLA	XCEL
Template file	Template file	XLT	SLM3	XCEL
Microsoft Multiplan®/SYLK	Microsoft Excel for Macintosh version 3.0	SLK	TEXT	XCEL
Microsoft PowerPoint® version 2.0	Microsoft PowerPoint for Macintosh version 2.0	PPT	SLD2	PPT2
Slides				
Microsoft PowerPoint version 3.0	Microsoft PowerPoint for Macintosh version 3.0	PPT	SLD3	PPT3
Slides				
Microsoft Project for Windows version 1.*x*	Microsoft Project for Macintosh version 1.*x*			
Projects	Projects	MPP	MSPF	MSPJ
Exchange format	Exchange format	MPX	MSPJ	MSPJ
Calendars	Calendars	MPC	MSPJ	MSPJ
Views	Views	MPV	MSPJ	MSPJ
Workspaces	Workspaces	MPW	MSPF	MSPJ

PC application/file format	Macintosh application	MS-DOS extension	Macintosh type	Macintosh creator
Microsoft Word for Windows version 2.0	Microsoft Word for Macintosh version 5.1	DOC	WDBN	MSWD
Document	Document	WRD	TEXT	MSWD
Text Document	Document	RTF	TEXT	MSWD
Rich Text	Rich Text	STY	TEXT	MSWD
Style sheet	N/A	GLY	TEXT	MSWD
Glossary	N/A			
N.A./Comma-Separated Values	Microsoft Excel for Macintosh version 4.0	CSV	TEXT	XCEL
N.A./SIT files	Alladin Stuffit	SIT	SIT!	SIT!
N.A./Text (TXT files)	Teachtext	TXT	TEXT	TTXT
PC Program	N.A.	EXE	DEXE	LMAN
		COM	DEXE	LMAN
		CMD	DEXE	LMAN
		BAT	DEXE	LMAN
Symantec Ready!	Symantec MORE	RDY	TEXT	MORE
Unknown File	N.A.	All others	TEXT	LMAN
Visicalc (DIF)	Microsoft Excel for Macintosh version 4.0	DIF	TEXT	XCEL

You can also add extension-type associations. You can add new associations for an application not listed in the preceding table, or you can add extra associations for any of the listed applications. For example, if your company has a custom of saving Microsoft Word documents with a .WRD extension, you could add the following extension:

MS-DOS extension	Macintosh file type	Macintosh file creator
.WRD	WDBN	MSWD

When you add a new extension-type association, it affects only files that are subsequently created on the server, not currently existing files. Moreover, you can associate multiple extensions with a Macintosh file type and creator. However, the reverse is not true. Only one file type and creator can be associated with an extension.

Note The WKS and WK1 formats allow a single data file to be used by users of Microsoft Excel, Lotus 1-2-3, and Informix® Wingz®. However, you can set up an extension for only one Macintosh application for this format. For example, if you map the WKS and WK1 extensions to the file type and file creator values for Microsoft Excel for Macintosh and then a Macintosh user double-clicks the file's icon, the file will be loaded into Microsoft Excel for Macintosh.

▷ **To make new extension-type associations**

2. In File Manager, from the **MacFile** menu, choose **Associate**.
3. In the Files with MS-DOS Extension box, type an extension, or select one from the list.

   If the extension is already associated with a file type and file creator, it will be highlighted in the Creator list.
4. In the **Creator** box, select a creator and type to which you want to associate this extension.
5. Click **Associate**.

   The new association is added to the Creator list in the **Extension-Type Association** dialog box.

▷ **To add file creators and types**

1. Click **Add**.
2. In the **Add Document Type** dialog box, type the file creator and type and, optionally, a description.
3. Click **OK**.

   You'll see the new creator in the Creator list. When you're ready to associate it with an extension, follow the previous instructions for creating an extension-type association.

Note File creator and type are case-sensitive on the Macintosh and thus must be entered exactly as they appear on the Macintosh.

▶ **To edit a description of a file type**

1. In the **Creator** box, select a file creator and type.
2. Click **Edit**.
3. In the **Edit Document Type** dialog box, type the new description.
4. Click **OK.**

   The new description will appear in the Creator list.

▶ **To remove a file type and associations**

1. In the **Creator** box, select a file creator and type.
2. Click **Delete**.
3. Click **Yes** to confirm that you want to remove the selected file type and associated extensions.

Backing Up Files on the Server

Following the Windows NT Server backup procedure will also back up Macintosh-accessible volumes. First, however, it is a good idea to stop the File Server for Macintosh service by using the Services icon in Control Panel. Stopping the service ensures that all files are backed up. You must stop the File Server for Macintosh before restoring a volume. The use of the Backup tool, which is available in the Windows NT Server Administrative Tools folder, is described in the *Windows NT Server Concepts and Planning Guide*.

You can also back up and restore volumes from the Macintosh client, using Macintosh backup software, such as FastBack™, RetroSpect, or Norton Utilities®.

▶ **To back up or restore Macintosh-accessible volumes from the Macintosh**

1. Make sure all the Macintosh-accessible volumes you want to back up are not in use by other Macintoshes.
2. Mount the Macintosh-accessible volumes you want to back up on the Macintosh desktop.
3. Start a Macintosh backup and restore program from the Macintosh.

   Follow the instructions given by your backup software program.

Getting Help

Help specific to SFM is available in Server Manager and in the **MacFile Properties** dialog box, which appears when you choose the MacFile icon in Control Panel.

▷ **To get Services for Macintosh Help in Server Manager**

- From the **Help** menu, choose **MacFile**.

▷ **To get Help when using the MacFile icon in Control Panel**

1. Choose the MacFile icon.

   The **MacFile Properties** dialog box appears.

2. Click **Help**.

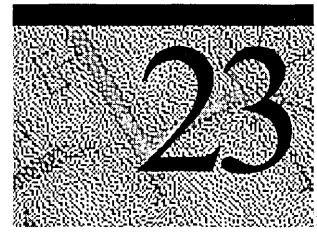
Using Macfile to Administer the Services for Macintosh Server

You can accomplish all of the server configurations discussed in this chapter (and volume, file, and directory management) using the **macfile** command at the command prompt. The **macfile** command allows administrators to automate SFM volume, directory, file, and server management by using batch programs.

For syntax of the **macfile** command, type **macfile /?** at the command prompt. For a complete reference to the **macfile** command, choose **Help** from the **MacFile** menu in File Manager.

CHAPTER 23

Troubleshooting



This chapter provides solutions for problems that might occur on a computer running Windows NT Server with Services for Macintosh (SFM) installed. This includes problems that both users and administrators might encounter. Network error messages are explained in the Windows NT Server message database, which is available as part of the Help system.

Administrator and User Issues and Solutions

When a Macintosh user is unable to gain access to an SFM resource, first check the Macintosh and ensure that the following are true:

- The Macintosh client is using version 6.0.7 or later of the Macintosh operating system (the system software).
- The Macintosh client is using current versions of its network drivers, and these versions are compatible with the version of the operating system on that Macintosh.

To determine whether the issue is with the Macintosh, try to access a network entity other than the computer running Windows NT Server or printer. (For example, try to access an AppleShare server or a printer that isn't used by SFM.) If the Macintosh cannot access any network entity, the problem might be with the Macintosh.

If a computer running Windows NT Server fails to start, and Event Viewer is filled with AppleTalk error messages see if your network has a bridge that is filtering packets. It might be filtering out the server's requests to find a unique address

See "Other Issues," later in this chapter.

The following are common user problems:

A Macintosh-accessible volume is unavailable to a user.

- The volume might be configured as a *private volume*. A private volume is any volume for which the owner, primary group, and/or everyone categories have no access permissions—only the volume's owner has permissions. In this case, only the owner has access to the volume.

  To make the volume accessible to users, the owner should use the **Permissions** dialog box, available from the **MacFile** menu, to give the primary group and/or everyone categories at least one permission for the volume.
- If the Macintosh-accessible volume is on a CDFS volume, and it appears in the Chooser but cannot be selected, the CD-ROM on which it was created might not be in the disk drive.

  Be sure that the correct CD-ROM is in the disk drive and that the drive door is closed.

A Macintosh user's password has expired without notification.

- Users will be notified that their passwords have expired only if the MS UAM files are installed on their clients. If they are using the Apple standard UAM, they will be told only that their logon attempts failed and to try again later. For more information on installing the Macintosh client software, see the Teachtext ReadMe file in the Microsoft UAM Volume.

A user has forgotten his or her password.

- Assign the user a new password. To do so, use User Manager to reset the password.

A user sees the message that their password is incorrect, even though it was entered correctly.

- The user might have two accounts, with different passwords, on separate domains. Have the user enter the domain and then the account name in the Name box when they log on. For example:

  ```
  Domain1\alex02A
  ```

The computer running Windows NT Server and SFM appears in the Chooser on Macintosh clients and then disappears. The appearances are erratic and unpredictable.

- Two physical AppleTalk networks have been given the same network numbers. The server started first works fine. When the second server is started, it appears in the Chooser on one Macintosh client, and then disappears and appears in the Chooser on a different client. The order of appearance is unpredictable.

  Use the **Configure** button, available when you choose the Network icon in Control Panel, to check the network numbers used for each physical network. When you find the duplicates, change one so that all physical networks use unique network numbers. After you make the change, restart the AppleTalk Protocol on the server on which you made the change. Refer to Chapter 19, "Configuring Services for Macintosh," for more information.

  If you find no duplicates, see if your network has a bridge that is filtering packets. It might be filtering out the second server's requests to find a unique address.

The computer running Windows NT Server and printers intermittently appears and disappears in the Chooser.

- Zones and network numbers are no longer in correspondence.

  When you change the name of a zone, you must shut down the routers directly connected to the networks in question for 10 to 15 minutes before restarting. This allows the other routers to discard old zone information.
- If you haven't changed zone names recently, this situation could occur if an AppleTalk network number is duplicated on your AppleTalk internet.

Cannot find a file or folder.

- The user might not have the necessary permissions for the folder that contains the file or folder in question. The administrator or the owner of the folder can reset permissions to allow the user to access the folder.

Cannot save a file with an 8.3 filename from the Macintosh.

- A short name might already exist with that name; however, Macintosh users cannot see it.

  Give the 8.3 filename a different name.

Cannot find a server.

Follow these steps:

1. Be sure the cable system between the client and the server is correct. Be sure the network connection, layout, and cable termination conform to the specifications of the cable system you are using.
2. Start with the client that can't find the server. If the cable system is LocalTalk, ensure that the LocalTalk connector box is firmly attached to the printer port on the back of the Macintosh client, not the modem port.

   If the cable system is not LocalTalk, ensure that the network connector is securely connected to its port. Select the Network icon in Control Panel to review other network settings.
3. Determine whether other clients are having the same problem.

   If they are, check the cables and connections at the server, and ensure that the server is operating properly. If the server is not the source of the problem, proceed to step 4.
4. Check for breaks in the cable system. If the missing server is on a local network, check each client between the client that can't find the server and the server until you find the server in the Chooser. The break in the cable system is between the client that shows the server in the Chooser and the one that does not.

   If the missing server is on a different physical network in the internet, use your router seeding plan and server information table to determine which client is the first one beyond the router that links the two networks. Test that client, and then test each client beyond it—in the direction of the server—until the server appears in the Chooser. For more information about router seeding plans and server databases, see Chapter 17, "Planning Your AppleTalk Network."

   If the server was visible at the first client, work backward toward your own network, testing the client adjacent to each router until the server fails to appear in the Chooser. Isolate the break by testing the clients on this network.
5. When you have isolated the network break, check the network cables and connections at that location to make sure all are securely attached, and try again to display the server in the Chooser. If necessary, try replacing cables or connectors.

Cannot see any zones within the Chooser on a Macintosh.

- Make sure AppleTalk is active in the Chooser.
- Open Control Panel, and then open the Network icon. Make sure the correct network port is selected.
- There might be router problems. Check for the following:
  - The Macintosh might be running on an AppleTalk Phase 2 Network without the correct Ethernet driver.
  - The router might be using Phase 1 and the rest of the internet is using Phase 2.
  - The Macintosh is configured for one type of network media (such as LocalTalk) but is actually on a network that uses a different media type (such as Ethernet or token ring).

If the problem persists, make sure all routers are configured properly.

The Microsoft UAM Volume cannot be found.

- When the computer running Windows NT Server was installed, there might have been insufficient disk space for the Microsoft UAM Volume. Or the computer running Windows NT Server might have been installed without an NTFS partition.

  In this case, you can create the volume by typing and entering the following at the command prompt:

  setup /i oemnxpsm.inf /c uaminstall

  This command line copies UAM files to the AppleShare folder in the first NTFS partition and sets up Registry values for this volume in the Registry Editor.

View of a folder is erased or does not match the view selected in the View menu.

The folder owner must log on to the server, connect to the Macintosh-accessible volume, and select a view (such as **View By Icon**, **View By Name**, and so on) from the **View** menu. The selected view then remains in effect.

The Finder occasionally cannot show the correct view of a folder. Having the folder owner log on and select the view resolves the situation.

A file is now displayed with the default PC icon instead of the correct icon.

- The application that uses that type of data file might have been removed from the Macintosh.

  If the file had no resource fork, use the Apple **ResEdit** utility to reset the file type and file creator of the file. Use this utility only if you are experienced with it.

A PC user cannot see the contents of a folder.

- The PC user does not have sufficient permissions to view the contents of the folder. Use the computer running Windows NT Server to make sure the user has Read permission, or the folder owner can use a Macintosh to give the PC user both the See Files and See Folders permissions. (A PC user must have both these permissions to get the Windows NT Server Read permission.)

A Macintosh user did not receive a server message.

- Only Macintosh clients running version 2.1 (or later) of the AppleTalk Filing Protocol can see server messages. Make sure the client has installed version 3.0 of AppleShare, which uses later versions of this protocol.

A user cannot automatically connect to a Macintosh-accessible volume using an alias.

- Macintosh clients can be configured to automatically connect to volumes when the client is started or when the user double-clicks an alias to an object on a volume. However, automatic connection to volumes is not supported by the Macintosh system software if the volume is configured with a volume password, or if the user originally connected to the volume using Microsoft Authentication.

  If the volume has a password, you can mount it through the Chooser and then use the alias. Or you can specify that it be opened at system startup time when you mount the volume.

  If you are using Microsoft Authentication to log on to the server, you must mount the volume through the Chooser and then use the alias.

Printing Issues and Solutions

The following are common situations involving printers or printing devices:

AppleTalk printers don't show up in the Printers Folder's Available AppleTalk Printer's dialog box.

- Clicking the AppleTalk Zone name does not display the printers in that zone. You must double-click the Zone name from this dialog box.

Printing error messages consistently appear when the printing device prints documents.

- Reset the printing device by turning it off and then on again.

The PostScript error "Offending command" appears at the end of the printed document or elsewhere.

- A user or administrator might have canceled the print job while it was spooling. No action is necessary, and you can reprint the file as desired.
- A user is spooling to a PSTODIB printing device, and it has PostScript level 2 elements or is a PostScript level 2 document.

Print jobs fail to print.

- Check each printing device that prints jobs for these printers. If one of the printing devices is turned off, all printing devices can stop printing.

Macintosh extended characters (such as bullets, smart quotes, and copyright and trademark symbols) are changed into other characters on the LaserWriter II.

- Set the communications port for the LaserWriter correctly, referring to the owner's manual for the printing device. If the LaserWriter hasn't been set correctly, printing problems can occur, regardless of how you set the COM port in Control Panel in Windows NT Server. This problem affects Macintoshes more frequently than PCs because Macintoshes use extended characters more often than other clients do.

Other Issues

Filenames—POSIX

- Do not use POSIX filenames in the same directory tree that Macintosh users can access through Macintosh-accessible volumes. The POSIX subsystem is case sensitive (that is, you could create one file called accounts, another called ACCOUNTS and even another called Accounts).

MCA Computers and LocalTalk Cards

- Because of a hardware issue, the LocalTalk card should not be set to either IRQL.5 or IRQL.6. Otherwise, Windows NT Server will not reboot on MCA computers.
- The interrupt setting used for the Local Talk card should not be shared with any other device.

Reinstalling and Permissions

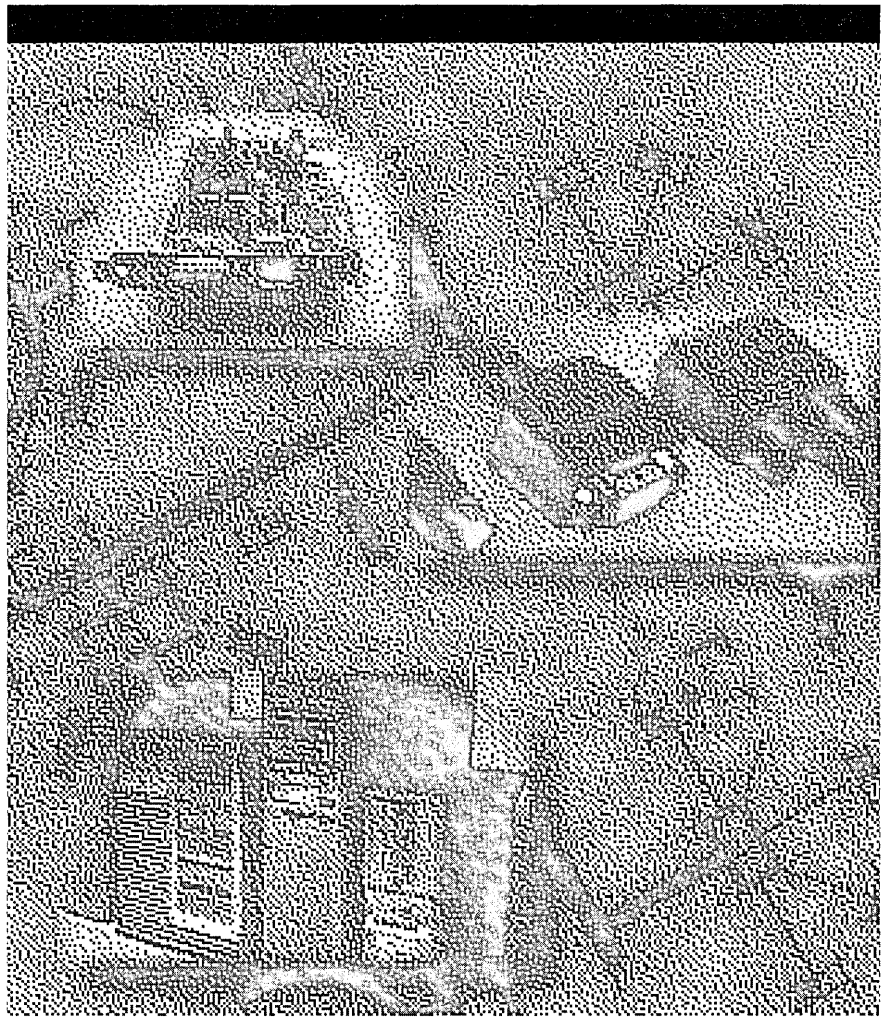
- If you install Windows NT Server on a computer that already has an NTFS partition, or if you reinstall Windows NT Server, you cannot designate or redesignate a directory as a Macintosh-accessible volume. You can avoid this situation by reformatting the NTFS partition or by simply not using formerly created NTFS directories when creating Macintosh-accessible volumes.

Adding and Removing Trusted Domains

- If a domain administrator adds or removes a trusted domain, you need to stop and restart the File Server for Macintosh so that it can register the changes.

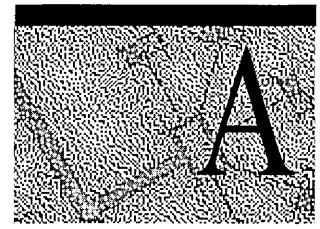
PART 6

Appendixes



APPENDIX A

RAS Registry Values



When you install the Remote Access Service on a Windows NT Server computer, the Setup program adds the **Remote Access** key to the Windows NT Registry. The **Remote Access** key and its subkeys contain parameters specific to Remote Access.

This appendix tells you how to modify Remote Access parameters in the Registry.

Modifying the Registry

The Remote Access Setup program adds Remote Access keys to the Windows NT Registry.

Remote Access generally supplies good default values for RAS parameters, which you normally do not need to override. Still, for some systems, you might want to adjust individual parameters to suit your particular needs.

There are several sets of parameters you can modify or add. To override their defaults, add or change the appropriate key in the Registry. You can find these keys on the paths indicated in each section below.

▷ To edit the Registry

1. In the **Start** menu, click **Run**.
2. In the **Open** box, type **regedt32**.

This command can also be run from the Command Prompt.

For detailed information on how to add a parameter to a key in the Registry, see online Help for the Windows NT Registry editor.

RemoteAccess Parameters

The default values of these parameters work well for all Windows NT operations.

The Parameters subkey for RemoteAccess has the following Registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters.
```

AuthenticateRetries **REG_DWORD** *0 to 10*

Sets the maximum number of unsuccessful retries that are allowed if the initial attempt at authentication fails.

Default: 2.

AuthenticateTime **REG_DWORD** *20–600 seconds*

Sets the maximum time limit, in seconds, within which a user must be successfully authenticated. If the client does not complete the authentication process within this time, the user is disconnected.

Default: 120 seconds.

AutoDisconnect **REG_DWORD** *0–1000 minutes*

Sets the time interval after which inactive connections are terminated. Inactivity is measured by lack of NetBIOS session data transfer, such as copying files, accessing network resources, and sending and receiving electronic mail. You might want to set this parameter to 0 minutes if clients are running NetBIOS datagram applications. Setting this parameter to 0 turns off **AutoDisconnect**.

Default: 20 minutes.

CallbackTime **REG_DWORD** *2–12 seconds*

Sets the time interval that the server waits before calling the client back when the Callback feature has been set. Each client communicates the value of its own callback time when connecting to a Remote Access server. This value can be found in the Modem.inf file for the client. If this value is not communicated (that is, if the client does not communicate a value for the callback time, as with Remote Access version 1.0 and 1.1 clients), then the value of the **CallbackTime** parameter becomes the default.

Default: 2 seconds.

EnableAudit **REG_DWORD** *0–1*

Determines whether Remote Access auditing is turned on or off. If this feature is enabled, all audits are recorded in the Windows NT event log. You can see these audits in the Windows NT Event Viewer.

Default: 1 (enabled).

NetbiosGatewayEnabled **REG_DWORD** *0–1*

Makes the server function like a NetBIOS gateway, allowing clients to access the LAN. If disabled, remote clients can access only the resources on the Remote Access server in a point-to-point connection; dial-in users cannot see the network or access network resources. This parameter should never be modified directly. Use RAS Setup to modify this parameter because RAS Setup also modifies bindings when changing this parameter.

Default: 1 (enabled).

NetbiosGateway Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parame
ters\NetbiosGateway
```

DisableMcastFwdWhenSessionTraffic **REG_DWORD** *0–1*

Allows NetBIOS session traffic (for example, Windows NT–based applications) to take priority over multicast datagrams (such as server messages). In other words, multicast datagrams are transferred only when there is no session traffic. Unless you're using an application that depends on multicast datagrams, leave this parameter enabled.

Default: 1 (enabled).

EnableBroadcast **REG_DWORD** *0–1*

Determines whether broadcast datagrams are forwarded to remote computers. Broadcast datagrams are not often useful and take up too much bandwidth on a slow link. Unless you're using an application that relies on broadcast datagrams, leave this parameter disabled.

Default: 0 (disabled).

See also **MultiCastForwardRate**.

EnableNetbiosSessionsAuditing **REG_DWORD** *0–1*

Turns on and off Remote Access auditing of the establishment of NetBIOS sessions between the remote clients and the Windows NT servers. Turning this parameter on helps the administrator track the NetBIOS resources accessed on the LAN.

Default: 0 (disabled).

MaxBcastDgBuffered **REG_DWORD** *16–255*

Sets the number of broadcast datagrams that the gateway buffers for a client. If you're using an application that communicates extensively through multicast or broadcast datagrams, then increase this parameter so that the Remote Access server can deliver all datagrams reliably.

Default: 32.

MaxDgBufferedPerGroupName **REG_DWORD** *1–255*

Sets the number of datagrams that can be buffered per group name. Increasing this value buffers more datagrams per group name but also takes up more virtual memory.

Default: 10.

MaxDynMem **REG_DWORD** *131072– 4294967295*

Sets the amount of virtual memory used to buffer NetBIOS session data for each remote client.

Note Because the Remote Access server is a gateway between the slow line and the LAN, data is stored (buffered) in its memory when coming from the fast line (LAN) before it is forwarded to the slow line (asynchronous line).

The Remote Access server minimizes the usage of the system's physical memory by locking only a minimal set of pages (about 64K per client) and making use of virtual memory (up to **MaxDynMem**) to buffer the rest of the data.

So, as long as you have space on your hard disk to expand Pagefile.sys, you can increase this parameter if needed.

You might have problems if you have an application with a LAN (fast) sender and an asynchronous (slow) receiver, and if the sender is sending more data than the Remote Access server can buffer in **MaxDynMem**. The Remote Access server tries to apply a form of NetBIOS level flow control by not submitting Ncb.receive on the session until it has enough buffer space to get incoming data.

For this reason, if you have such an application, you should increase your NetBIOS SEND/RECEIVE time-outs on the application server so that it waits for all data to be transmitted over the slow link to the remote client.

Default: 655350.

MaxNames **REG_DWORD** *1–255*

Sets the number of unique NetBIOS names each client can have, with a limit of 255 names for all clients together.

Note Remote clients running Windows NT and Windows for Workgroups might need as many as seven or eight names each. To accommodate these computers, make sure **MaxNames** is set to 8 or greater. If you have Windows NT or Windows for Workgroups clients dialing in to servers running Remote Access version 1.1 or earlier, set this parameter to 8 or greater.

Default: 255.

MaxSessions **REG_DWORD** *1–255*

Sets the maximum number of simultaneous NetBIOS sessions each client can have, with a limit of 255 sessions for all clients together. If you have multiple clients connecting simultaneously with each running 4 or 5 sessions, decrease the value of this parameter so that the total number of sessions does not exceed 255.

Default: 255.

MultiCastForwardRate REG_DWORD *–1 (disabled), 0–32,767 seconds*

Governs the multicasting of group name datagrams to all remote computers. This parameter filters datagrams sent on group names by forwarding them at a time interval specified by the parameter.

Default: 5.

The value –1 disables forwarding. The value 0 guarantees delivery of group name datagrams. The value *n* forwards datagrams every *n* seconds, where $1 \leq n \leq 32,767$.

If the **EnableBroadcast** parameter is set to 0, then broadcasts are not forwarded even if the **MultiCastForwardRate** parameter is set to a positive number (in this case, only multicast datagrams are forwarded). If **MultiCastForwardRate** is set to -1, broadcasts are still not forwarded even if **EnableBroadcast** is set to 1. See also **EnableBroadcast**.

To save bandwidth for session traffic, you should filter the datagrams. However, if you have an application based on multicast datagrams, set this parameter to 0. Setting it to 0 guarantees delivery of all datagrams sent on group names from the LAN to the remote client.

NumRecvQueryIndications **REG_DWORD** *1-32*

Allows a Remote Access client to initiate multiple network connections simultaneously. If a remote client is running a NetBIOS application that does multiple NCB.CALL commands simultaneously, increase this parameter to improve performance.

Default: 3.

RcvDgSubmittedPerGroupName **REG_DWORD** *1–32*

Determines the number of NetBIOS commands of the type Receive Datagram that can be submitted simultaneously per group name on the LAN stack. Keep this setting as small as possible to minimize the amount of memory consumed by system resources. Each datagram command received locks about 1.5K of physical memory in the system.

Default: 3.

RemoteListen **REG_DWORD** *0–2*

Sets the level of access that a LAN client has to a remote client's resources. This is done by posting NCB.LISTEN commands on the NetBIOS names of the client.

Setting	Meaning	Remark
0	Allows no access.	Because every remote listen posted consumes one session, setting this parameter to 0 saves sessions.
1	Makes the Server and Messenger services available on the client.	A remote client running the Server service can make its resources (such as disks and printers) available to LAN users. A remote client running the Messenger service can receive messages from LAN users, printers, and so on.
2	Enables NCB.LISTEN for all remote client NetBIOS names.	This setting allows any NetBIOS application running on a client to answer NCB.CALL commands issued by LAN applications.

Note It is best to leave the **RemoteListen** parameter set to the default, 1 (messages).

Allowing NCB.LISTEN capability on remote clients can significantly drain system resources and therefore is not recommended. If the **RemoteListen** parameter is configured to 2, Remote Access posts an NCB.LISTEN on all NetBIOS names of Remote Access clients. Considering that the average Windows NT client has about 7 or 8 NetBIOS names assigned to it, the total number of NetBIOS names for which an NCB.LISTEN would be posted is 7 or 8 * 256 (the maximum number of clients per Remote Access server).

Default: 1 (messages).

SizWorkBufs **REG_DWORD** *1024–65536*

Sets the size of work buffers. The default setting is optimized for the server message block (SMB) protocol, the protocol between the client and the server running Windows NT Server.

Default: 4500.

IP Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess
\Parameters\IP
```

WINSNameServer **REG_SZ** *IP Address*

Change this parameter in a RAS server's Registry to override the automatic assignment of the RAS server's WINS server to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

WINSNameServerBackup **REG_SZ** *IP Address*

Add this parameter to a RAS server's Registry to override the automatic assignment of the RAS server's backup WINS server to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

WIDNSNameServers **REG_MULTI_SZ** *IP Addresses*

Add this parameter to a RAS server's Registry to override the automatic assignment of the RAS server's DNS servers to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

AsyncMac Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\AsyncMacn\Parameters
```

MaxFrameSize **REG_DWORD** *576–1514*

Determines the maximum frame size. Use smaller frames for noisy links. A lower setting sends less data per frame, slowing performance. Do not change this parameter for previous versions of the Remote Access Service. The value is negotiated between the server and Windows NT clients.

Default: 1514.

TimeoutBase **REG_DWORD** *500–1000*

Determines the amount of time that elapses on a NetBIOS gateway before a connection is disconnected. If you are experiencing an abnormal number of time-out errors using the NetBIOS gateway (more than 10 time-outs per 100 kilobytes received), increase the **TimeoutBase** value from 500 to 1000 if your computer has a security device or your computer's modems have hardware compression or error control enabled.

With **TimeoutBase** increased to 1000, network functionality may on very rare occasions act abnormally. For example, you might have to type network commands more than once, or functionality may periodically slow down.

Default: 500.

NdisWan Parameter

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\NdisWan\Parameters
```

NetworkAddress="*xxxxxx*" **REG_SZ** *Network address*

Add this parameter to reassign the first 4 bytes of the 6-byte IEEE address. For example, if you reset the address to "03-1F-2C-81-92-34", only the first 4 bytes are looked at. The last 2 bytes are reserved to uniquely identify the port. Reset this parameter in the **NdisWan\Parameters** key with the datatype REG_SZ.

NwlnkRip Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NwlnkRip\Parameters
```

NetbiosRouting **REG_DWORD**

Range: 0, 2, 4, or 6

Controls the forwarding of IPX NetBIOS broadcast packets to and from the LAN. The RAS server can forward NetBIOS broadcast packets (IPX type-20) between RAS clients and the local network.

Set to 2, this parameter enables forwarding of NetBIOS broadcast packets from the remote client to the LAN.

Set to 4, this parameter enables forwarding of NetBIOS broadcast packets from the LAN to the remote client.

Set to 6, this parameter enables two-way forwarding of NetBIOS packets between remote clients and the LAN.

You may also need to set the **DisableDialinNetbios** registry entry, depending on your IPX NetBIOS application configuration. See the "NwlnkIpx Parameters" section for more information.

Default: 2.

RasMan Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
```

Logging **REG_DWORD** *0–1*

Sets logging of all communication from serial ports to the device connected to them during command mode. This parameter is useful for solving problems with serial devices and for testing new entries added to the Modem.inf or Pad.inf files.

Because some of the information will not be printable characters, you might want to view the Device.log file in a text editor that can display both character and hexadecimal output. Also, Device.log contains a carriage return and line feed at the end of each line. These bytes are provided by the program that creates the Device.log file and do not represent information communicated from or to the device.

Set to 1, communication from the serial port to the device connected to it will be logged in the file *systemroot*\system32\ras\device.log.

Logging is suspended after successful connection to the remote device and transmission of data. Logging resumes when a new connection is established and is appended to Device.log until the file size exceeds approximately 100K. Device.log is then cleared and logging resumes. Device.log is also cleared when any RAS component is started after all RAS components have been stopped.

Default: 0.

PPP Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP
```

MaxTerminate **REG_DWORD** *0–unlimited*

Sets the number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond.

Default: 2.

MaxConfigure **REG_DWORD** *0–unlimited*

Sets the number of Configure-Request packets sent without receiving a valid Configure-Ack, Configure-Nak, or Configure-Reject before assuming that the peer is unable to respond.

Default: 10.

MaxFailure **REG_DWORD** *0–unlimited*

Sets the number of Configure-Nak packets sent without sending a Configure-Ack before assuming that the configuration is not converging.

Default: 10.

MaxReject **REG_DWORD** *0–unlimited*

Sets the number of Config-Rejects sent before assuming that the PPP negotiation will not converge.

Default: 5.

RestartTimer **REG_DWORD** *0–unlimited*

Sets the time (in seconds) available for transmission of Configure-Request and Terminate-Request packets. Expiration of the Restart timer causes a time-out event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.

Default: 3.

NegotiateTime **REG_DWORD** *0–unlimited*

Sets the amount of time allowed (in seconds) for PPP negotiation to converge successfully before disconnecting the line. 0 means that the line will never be hung up.

Default: 150.

ForceEncryptedPassword **REG_DWORD** *0–1*

Used on RAS servers only. Sets the use of the Crypto-Handshake Authentication Protocol (CHAP) while authenticating clients. Set to 1, the server will use CHAP during authentication. Set to 0, the server will negotiate PAP.

Default: 1.

Logging **REG_DWORD** *0–1*

Sets logging of PPP events. Set to 1, all PPP events will be logged in the file *systemroot*\system32\ras\ppp.log. This parameter is useful for solving problems with PPP connections.

Default: 0.

DisableSoftwareCompression **REG_DWORD** *0–1*

Enables or disables software compression. Set to 1, software compression is disabled. Set to 0, software compression is enabled.

Default: 0.

PPP Subkeys

The following entries are subkeys to the PPP key:

CBCP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Callback Control Protocol (CBCP) DLL. CBCP negotiates callback information with the remote client. Always present.

CHAP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Crypto-Handshake Authentication Protocol (CHAP) DLL. Always present.

COMPCP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Compression Control Protocol (CCP) DLL. CCP negotiates compression with the remote client. Always present.

IPCP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Internet Protocol Control Protocol (IPCP) DLL. Present if RAS is configured to use TCP/IP and TCP/IP is installed.

These parameters can be added to the **IPCP** subkey:

AcceptVJCompression **REG_DWORD**

Range: *0 - 1*

Add this parameter to prevent IPCP from accepting IPCP standard option 0x02, Van Jacobson header compression. If this parameter has not been added or is set to 1, RAS clients will accept VJ compression.

Default: not in registry

PriorityBasedOnSubNetwork **REG_DWORD**

Range: *0-1*

A computer can connect to the LAN using a network card and a RAS connection. If the RAS connection and the LAN network adapter card are assigned addresses with the same network number and the **Use Default Gateway On Remote Network** checkbox is selected, then all packets will be sent over the RAS connection, though the two addresses are in different subnetworks within the same network.

Set this parameter to 1 to send packets over the network card.

For example, if the network adapter card has IP address 10.1.1.1 (subnet mask 255.255.0.0) and the RAS connection is assigned the address 10.2.1.1, RAS will send all 10.x.x.x packets using the RAS connection. If the parameter is set, RAS will send 10.2.x.x packets using the RAS connection and 10.1.x.x packets using the network adapter card.

Default: not in registry

RequestNameServerAddresses **REG_DWORD**

Range: *0-1*

Add this parameter on RAS clients to prevent IPCP from requesting the Microsoft extension options for WINS and DNS server address negotiation, i.e. IPCP options 0x81, 0x82, 0x83, 0x84. If this parameter has not been added or is set to 1, the client-side will request the addresses.

Default: not in registry

RequestVJCompression **REG_DWORD**

Range: *0-1*

Add this parameter on RAS clients to prevent IPCP from requesting IPCP standard option 0x02, Van Jacobson header compression. If this parameter has not been added or is set to 1, RAS clients will request VJ compression.

Default: not in registry

IPXCP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Internetwork Packet Exchange Control Protocol (IPXCP) DLL. Present if RAS is configured to use IPX and the Client Service for NetWare or Gateway Service for NetWare is installed.

NBFCP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the NetBEUI Framing Control Protocol (NBFCP) DLL. Present if RAS is configured to use NetBEUI and NetBEUI is installed.

PAP **REG_EXPAND_SZ** *DLL Path*

Specifies the location of the Password Authentication Protocol (PAP) DLL. Always present.

Rdr Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters
```

RawIoTimeLimit **REG_DWORD** *see below*

This parameter applies only to configurations using the NetBIOS gateway.

Sets the redirector to send data in 64 kilobyte blocks. When **RawIoTimeLimit** turned on, throughput increases by 10-15 percent. All other simultaneous data transfers are blocked when communicating at this speed.

This parameter is turned off for slow links and on for faster links, by default. For example, if you are communicating at 14,400 bps or slower, this feature is turned off. If you are communicating at faster speeds, such as through an ISDN line, this feature is turned on.

The following list shows what values turn raw I/O on and off for ISDN connections:

RawIoTimeLimit set to 9:
Raw I/O is enabled when connected through one 64K channel. Raw I/O is enabled when connected through two 64K channels.

RawIoTimeLimit set to 5 (default):
Raw I/O is disabled when connected through one 64K channel. Raw I/O is enabled when connected through two 64K channels.

RawIoTimeLimit set to 0:
Raw I/O is disabled when connected through one 64K channel.Raw I/O is disabled when connected through two 64K channels.

RasArp Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasArp\Parameters
```

FilterBroadcasts **REG_DWORD**
Range: *0 - 1*

Add this parameter to cause RAS to transmit broadcast packets (for example, destination IP address 255.255.255.255) and subnet multicasts (for example, destination IP address 11.101.255.255). Set this parameter to 0 on clients if the computer is calling into third-party remote access routers that support broadcast/multicast forwarding. (Windows NT Remote Access servers do not forward broadcasts or multicasts.)

Default: 1.

Nbf Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nbf\Parameters
```

InitUIFrames **REG_DWORD**
Range: 0 - unlimited

Add this parameter to set the number of NetBIOS names that can be added to the network simultaneously from a RAS client.

Default: 5.

NwlnkIpx Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NwlnkIpx\Parameters
```

DisableDialinNetbios REG_DWORD

Range: *0 - 3*

Controls the forwarding of IPX type 20 packets between the remote RAS client, the LAN (by means of the RAS IPX router) and the RAS server running an IPX NetBIOS application (internal net). This parameter controls only dial-in lines on RAS servers.

Set to 0, IPX type 20 packets will broadcast from the RAS server to remote clients and from the remote clients to the RAS server then through the IPX router for broadcast on the LAN (if the router is configured to forward IPX NetBIOS packets.

Set to 1 (default), IPX type 20 packets will broadcast only from remote clients to the internal net and to the RAS IPX router. This setting disables broadcasts from the internal net to the remote clients.

Set to 2, IPX type 20 packets will broadcast from the internal net to the remote clients.

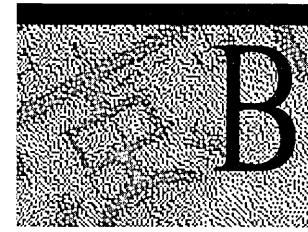
Set to 3, all IPX type 20 broadcasts are disabled.

You might also need to set the **NetbiosRouting** registry entry, depending on your IPX NetBIOS application configuration. See the "NwlnkRip Parameters"section for more information.

Default: 1.

APPENDIX B

RAS Cabling



Most ISA and EISA computers have one of the following serial port connectors:

- 25-pin male "D-shell" connectors
- 9-pin male connectors

Most—but not all—off-the-shelf cables will work with your modems. Some cables do not have all the pins connected as shown in the following tables. When purchasing cables, tell your dealer exactly what you need, and provide the information in these tables to be sure you have the correct match.

Note Do not use the 9-to-25-pin converters that come with most mouse hardware, because some of them do not carry modem signals.

25-Pin Cabling

As Table B.1 shows, pins 1 through 8 on the serial port connector are wired to their counterparts on the modem connector. Ribbon cables usually have all 25 pins wired straight across, but they can cause interference to TVs, radios, and VCRs. To prevent this problem, use shielded RS-232 cable.

Table B.1 25-Pin Cable Wiring

25-pin serial port connector	25-pin modem connector	Signal
1	1	Ground
2	2	Transmit Data
3	3	Receive Data
4	4	Request to Send

(continued)

Table B.2 25-Pin Cable Wiring

25-pin serial port connector	25-pin modem connector	Signal
5	5	Clear to Send
6	6	Data Set Ready
7	7	Signal Ground
8	8	Carrier Detect
20	20	Data Terminal Ready

9-Pin Cabling

The following table shows how to connect a 9-pin serial port connector on a computer to a 25-pin connector on a modem. Again, if you buy an off-the-shelf cable, be sure all pins are connected as shown in Table B.2.

Table B.2 9-Pin Cable Wiring

9-pin serial port connector	25-pin modem connector	Signal
1	8	Carrier Detect
2	3	Receive Data
3	2	Transmit Data
4	20	Data Terminal Ready
5	7	Signal Ground
6	6	Data Set Ready
7	4	Request to Send
8	5	Clear to Send
9	22	Ring Indicator (optional)

Note Some modems have the Data Set Ready (DSR) signal physically tied to the Data Carrier Detect (DCD) signal. Some 1200-bps modems and other 2400-bps modems have dip switches default to this setting as well. As a result, if such a modem loses power while listening for a call, the Remote Access server cannot detect the condition because the DSR will not change as it does with other modems.

Serial Cabling Requirements

The remote Access Service requires the following pins on the RS-232 cable:

Rx	Receive
Tx	Transmit
CTS	Clear To Send
RTS	Ready To Send
DTR	Data Terminal Ready
DSR	Data Set Ready
DCD	Data Carrier Detected

Caution All the pins listed above must be present. The Remote Access Service does not work if any of the seven pins is missing. If any pins are not present and working, the Remote Access Service reports a hardware error.

Null Modem Cabling

If you are using a null modem to make a direct serial connection between two computers, your cable must be wired as shown in tables B.3 and B.4.

Table B.3 9-Pin Null Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
3	2	Transmit Data
2	3	Receive Data
7	8	Request to Send
8	7	Clear to Send
6, 1	4	Data Set Ready and Carrier Detect
5	5	Signal Ground
4	6, 1	Data Terminal Ready

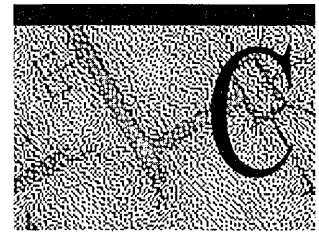
Table B.4 25-Pin Null Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
2	3	Transmit Data
3	2	Receive Data
4	5	Request to Send
5	4	Clear to Send
6, 8	20	Data Set Ready and Carrier Detect
7	7	Signal Ground
20	6, 8	Data Terminal Ready

Off-the-shelf null modem cables might be improperly wired. Be sure to tell your dealer that your null modem cables must be wired as shown in Table B.4.

APPENDIX C

Understanding Modem.inf



RAS now supports modems through the Universal Modem Driver (Unimodem) and continues to support modems described in this chapter for older legacy systems. To configure a previously installed unsupported modem to work with the Remote Access Service, add an entry for that modem in the Modem.inf file.

For more information on Unimodem, see the files Mdk.doc and Reg.doc at the following location: ftp://ftp.microsoft.com/developr/drg/modem/modemdev.exe.

Modemdev.exe is a self-extracting compressed file. Run it to obtain Mdk.doc and Reg.doc.

Note The files are Windows 95 documents that are also relevant to Windows NT except for the following areas:

- Plug and Play (PnP)
- Voice INF structures
- VoiceView support
- Parallel port modems

The Modem.inf File

The Modem.inf file lists all modems supported by Remote Access, along with the command and response strings each modem needs for correct operation. When you select a modem during Remote Access installation, the Setup program associates the selected modem with the specified communication port. Remote Access connection utilities read Modem.inf to obtain the command strings for the modem associated with each communication port. You can find Modem.inf in the *\systemroot*\system32\ras directory.

The Modem.inf file consists of two main parts:

- A global [Responses] section
- Individual sections for each supported modem, such as [Hayes V 9600]

Each section contains the following four components. The first three must appear in the order given. Comment lines can appear anywhere.

Component	Quantity
Section header	Only one
Configuration parameters and substitution macros	Zero or more
Commands	One or more
Comment lines	Zero or more

Responses

A *command-response set* consists of one command followed by zero or more *responses*. Responses are strings expected from the device; they can contain macros. Responses take the following form:

keyword=value_string

The Modem.inf file contains two types of responses:

Type of response	Location
Global	In the [Responses] section
Private	Immediately following the command line that is expected to produce the response, and before the next command line

A modem can match any response. If the modem returns only carrier bps, put the expected responses in the private modem section; if the modem returns connect bps or both carrier bps and connect bps, put the expected responses in the global section. To find out which bps string(s) your modem returns, see the modem documentation.

Global Responses

Responses used by most modems are in the global [Responses] section of Modem.inf. For example:

```
[Responses]
    LOOP=<cr><lf>RING<cr><lf>
    CONNECT_V42=<cr><lf>CONNECT <connectbps> RELIABLE  EC=(LAPM) \
    DC=(None)<cr><lf>
    ERROR=<cr><lf>ERROR<cr><lf>
```

The only information contained by LOOP is that another response is coming. Remote Access then waits for that response before moving on. Any response keyword beginning with LOOP or LOOP_ acts this way.

Private Responses

Specific Modem.inf sections can contain private response strings. Remote Access checks for private responses first. If it doesn't find a response string to match the actual string returned by the modem, it continues checking in the global response section. There is one exception: If the first part of a string containing an <append> macro is matched in the private section, the global section will not be searched. Instead, Remote Access waits a few seconds for the rest of the string to arrive from the modem.

For information about adding an entry to Modem.inf, see "Adding a New Modem to Modem.inf," in this appendix.

The following example shows a section with private responses. Microsoft encourages you to use this method of inserting responses for any section you add.

```
COMMAND_LISTEN=ATS0=1<cr>
CONNECT=<cr><lf>CONNECT <carrierbps><cr><lf>
CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP<cr><lf>
CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP/COMPRESSED<cr><lf>
CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP COMPRESSED<cr><lf>
CONNECT_EC=<cr><lf>CONNECT <carrierbps>/V42<cr><lf>
CONNECT_EC=<cr><lf>CONNECT <carrierbps>/V42BIS<cr><lf>
```

Syntax

Modem.inf file syntax consists of two components: *section headers* and *configuration parameters*.

Section Headers

A *section header* is a string of up to 32 characters between square brackets, and it occupies the first line in each section. It identifies the specific device to which the section applies. In Modem.inf, the section header typically lists the modem make and model. For example, [Hayes V 9600].

Configuration Parameters

Remote Access works with the modem through configuration parameters, which take the following form:

parameter_name=value_string

For example:

```
MAXCARRIERBPS=9600
CALLBACKTIME=8
```

Substitution Macros

Substitution macros are placeholders that are replaced in command strings. Macros follow these rules:

- In the Modem.inf file, macros must come before the first command and, by convention, after the configuration parameters.
- Macro names must be enclosed in angle brackets (< >).

For example:

```
<reset>=&F
<speaker_on>=M1
<speaker_off>=M0
```

There are two types of macros:

Macro Type	Form
Unary	*<macro_name>=value_string*
Binary	*<macro_name_ON>=value_string*
	<macro_name_OFF>=value_string

The command AT<reset><cr> would be sent as AT&F<cr>. Binary macro placeholders are replaced according to instructions from the user. For example, if the user disables the speaker, the command AT<speaker><cr> is sent as ATM0<cr>. If the user enables the speaker, it is sent as ATM1<cr>.

Some responses can also use macros. Most macros in response strings behave as they do in commands. However, certain macros (such as <carrierbps> and <diagnostics>) capture information such as baud rate from the device response string.

Nested macros are not allowed. Two adjacent left angle brackets are interpreted as a less than sign, and two adjacent right angle brackets are interpreted as a greater than sign. This allows greater than and less than symbols to be used in a command string when required.

The macros in the following list are *reserved words*: You cannot define them in Modem.inf when creating a new macro. Reserved words are case insensitive.

- **carrierbps**
- **connectbps**
- **message**
- **phonenumber**
- **cr**
- **lf**
- **match**
- **?**
- **append**
- **hXX**
- **ignore**

Caution These macros are defined internally and can be used in Modem.inf, just as **phonenumber** is used in the COMMAND_DIAL= string.

For additional reserved words, see "PAD.INF Format," in Chapter 9, "X.25 PAD Support."

Table C.1 lists macros defined in the file's Modem.inf. Always enclose these macros in angle brackets (< >).

Table C .1 Macros Defined in Modem.inf

Macro	Function
speaker	Turns the modem speaker on or off.
protocol	Turns the error correction protocol on or off.
compression	Turns modem compression on or off.
hwflowcontrol	Tells the modem whether to use hardware flow control between the COM port and modem.
cr	Inserts a carriage return.
lf	Inserts a line feed.

(continued)

Table C .1 Macros Defined in Modem.inf

Macro	Function
match	Reports a match if the string enclosed in quotation marks is found in the device response. For example, <match>"Smith" matches Jane Smith and John Smith III.
?	Inserts a wildcard character, for example, CO<?><?>2 matches COOL2 or COAT2, but not COOL3.
append	Causes information to be broken into two segments and received from the modem one segment at a time. The client expects delays between the segments and waits until all the information has arrived. See the sample Modem.inf file for an example.
hXX (XX are hexadecimal digits)	Allows any hexadecimal character to appear in a string including the zero byte, <h00>.
ignore	Ignores the rest of a response from the macro on. For example, <cr><lf>CONNECTV-<ignore> reads the following responses as the same: "crlfCONNECTV-1.1" and "crlfCONNECTV-2.3."

In Table C.1, the first four macros (**speaker**, **protocol**, **compression**, and **hwflowcontrol**) are binary macros. Define them, using the **speaker** example (first example in this section) as a model.

As values, use them as shown in the following example:

```
COMMAND_INIT=AT<speaker><cr>
```

This command sends ATM1<cr> to the modem if the speaker is to be turned on and ATM0<cr> if the speaker is to be turned off. Through the Remote Access Phone Book, the user determines which macros are to be on or off. The Phone Book then reads the Modem.inf file to find out which value string to send to the modem. Note that value strings sometimes differ among modems.

The Remote Access Service uses the last five macros in the Table C.1 (**match**, **?**, **append**, **hXX**, and **ignore**) in response strings to recognize responses from a modem or another device.

Commands

Commands are strings of characters sent to the modem. These strings can contain macros and take the following form:

command_keyword=value_string

The set of command keywords (or *types*) is as follows:

- **COMMAND_INIT**
- **COMMAND_DIAL**
- **COMMAND_LISTEN**

The Modem.inf file initializes the modem, dials a phone number, and puts the modem into answer mode with the command types **COMMAND_INIT**, **COMMAND_DIAL**, and **COMMAND_LISTEN**. Commands of a given type are executed in the order found in the Modem.inf file. By convention, commands of the same type are grouped together, as shown in the following example from Modem.inf:

```
COMMAND_INIT=AT&F&C1&D2 V1 S0=0 S2=128 S7=55 W0 S95=44<cr>
COMMAND_INIT=AT<speaker><protocol><compression><hwflowcontrol><cr>
COMMAND_LISTEN=ATS0=1<cr>
COMMAND_DIAL=ATDT<phonenumber><cr>
```

Multiple Command Strings

Because most modems accept strings of about 50 characters, the Remote Access Service supports multiple command strings. This allows you to break up long commands into strings the modem can accept.

For example, the first line could be rewritten as a multiple command string:

```
COMMAND_INIT=AT&F&C1&D2 V1 S0=0 S2=128 S7=55 W0 \
    S95=44<speaker><protocol><compression><hwflowcontrol><cr>

COMMAND_INIT=AT&F&C1&D2 V1 S0=0 S2=128 S7=55 W0 S95=44<cr>
COMMAND_INIT=AT<speaker><protocol><compression><hwflowcontrol><cr>
```

Notice that each string

- Is a command in its own right
- Begins with AT and ends with a carriage return (<cr>)
- Gets a response before going to the next string

Comment Lines

Comment lines convey important information to those who maintain the .INF files. Comment lines begin with a semicolon (;), and can appear anywhere in the file. For example:

```
; Explanation of modem commands
; &F Reset modem to factory default settings
; &C1 DCD tracks presence of modem carrier
; &D2 Hangup & disable autoanswer when DTR goes from ON TO OFF
```

Line Continuation

A backslash (\) indicates that commands or responses are continued on the next line. Line continuations can make files more legible. A double backslash (\\) denotes a backslash.

For example:

```
CONNECT_EC=\
<cr><lf>CARRIER <carrierbps><cr><lf><append>\
<cr><lf>PROTOCOL: V.42/LAPM<cr><lf>\
<cr><lf>COMPRESSION: NONE<cr><lf>\
<cr><lf>CONNECT <connectbps><cr><lf>

<protocol_on>=K0
<protocol_off>=K1
```

Assigning an Alias

If a modem's command strings are identical to those already listed for another modem, the name of the latter modem can be used as an alias for the former.

For example:

```
[QT Modem]
ALIAS=Codex 326X Fast
```

In this example, the QT modem uses command strings of a Codex 326X Fast modem.

An alias to an alias is not allowed. In other words, you cannot nest aliases. For example, to alias two modems to another modem, you must alias them directly:

```
[Modem 1]
;Modem 1's normal entries go here
[Modem 2]
ALIAS=Modem 1
[Modem 3]
ALIAS=Modem 1
;You cannot say ALIAS=Modem 2
```

Adding Modem Detection Information to Modem.inf

The command and response that enable Remote Access Setup to automatically detect modems are

- DETECT_STRING
- DETECT_RESPONSE

Insert the appropriate modem identification command after the DETECT_STRING parameter, followed by <cr>. Then insert the response expected from the modem after the DETECT_RESPONSE parameter. For example:

```
[DataRace RediModem V.32bis]; Command sent is ATI3<cr>, and the response
is ; "PC Half-Card V.32bis/V.42bis/Fax". Actually, the modem; might
return more than just the string in quotation marks,; but all that is
needed to make a positive identification is; the information in
quotation marks.
DETECT_STRING=ATI3<cr>DETECT_RESPONSE=PC Half-Card V.32bis/V.42bis/Fax
```

If several possible responses might be returned for a specific modem, then for each DETECT_STRING command, list all possible combinations of responses. For example, the following section enables Setup to detect the [Datatrek 2424AMH] modem. Setup sends the ATI9 command and expects any one of the four possible responses to be returned.

```
DETECT_STRING=ATI9<cr>DETECT_RESPONSE=C3DETECT_RESPONSE=C2DETECT_RESPONS
E=3.DETECT_RESPONSE=2.
```

If multiple commands are required to make a positive identification, list all the required commands and their corresponding responses. For example, the following section enables Setup to detect the [Intel 9600EX] modem. Setup expects specific responses for both the ATI0 and ATI3 commands in order to make a unique identification.

```
DETECT_STRING=ATI0<cr>DETECT_RESPONSE=969DETECT_STRING=ATI3<cr>DETECT_RE
SPONSE=U21
```

Adding a New Modem to Modem.inf

If you use a modem that is not explicitly supported in Modem.inf, you can append a new section containing the command strings the modem requires. The name of the section should be the name of your modem and should be enclosed in brackets. For information about macros used in building a new section, see "Substitution Macros," in this appendix.

Note To minimize the risk of corrupting existing modem sections, be sure to add new sections to the *end* of the Modem.inf file.

▶ To edit Modem.inf for a new modem

1. Back up your existing Modem.inf file.
2. Copy an existing section to the end of Modem.inf and rename the section header of the copy to the name of your modem. For information about section headers, see "Section Headers," in this appendix.
3. Change **MAXCONNECTBPS** and **MAXCARRIERBPS** to the values of the new modem, and set values for **CALLBACKTIME** and **DEFAULTOFF**. For example:

```
MAXCARRIERBPS=9600
MAXCONNECTBPS=19200
CALLBACKTIME=10
DEFAULTOFF=speaker compression
```

Configuration parameter	Description
MAXCARRIERBPS	The maximum speed at which the client's modem and the Remote Access server's modem exchange data (bps rate on the telephone line). This speed is always equal to or less than **MAXCONNECTBPS**.
MAXCONNECTBPS	The maximum speed at which a modem talks to the computer (DTE to DCE bps transfer rate). Set this value to the maximum serial port bps that the modem can support.
CALLBACKTIME	The time in seconds that the server waits before calling the client back. This delay allows the client's modem to reset itself. Start with 10 seconds, and increase this number if there are problems.
DEFAULTOFF	A list of all the on/off macros that you want set to off by default, until turned on by Rasphone.exe.

4. Change the command strings for **hwflowcontrol**, **protocol** (error control), **compression**, and **speaker**. Check your modem's documentation for the correct values.

   For example:

```
<hwflowcontrol_off>=&K0
<hwflowcontrol_on>=&K3
<protocol_off>=&Q0 S36=1
<protocol_on>=&Q5 S36=5 S46=138
<compression_off>=*DC0
<compression_on>=*DC1
<speaker_on>=M1
<speaker_off>=M0
```

Note If you don't find values for these commands in your modem's documentation, contact the modem manufacturer. If a modem does not support these features, omit these macros from Modem.inf. (If you omit a macro definition in step 4, be sure to also omit the same macro in the COMMAND_INIT string in step 5.)

5. And finally, change the commands in the following example. Again, check your modem's documentation for the correct values.

```
COMMAND_INIT=AT&F&C1&D2 v1 s0=0 s2=128 s7=55 w1<cr>
COMMAND_INIT=AT<hwflowcontrol><protocol><compression><speaker><cr>
COMMAND_LISTEN=ATS0=1<cr>
COMMAND_DIAL=ATDT<phonenumber><cr>
```

Command	Description
COMMAND_INIT	Initializes the modem.
COMMAND_LISTEN	Sets the modem to autoanswer mode. Check your modem's documentation for the value that makes the modem answer after the first ring. Insert this value for Remote Access servers and clients configured for callback.
COMMAND_DIAL	Dials the phone number and connects. Do not enter an actual phone number here. Enter **<phonenumber>**, as shown in the example.

The following table lists the modes to which you should initialize your modem. The codes in the left column show examples of each mode. Codes like these form the **COMMAND_INIT** string. For the codes used by your modem, consult the modem's documentation.

Table C.2 Sample COMMAND_INIT Codes

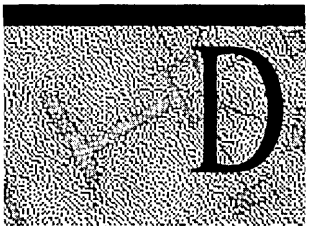
Code	Meaning
&F	Restores factory settings
&C1	Causes data carrier detect (DCD) to track the presence of a data carrier
&D2	Hangs up and disables autoanswer when the data terminal ready (DTR) signal goes from on to off (high to low)
V1	Allows verbose (English words) return codes
L1	Lowers the speaker volume
Q0	Lets the modem return result codes
E1	Enables character echo in the command state
S0	Answers on a certain ring number: S0=0 for **COMMAND_INIT**, S0=1 for **COMMAND_LISTEN**
S2=128	Disables the escape character
S7=55	Sets the carrier waiting time (to about 55 seconds)
W1	Enables negotiation progress messages
S95=44	Allows carrier, protocol, and compression messages

By being meticulous when you create a new modem section, you can reduce the need for debugging later. Microsoft also recommends that you document your work: Doing so allows others to quickly understand the entries and helps you remember your programming rationale. Be sure to type a semicolon (;) at the beginning of each comment line.

Important If you edit Modem.inf and your new modem does not work, restore the original version of the file and use one of the modems listed in the *Hardware Compatibility List.*

APPENDIX D

Services for Macintosh Registry Values



Windows NT Server maintains configuration information in a database called the *Registry*. The database consists of keys and subkeys where values are stored. You can change the values with the Registry Editor, REGEDT32.EXE. (The Registry replaces the .INI files you might have used in previous versions of the Windows environment and LAN Manager.) The Registry and Registry Editor are explained more fully in the Windows NT Server Registry Editor online Help and in the *Windows NT Server Resource Kit.*

When Services for Macintosh (SFM) is set up, additional values are added to the keys and subkeys of the Registry. It's a good idea to retain the default values. (If you must perform repair, refer to this chapter for some values you might need to change.).

Changing Registry Key Values

This section provides a brief description of the process for changing key values.

▷ **To edit the Registry**

For detailed information on how to add a parameter to a key in the Registry, see online Help for the Windows NT Registry editor.

▷ **To change key values**

1. From the **Start** menu, click **Run**.
2. Type **regedt32** and click **OK**.

   This command can also be run from the Command Prompt.
3. In the HKEY_LOCAL_MACHINE window, choose the System directory, and then the CurrentControlSet directory.
4. Choose the Services directory.

5. Choose the directory corresponding to the service you want to change, either AppleTalk or MacFile. (Do not change entries in the MacPrint or MacSrv service.)
6. Look at the corresponding section of this appendix to review the values for that service.
7. When you're ready to make changes, double-click the entry to display the appropriate editor for that data type.

AppleTalk Key Values

To change the key values for the AppleTalk stack, choose AppleTalk in step 5 of the preceding section. Values for AppleTalk Adapter and Parameter subkeys follow. (Linkage values should not be changed and are not described.)

Adapter Key Values

One subkey exists for each AppleTalk-compatible adapter on the computer. The Registry entries for the Elnkii01 adapter are used as an example.

Entry Name	Data Type	Range of Values
AarpRetries:	**REG_DWORD:**	**0xa**

This hexadecimal value specifies the maximum number of AppleTalk address resolution protocol packets to be sent by the AppleTalk Protocol.

The default is 0xa.

DdpCheckSums:	**REG_DWORD:**	**0**

This hexadecimal value tells the AppleTalk Protocol whether or not to compute checksums in the DDP layer. If this entry is 1, the AppleTalk Protocol will use sums in the DDP layer.

The default is 0.

DefaultZone:	**REG_SZ:**	**Not applicable**

This data-string value contains the default zone for this network if this adapter is seeding the network. If the adapter is seeding the network, the default zone is chosen when you configure SFM.

There is no default.

NetworkRangeLowerEnd: **REG_DWORD:** **0x1–0xfeff**
1–65279 (decimal)

This hexadecimal value is the lower network number of the network range if this adapter is seeding the network. If seeding the network, this number is set from the **Services For Macintosh** dialog box.

There is no default.

NetworkRangeUpperEnd: **REG_DWORD** **0x1–0xfeff**
1–65279 (decimal)

This hexadecimal value is the upper network number of the network range for this network if this adapter is seeding the network. If seeding, this number is set from the **Services For Macintosh Configuration** dialog box.

There is no default.

PortName: **REG_SZ:AdapterName@ComputerName**

This data-string value is the name used to identify the AppleTalk Protocol running on a particular adapter on a computer.

There is no default.

SeedingNetwork: **REG_DWORD:** **0–1**

This hexadecimal value is used by the AppleTalk Protocol during startup. If Seeding Network is 0, this adapter is not seeding the network, and the AppleTalk Protocol ignores any seeding information for the adapter, if specified. If SeedingNetwork is 1, the AppleTalk Protocol reads in all seeding information and seeds the network, if valid.

The default is 0.

ZoneList: **REG_MULTI_SZ:** **(List of zones)**

This multistring value is relevant only when the adapter is seeding the network. The network is seeded with this list of zones by the AppleTalk Protocol. To make changes, use the **Services For Macintosh Configuration** dialog box.

There is no default.

Parameter Key Values

Parameter values set port, zone, and router information.

DefaultPort: **REG_SZ:** **Not applicable**

This data-string value is the network on which the SFM service names are registered. If the AppleTalk Protocol is not routing, only Macintosh clients connected to this network can see the file and print services. During initial installation, the default port is automatically set to the first Ethernet adapter found, to the first token-ring adapter, or to a LocalTalk adapter (in that order). To change the default port, use the **AppleTalk Configuration** dialog box.

The default is the first adapter found.

DesiredZone: **REG_SZ:** **Not applicable**

This data-string value is the zone in which SFM is present. If this key is not set, Services for Macintosh is present in the default zone for that network. To set the preferred zone, use the **AppleTalk Configuration** dialog box.

There is no default.

EnableRouter: **REG_DWORD:** **0–1**

This hexadecimal value tells the AppleTalk Protocol if routing needs to be started on this computer. If routing is started, Macintosh clients connected to any of the networks this computer is on should be able to use the File and Print Servers for Macintosh. This value is critical. Unless absolutely essential, do not set this value to 1. The value can be changed when configuring SFM.

The default is 0.

File Server Key Values

The key values for the File Server for Macintosh are specified when you choose MacFile in step 5 of the "Changing Registry Key Values" section, which appears earlier in this appendix. The Parameter keys that can be changed are explained in this section. (Do not change Icon or Extension entries.)

Parameter Key Values

These key values specify server options, which can be set from Server Manager. All others are added when changes to the default values occur.

ServerName **REG_SZ:** **(Server Name)**

This data string value is the name of the computer running Windows NT Server and SFM. Use the Windows NT Server name as the default if you need to add this entry.

There is no default.

ServerOptions **REG_DWORD:** **0x7**

This hexadecimal value specifies server options that are set in Server Manager. If needed for repair purposes, change Bits 1 through 3; do not change the other bits. When on, Bit 1 allows guest logons, Bit 2 allows cleartext passwords, and Bit 3 allows Macintosh users to save passwords on their clients.

The defaults are bits 1, 2, and 3 set to on.

MaxSessions **REG_DWORD:** **1–unlimited**

This hexadecimal value is the maximum number of user sessions that File Server for Macintosh can accommodate.

The default is 0xff 255 (in decimal).

LoginMsg **REG_SZ:** **1–198 characters**

This data-string value specifies the message you want Macintosh users to see when they log on to the Windows NT Server.

There is no default.

PagedMemLimit **REG_DWORD:** **0x3e8—0x3e800**
1000–256000
(decimal)

This hexadecimal value is the maximum amount of page memory that the File Server for Macintosh will use. Performance of the MacFile service increases with an increase in this value. However, the value should not be set lower than 0x3e8, or 1000 kilobytes (K). It is especially important that you are well acquainted with memory issues before changing this resource parameter. You cannot change this value from Server Manager.

The default is 0x4e20 (20000 in decimal).

NonPagedMemLimit **REG_DWORD** **0x100–0x3e80**
256–16000 (decimal)

This hexadecimal value is the maximum amount of RAM that is available to the File Server for Macintosh. Increasing it helps performance of the File Server but decreases performance of other system resources.

The default is 0xfa0 (4000 in decimal).

Volume Key Values

This multistring value specifies information about the Macintosh-accessible volumes on the computer running Windows NT Server. It's recommended that you add Macintosh-accessible volumes from File Manager.

▷ **To change the values for a Macintosh-accessible volume**

1. Double-click on the name of the Macintosh-accessible volume for which you want to change key values.
2. In the Data box, change the values, as described next:

MaxUses
This decimal value is the maximum number of simultaneous clients that can be connected to the File Server for Macintosh. The limit is dictated by hardware and by network media.

Properties
This decimal value (32768) specifies security options. When bit 1 is set to on, the volume is read-only. When bit 16 is set to on, guests can use this volume. The default value (in binary notation) is 1000000000000000. (Guests can use this volume.)

Password
This value contains the encrypted password. Don't change it. If a user forgets his or her password, you can delete this entry, thus removing a password requirement from the user's account. Then the user can specify a new password at logon.

Path
This value is the path of the root directory of the volume. If a volume has been deleted, the path might still be valid; consequently, you should not delete it. If volumes have been deleted from the user interface, you can delete this value.

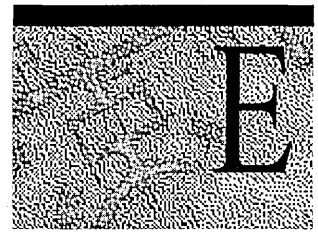
Type-Creators

These values are a list of all Macintosh type-creators to which PC-type extensions are associated. It's best to change these from File Manager, through the **Associate** command on the **MacFile** menu. If you decide to change these entries in the Registry, refer to the following range of values:

- *Creator* must have from 1 through 4 characters.
- *Type* must have from 1 through 4 characters.
- *Description* must have from 0 through 29 characters.

APPENDIX E

How Macintosh Filenames Are Translated



Information in this appendix supplements information provided in Chapter 16, "How Services for Macintosh Works."

Windows NT, Macintosh, and MS-DOS systems each follow different file-naming conventions:

Operating system	File system	Character limit
MS-DOS	FAT	8.3 (8 characters, plus an optional extension, signaled by a period and up to 3 characters)
Macintosh	System software	31 characters
Windows NT	NTFS	256 characters

When a file with a long name (any name over the 8.3 MS-DOS standard) is saved on an NTFS partition, the long name is maintained and a short name is created so that MS-DOS users can gain access to the file if they have permission to do so. For example, Macintosh users who create folders or files on an SFM volume and use the 31-character limit will see the original, long names. MS-DOS users, however, will see a shortened version of the name. Windows NT system users will see the longer Macintosh filenames because NTFS has a 256-character filename limit.

Even though NTFS translates long names to short names, it's a good idea for users to name shared files following the 8.3 convention used by the FAT file system in MS-DOS. This simplifies file identification for users working on different platforms. This appendix explains how file translations work on Windows NT Servers running SFM. For more information, refer to the *Windows NT Server Concepts and Planning Guide.*

Naming Differences

In general, the FAT file naming system, which is used on MS-DOS systems, is more restrictive than the Macintosh system. The two systems differ in the following ways:

- Macintosh filenames and folder names can have as many as 31 characters and include blank spaces. FAT filenames and directory names can have as many as eight characters, followed by an optional extension (signaled by a period and up to three additional characters), and they cannot include blank spaces.
- Macintosh filenames and folder names can include any Macintosh character except a colon (:). MS-DOS filenames and directory names have more exceptions, such as the following:

  / [ ] ; = " \ : | , * . (except the period signaling the extension)
- Both Macintosh and MS-DOS filenames and folder names (or directory names) can include extended characters; however, the Macintosh and MS-DOS extended character sets are different.

FAT filenames and directory names are acceptable as Macintosh filenames and folder names unless they contain extended characters not found in the Macintosh character set. In such cases, Macintosh users will see valid characters substituted for the invalid ones.

Overview of Macintosh-to-8.3 Translation

When a file is created on a Macintosh and saved on a computer running Windows NT Server, the File Server for Macintosh first checks it for illegal NTFS characters. Then NTFS takes over the file translation process.

What File Server for Macintosh Does

When a Macintosh filename is saved on a computer running Windows NT Server, the File Server for Macintosh component of SFM does the following:

- If required, the File Server for Macintosh changes illegal NTFS characters to the available range of Unicode™ characters, which are then mapped to the ANSI default character—a question mark (?). The following are the illegal NTFS characters:

  " / \ * ? < > | :

What NTFS Does

When NTFS receives a legal NTFS name from the File Server for Macintosh, it translates the name as follows:

- Macintosh names that are valid MS-DOS names do not change: The long name and short name are the same. For example, Sample.art remains Sample.art.
- Long names) are truncated to six characters, followed by a tilde (~) and a unique number, for a total of eight characters (not including any extension).
- The last period (if any) in a long name signals the extension, which is retained.

In detail, here is what the File Server for Macintosh and Windows NT Server do to translate a valid long filename to a short name that MS-DOS users can see:

1. NTFS then shortens a long name to the first six characters of the Macintosh name, followed by a tilde (~) and a unique number. For example, the Macintosh long name *Project Overview* is translated to *Projec~1*.
2. If the short name is a duplicate of another name (long or short), NTFS automatically modifies the short name of the new file or folder by truncating the name to six characters and adding a tilde (~) and number until it creates a unique name.

   For example, suppose a Macintosh user creates a file called *Regional Data-East Coast*. NTFS renames that file *REGION~1*. Next, the user creates a file named *Regional Data-West Coast*. That file becomes *REGION~2*. A third file, *Regional Data-Europe*, becomes *REGION~3*.
3. If the original name has an extension (signaled by the last period in the name), it is retained. For example, *Project Overview.Jan.txt* becomes *Projec~1.txt*.

Note If a Macintosh user gives a file or a folder a valid MS-DOS name, making translation to a short name unnecessary, the user might see a message that states that the name already exists, and that the user must choose a new name. For example, this message appears if the user creates a file named Sales.dat when another file in the folder already has that name.

How Extended Characters Are Mapped

If Macintosh extended characters are used in filenames or folder names that are saved to the computer running Windows NT Server by Macintosh users, the File Server for Macintosh translates these extended characters to the equivalent Unicode characters so that PC users can see them.

If MS-DOS extended characters are used in filenames or directory names that are saved to the computer running Windows NT Server by PC users, the File Server for Macintosh also translates these extended characters to the equivalent Macintosh ANSI characters so that Macintosh users can see them.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Recyclable Paper

Microsoft®