Microsoft®
Windows NT®

MICROSOFT® PROFESSIONAL EDITIONS

For Windows NT Server Version 4.0

Microsoft® Windows NT® Server Internet Guide

Technical Information and Tools for the Support Professional

Microsoft® Press

MICROSOFT® PROFESSIONAL EDITIONS

Microsoft® Windows NT® Server Internet Guide

Microsoft® Press

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Cataloging-in-Publication Data
Microsoft Windows NT Server resource kit : for Windows NT Server
version 4.0 / Microsoft Corporation.
p. cm.
Includes index.
ISBN 1-57231-344-7
1. Microsoft Windows NT. 2. Client/server computing.
I. Microsoft Corporation.
QA76.76.W56M5317 1996
005.7'1369--dc20 96-33396
CIP

Printed and bound in the United States of America.

3 4 5 6 7 8 9 Rand-T 1 0 9 8 7

Distributed to the book trade in Canada by Macmillan of Canada, a division of Canada Publishing Corporation.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office. Or contact Microsoft Press International directly at fax (206) 936-7329.

Part Number: 097-0001649 (Internet Guide)

Acquisitions Editor: Casey Doyle
Project Editor: Stuart J. Stuple

This book is dedicated to Windows NT Webmasters around the world.

Contributors to this book include the following:

Technical Writers:

Peggy Etchevers, Jeff Howard, Laura Sheppard, Maureen Sullivan,

Technical Consultants:

Greg Allen, Noland Angara, Carl Calvello, Ty Carlson, Doug Hebenthal, Jerry Hittle, Cliff Hudson, Aaron Lee, Richard Lerz, Ryan Marshall, Sam Patton, Lester Waters, Valerie Whitcomb, Jim Yagelowich, and numerous other hardworking Windows NT Developers, Program Managers, and Product Support Specialists

Technical Editor:

Kate Robinson

Managing Editor:

Sonia Marie Moore

Software Program Managers:

Louis Kahn, Ryan Marshall

Software Developer:

Martin Holladay

Writing Manager:

Peggy Etchevers

Product Support Liaison:

Todd Hafer

Technical Marketing Liaison:

Ty Carlson

Indexers:

Jane Dow, Barbara Sherman

Production Team:

Karye Cattrell, Nikole Faith, Jay French, Patrick Ngo, Cathy Pfarr, Keri Segna, Jeff Weaver, Todd White

Lead Graphic Designer:

Chris Blanton

Design Support Team:

Johnni Cutler, Amy Iffland, Casey McGahan, Wendy Salvatori, Gabriel Varela, Sue Wyble, Jan Yeager

Contents

Figures and Tables

Figures

Tables

Introduction

Welcome to the *Microsoft® Windows NT® Server Resource Kit: Windows NT Server Internet Guide.*

The *Microsoft Windows NT Server Resource Kit* for version 4.0 consists of three new volumes and a single compact disc (CD) containing utilities for both Windows NT Workstation and Windows NT Server. An online version of the new, comprehensive *Windows NT Workstation Resource Guide* is also available on the CD. Update books for the *Windows NT Server Resource Kit* will be released on a semi-annual basis. They will contain new information and major revisions of existing topics.

The *Windows NT Server Internet Guide* presents detailed information on the Microsoft Internet Information Server, some scenarios for its use on the Internet/intranet, descriptions of Internet-related tools provided on the *Windows NT Server Resource Kit* CD, and suggestions for troubleshooting. Update books will contain more extensive Internet-related information. Some of the scenarios provided here use a fictitious company, Terra Flora, as an example to demonstrate challenges and solutions. The Terra Flora network is based on a real network that has been created at Microsoft in the Windows NT Server Resource Kit Interoperability Lab. The networking model that Terra Flora will implement is shown in the network diagram on the inside back cover of this book.

This information is intended to be a technical supplement to the printed and online documentation included as part of the Windows NT Server version 4.0 product. It does not replace that information as the source for learning how to use the product features and utilities. It is also supplementary to the networking information presented in the *Windows NT Server Networking Guide.*

This Introduction includes the following types of information you can use to get started.

- The first section outlines the contents of this book, so that you can quickly find pertinent technical details.
- The second section introduces the *Windows NT Server Resource Kit* CD.
- The third section describes the support policy for the *Windows NT Server Resource Kit.*

About the Windows NT Server Internet Guide

This book includes the following chapters.

Chapter 1, "Internet Information Server Architecture," provides an overview of the architectural structure of Microsoft Internet Information Server (IIS) and a foundation for understanding the technical concepts presented in the following chapters.

Chapter 2, "Connecting Windows NT Server to the Internet," provides a conceptual overview of the requirements for connecting to the Internet.

Chapter 3, "Server Security on the Internet," describes Internet Information Server authentication and security and then illustrates secure topology configurations for connecting to the Internet.

Chapter 4, "Desktop Scenarios," presents IIS intranet scenarios that use single computers and describes their configuration running Peer Web Services (PWS) and Internet Information Server.

Chapter 5, "Enterprise Scenarios," presents IIS intranet scenarios involving simulated or multiple servers and describes their configuration using IIS virtual servers, IIS database applications, and the IIS FTP service..

Chapter 6, "Internet Connectivity Scenarios Using the Remote Access Service," presents scenarios that use the Windows NT Remote Access Service to provide remote clients access to the Internet.

Chapter 7, "Internet Tools," describes *Windows NT Server Resource Kit* utilities and Microsoft products that can be installed on a Microsoft Internet Information Server to provide a variety of information publishing services.

Chapter 8, "Troubleshooting an Internet Information Server Installation," presents troubleshooting tips that are useful for both IIS and PWS.

Glossary of Internet-related terms used in this book.

Index to this *Windows NT Server Internet Guide*.

Resource Kit Compact Disc

The *Windows NT Server Resource Kit* CD includes a wide variety of tools and utilities to help you work more efficiently with both Windows NT Workstation and Windows NT Server. Notes describing some of the enhancements made to the existing tools and utilities and introducing new ones that have been added for this version 4.0 release are provided in the Introduction to the *Windows NT Server Resource Guide.*

The CD that accompanies the *Windows NT Server Resource Kit* contains utilities that apply to information in the *Windows NT Workstation Resource Guide,* the *Windows NT Server Resource Guide,* the *Windows NT Server Networking Guide*, and the *Windows NT Server Internet Guide.* This new CD replaces all previous ones. It includes a collection of information resources, tools, and utilities that can make networking and working with the Windows NT platform even easier.

Note The utilities on this CD are designed and tested for the U.S. version of Windows NT version 4.0. Use of these utilities on any other version of Windows NT may cause unpredictable results.

A large Help file with explanations and user actions for the majority of the messages included in Windows NT version 4.0, and a large Help file of Performance Counter Definitions are just two of the major items included on the *Windows NT Server Resource Kit* CD. Updates to these files and others will be provided, when available, on the Microsoft Internet web site for the Windows NT Resource Kits. See the Rktools.hlp file for the exact site address, as well as the addresses of other Microsoft information sites.

After installing the *Windows NT Server Resource Kit,* please refer first to the following three files.

- The Readme.wri file, which contains a complete list of all the tools and utilities on the *Windows NT Server Resource Kit* CD and additional setup instructions for some of them.
- Either the Rkdocw.hlp (for Windows NT Workstation) or the Rkdocs.hlp (for Windows NT Server) file, which provides a single entry point for all of the major components of the Resource Kit's online documentation.
- The Rktools.hlp file, which provides an overview of the Resource Kit tools and utilities and basic instructions on how to use many of them, along with links to additional documentation and, in some cases, to the actual program files.

The most current corrections to those tools and utilities and their documentation, as well as the POSIX and Perl source code files, are available on the Internet at the following Microsoft FTP site.

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/

Resource Kit Support Policy

The SOFTWARE supplied in the *Windows NT Server Resource Kit* is not officially supported. Microsoft does not guarantee the performance of the *Window NT Server Resource Kit* tools, response times for answering questions, or bug fixes to the tools. However, we do provide a way for customers who purchase the *Windows NT Server Resource Kit* to report bugs and receive possible fixes for their issues. You can do this by either sending Internet mail to RKINPUT@MICROSOFT.COM or by referring to one of the options listed in the *Start Here* book, which is included with your Windows NT Server product. This mail address is only for *Windows NT Server Resource Kit* related issues.

The SOFTWARE (including instructions for its use and all printed and online documentation) is provided "AS IS" without warranty of any kind. Microsoft further disclaims all implied warranties, including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The entire risk arising out of the use or performance of the SOFTWARE and documentation remains with you.

In no event shall Microsoft, its authors, or anyone else involved in the creation, production, or delivery of the SOFTWARE be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the SOFTWARE or documentation, even if Microsoft has been advised of the possibility of such damages.

CHAPTER 1

Internet Information Server Architecture

Microsoft Internet Information Server is a network file and application server included with the Microsoft Windows NT Server operating system.

This chapter explains design principles and the architecture behind Internet Information Server. Internet Information Server supports three information protocols: HTTP, FTP, and Gopher. This chapter explains how these protocols work with Internet Information Server and how to configure their operation.

Internet Information Server Design Priorities

The design goal for Internet Information Server was to build a set of integrated server services to support File Transfer Protocol (FTP), Gopher, and Hypertext Transport Protocol (HTTP) services.

Internet Information Server is designed for maximum performance, integration, and extensibility.

- *Performance.* Internet Information Server maximizes speed while using the minimum amount of memory (RAM). Internet Information Server uses approximately 400K of RAM when running all three services (HTTP, FTP, Gopher).
- *Integration.* Internet Information Server is integrated with Microsoft Windows NT Server. Internet Information Server uses the same directory database (user accounts) as Windows NT Server. Using the same directory database eliminates the need for additional user account administration. Internet Information Server administration also uses existing Windows NT Server tools such as Performance Monitor, Event Viewer, and Simple Network Management Protocol (SNMP) support to maintain similar administrative procedures.

- *Extensibility.* Internet Information Server is extensible. Internet Information Server supports the Internet Server Application Programming Interface (ISAPI). By using ISAPI you can extend the functionality of the HTTP service: You create programs that can preprocess and postprocess data sent to and from Internet Information Server. ISAPI is also used in Internet Information Server to create connectors, such as the Internet Database Connector. Internet Information Server uses connectors to use the services of other servers, such as ODBC databases.

Architecture Overview

All of the standard Internet services (FTP, Gopher, and HTTP) reside in a process called Inetinfo. This process is about 400K in size. In addition to the Internet services, this process contains the shared thread pool, cache, logging, and SNMP services of Internet Information Server.

Internet Information Server Connectors

Extensions are built into Internet Information Server in the form of connectors. A connector is an ISAPI dynamic-link library (DLL) that acts as a communication pipe between Internet Information Server and a service. The following connectors are supported.

- Microsoft BackOffice™ connectors
  - Microsoft Exchange Server/Web connector supports public folder integration with Internet Information Server.
  - Internet Database Connector (IDC) connector allows communication with any ODBC-compliant database engine.
- Common Gateway Interface (CGI) was developed for UNIX-based systems to extend Web server software. Internet Information Server supports CGI applications for backward compatibility.
- ISAPI filters preprocessing packets before they enter or leave the Internet Information Server process. These filters give added flexibility to the Internet Information Server architecture. Secure Sockets Layer (SSL) is one example of an ISAPI filter.

Internet Service Manager

Internet Service Manager enables administrators to manage many Internet Information Server sites from a single location anywhere on the Internet. Internet Service Manager communicates by using remote procedure calls (RPCs). Internet Information Server can be used locally or remotely because of its support for RPCs.

Logging

Internet Information Server logging enables you to track which users access your site and when they access your site. Tracking users helps to identify security and performance issues. Logging can be directed either to a log file that can be processed offline and offers faster performance, or to an ODBC Data Source Name (DSN) for dynamic evaluation.

WWW Service

The World Wide Web (WWW) service uses the Hypertext Transport Protocol. HTTP is implemented through an interface to Windows Sockets. Internet Information Server version 2.0 (included with Windows NT Server version 4.0) supports HTTP version 1.0.

The Hypertext Transport Protocol is an application-level protocol. HTTP is a distributed, collaborative, hypermedia information system that has been in use since 1990. HTTP technology has enabled what most commonly refer to as the World Wide Web.

HTTP grew out of a need for a universal protocol to simplify the way users access Internet information. HTTP is generic, stateless, and object oriented. It can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands). Because HTTP types and negotiates data representation, systems based on it can be built independently of the data being transferred.

The current specification reflects common usage of the protocol referred to as HTTP/1.0, and is the basis for the information in this section.

Discussion and improvement of the HTTP standard is ongoing. You can find extensive information about HTTP at the Internet address **http://www.w3.org/pub/WWW/**.

HTTP Communication Process

Hypertext Transport Protocol is a client/server protocol. This means that the client and server interact to perform a specified task. For example, when a user clicks a link on a Hypertext Markup Language (HTML) page, it apparently causes that page to be replaced with the new page. What actually happens is more complex.

1. The client browser uses HTTP commands to communicate with the HTTP server.
2. A connection is established from the client to the server by means of TCP port 80 (the default).

3. The request message is sent to the server. The requests are typically for a file consisting of images, audio clips, animation clips, video clips, or another hypertext document.
4. The server sends a response message with the requested data to the client.

   For example, when the user clicks a link on an HTML page, the data in the response message comprises the code used to build the page on the client computer.
5. The server (in most cases) closes the connection.

Table 1.1 defines some of the terms used to refer to the roles played by participants in, and objects of, the HTTP communication process.

Table 1.1 Terms Used in HTTP Communication

Term	Meaning
connection	A virtual circuit (in the transport layer) established between two application programs for the purpose of communication.
message	The basic unit of HTTP communication. It consists of a structured sequence of octets and is transmitted through the connection.
request	An HTTP request message.
response	An HTTP response message.
resource	A network data object or service that can be identified by a URL.
entity	The information transferred as the payload of a request or response. An entity consists of metainformation in the form of entity-header fields and content in the form of an entity-body.

HTTP Requests

The Simple-Request message to the server is sent in the form of a request method, Uniform Resource Locator (URL), and protocol version. The following is an example of an HTTP request.

get http://www.w3.org/hypertext/WWW/TheProject.html HTTP/1.0

This request uses the elements described in Table 1.2.

Table 1.2 Elements of an HTTP Request

Element	Purpose
get	Specifies the request type.
http:	Specifies the request protocol.
//www.w3.org/hypertext/WWW/TheProject.html	States URL for the object requested.
HTTP/1.0	Indicates that version 1.0 of HTTP will be used.

In a Full Request message, the additional information is followed by a Multipurpose Internet Mail Extensions (MIME) message containing request modifiers, client information, and sometimes body content.

HTTP Server Response Messages

When an HTTP server receives a request, it responds with a status message that includes the message's protocol version and a success or error code, followed by a MIME message containing server information, entity metainformation, and sometimes body content.

Table 1.3 lists examples of server status messages and their meanings. For more information, see Chapter 8, "Troubleshooting an Internet Information Server Installation."

Table 1.3 Explanations for Server Status Messages

Message	Type	Explanation
1*xx*	Informational	This series of responses is not currently used. They are reserved for future use.
2*xx*	Success	The action was successfully received, understood, and accepted.
3*xx*:	Redirection	Further action must be taken in order to complete the request.
4*xx*	Client Error	The request contains incorrect syntax or cannot be fulfilled.
5*xx*	Server Error	The server failed to fulfill an apparently valid request.

URLs

In all Internet protocols, including HTTP, a client must locate Internet resources by using a Uniform Resource Locator. The URL for an HTTP address can be broken into three parts.

- *How (scheme).* Defines how the request is made. When the HTTP scheme is used, network resources are located by means of the Hypertext Transport Protocol.
- *Where.* Defines the host.
- *What.* Specifies the complete path to the object and the object's name that is being requested by the client.

For example, this is the syntax for a URL that uses the HTTP scheme:

http: *//host*[:*port*]*abs_path*

where

host
A legal Internet host domain name or IP address (in dotted-decimal form), as defined by Section 2.1 of RFC 1123.

:port
Port 80 is used if no port is specified. However, by using this optional parameter, you can specify any port.

abs_path
The full path and filename.

The type of scheme used depends upon the object being requested. The following schemes are currently supported by Internet Explorer.

File
FTP
Gopher
HTTP
Mailto
News
NNTP
Prospero
Telnet
WAIS

For more information about these and other schemes, see the Internet address **http://www.w3.org/pub/WWW/Addressing/schemes.html**.

HTTP Browser

On the client side, the browser issues a command when the user either clicks an object or types a URL in the location field.

Included with Microsoft Internet Information Server is a browser (Microsoft Internet Explorer) you can use to access Internet sites. After you connect to the Internet, you can use Internet Explorer to view information on the Internet. You can incorporate this information into your documents, or save it to a file on your computer.

To begin exploring the Internet, click an item in the Internet Explorer main window.

Monitoring HTTP Sessions

You can monitor HTTP sessions by using the **netstat** TCP/IP utility and the Performance Monitor.

The **netstat** utility shows static information at a given point in time. **Netstat** is best used to determine the status of connections. Table 1.4 provides examples of **netstat** syntax and the results of each.

Table 1.4 Netstat Command Examples

Example syntax	Result
netstat	Displays protocol (TCP or User Datagram Protocol) being used, local and foreign (remote) addresses by their friendly names, the port number used on the local computer, and the state of the connection.
netstat -n	Displays protocol (TCP or UDP) being used, local and foreign socket addresses, and the state of the connection.
netstat -s -p tcp	Displays active opens, passive opens, failed connection attempts, reset connections, current connections, segments received, segments sent, and segments retransmitted.

For more information on the **netstat** utility, see the online Command Reference in Windows NT Help.

Performance Monitor shows events happening in real time. Performance Monitor is best used to check the status of users. Table 1.5 shows real-time statistics that Performance Monitor displays for HTTP as well as FTP and Gopher.

Table 1.5 Statistics Displayed by Performance Monitor

Counter	HTTP service	Objects for FTP service	Gopher service
Aborted Connections	NA	NA	✓
Bytes Received/sec	✓	✓	✓
Bytes Sent/sec	✓	✓	✓
Bytes Total/sec	✓	✓	✓
CGI Requests	✓	NA	NA
Connection Attempts	✓	✓	✓
Connection/sec	✓	NA	NA
Connections in Error	NA	NA	✓
Current Anonymous Users	✓	✓	✓
Current CGI Requests	✓	NA	NA
Current Connections	✓	✓	✓
Current ISAPI Extension Requests	✓	NA	NA
Current NonAnonymous Users	✓	✓	✓
Directory Listings Sent	NA	NA	✓
Files Received	✓	✓	NA
Files Sent	✓	✓	✓
Files Total	✓	✓	NA
Get Requests	✓	NA	NA
Gopher Plus Requests	NA	NA	✓
Head Requests	✓	NA	NA
ISAPI Extension Requests	✓	NA	NA
Logon Attempts	✓	✓	✓
Maximum Anonymous Users	✓	✓	✓
Maximum CGI Requests	✓	NA	NA
Maximum Connections	✓	✓	✓
Maximum ISAPI Extension Requests	✓	NA	NA
Maximum NonAnonymous Users	✓	✓	✓
Not Found Errors	✓	NA	NA
Other Request Methods	✓	NA	NA
Post Requests	✓	NA	NA
Searches Sent	NA	NA	✓
Total Anonymous Users	✓	✓	✓
Total NonAnonymous Users	✓	✓	✓

Modifying HTTP Ports

For most installations of Internet Information Server, you keep the HTTP server port number set at the default 80 to allow HTTP clients access to your site. However, it is simple to modify the well-known (standard) port numbers for HTTP.

Warning Using Registry Editor incorrectly can cause serious, systemwide problems that may require you to reinstall Windows NT to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk.

When possible, change configuration through Control Panel settings. However, as in the procedure that follows, there are settings that can be changed only by using Registry Editor.

▷ **To change the port used by the HTTP service**

1. Start the Registry Editor, **Regedt32.exe**.
2. Click the HKEY_LOCAL_MACHINE window and locate the following key:

```
\System
 \CurrentControlSet
  \Control
   \ServiceProvider
    \ServiceTypes
     \W3SVC
```

3. Click W3SVC, then double-click the **TcpPort** entry on the right side of the screen.

   The **DWORD Editor** dialog box appears.
4. Click **Decimal**, then enter the port number in the **Data** box.
5. Click **OK** and close Registry Editor.
6. Stop and restart the WWW service.

Your HTTP server now monitors the specified port for all HTTP client requests.

Note This situation affects the default port on the HTTP server only.

Troubleshooting HTTP with Network Monitor

By using the Microsoft **network monitor** utility, you can reveal the contents of a specific frame. By examining the HTTP messages, you can determine whether the correct messages were sent.

Network monitor captures the full frame before it reaches the network components and the browser client. Thus, you can isolate the symptoms of events that occur before the frames reach the host computer.

For more information about **network monitor**, see the *Windows NT Server Concepts and Planning Guide.*

FTP Service

FTP is the protocol used to transfer files between two computers on a network that uses Transmission Control Protocol/Internet Protocol (TCP/IP). FTP was one of the earliest protocols used on TCP/IP–based networks and the Internet. Although the World Wide Web has replaced most functions of FTP, FTP is still the only way to copy files from a client computer to a server over the Internet.

To use FTP to transfer files between two computers, both computers must support their respective FTP roles. In other words, one needs to be an FTP client and the other an FTP server. The FTP client can issue commands to the server, such as commands to download files, upload files, create directories on the server, and change directories on the server.

FTP uses TCP as its transport protocol for all communication and data exchanges between the client and the server. However, Internet Information Server communicates with Windows Sockets, then Windows Sockets communicates with TCP.

TCP is a *connection-oriented* protocol. “Connection-oriented” means that the communications session is established between the client and the server before data is transmitted. The connection remains active during the entire FTP session. Connection-oriented sessions are known for their reliability and error-recovery features. This means that FTP file transfers are very reliable.

TCP has the features described in Table 1.6.

Table 1.6 TCP Connection Features

Feature	Description
Flow control	Both client and server computers participate in the transmission of the packets, which virtually eliminates potential problems with packet overflows and lost packets.
Acknowledgment	The computer sending data packets expects an acknowledgment message (ACK) from the destination computer. This acknowledgment verifies that the packet was successfully received at the destination.
Retransmission	If the sending computer does not receive an ACK in a specified period of time, it assumes the packet became lost or corrupted and retransmits the packet.
Sequencing	All packets are numbered and sent in order so that the receiving computer reorganizes the data correctly.
Checksum	All packets contain a checksum to ensure integrity of the data. If the data is corrupted somewhere during the transmission, the checksum is used to indicate that the data is not the same data that was sent.

Note Do not confuse FTP with Trivial File Transfer Protocol (TFTP). TFTP is a fast, simple file transfer protocol that uses the User Datagram Protocol (UDP) transport. UDP, unlike TCP, is a connectionless protocol and cannot retransmit packets. This means that UDP is not as reliable as TCP.

TCP Ports and Sockets

Three identification numbers are commonly used when referring to TCP sockets.

- The *IP address* identifies the computer on the network.
- The *TCP port number* identifies a process or application inside the computer.
- The *socket* identifies both the computer and the process simultaneously. A socket is used as an endpoint.

Note TCP ports are known by a variety of names. These names include TCP port number, TCP port address, TCP port, port number, port address, port, and data port.

Any application or process that uses TCP for its transport is assigned a unique identification number called a TCP port. TCP ports specify the path of communication between client and server applications. These ports are numbered beginning with zero. Port numbers for client applications are dynamically assigned by the operating system when there is a request for service. Port numbers for server applications are preassigned by the Internet Assigned Numbers Authority (IANA) and do not change.

IANA is the group that assigns processes to port numbers 0 through 1023. This range of numbers is reserved for services. A client application or process that uses TCP as a transport is assigned a port number greater than 1023 by the operating system.

A server application or process that uses TCP as a transport has at least one preassigned port number. For example, the preassigned port numbers for FTP server services are 20 (data) and 21 (control). These port assignments are called the "Well Known Port Numbers" and are documented in RFC 1700 (see **http://ds.internic.net/std/std2.txt**). Table 1.7 is a short list of some Well Known Port Numbers. (For more port numbers, see Appendix B, "Port Reference for Microsoft TCP/IP," in the *Windows NT Server Networking Guide.*)

Table 1.7 Some Well Known Port Numbers

Port number	Process name	Description
1	TCPMUX	TCP Port Service Multiplexer
5	RJE	Remote Job Entry
20	FTP-DATA	File Transfer Protocol - Data
21	FTP	File Transfer Protocol - Control
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer Protocol
42	NAMESERV	Host Name Server
49	LOGIN	Login Host Protocol
53	DOMAIN	Domain Name System
69	TFTP	Trivial File Transfer Protocol
70	GOPHER	Gopher
80	HTTP	HTTP
103	X400	X.400
110	POP3	Post Office Protocol version 3
137	NETBIOS-NS	NetBIOS Name Service
139	NETBIOS-DG	NetBIOS Datagram Service

Table 1.7 Some Well Known Port Numbers *(Continued)*

Port number	Process name	Description
150	NETBIOS-SS	NetBIOS Session Service
156	SQLSRV	SQL Server
179	BGP	Border Gateway Protocol

Port numbers are used in conjunction with an IP address to form a *socket.* Sockets always have a number (or address) associated with them and designate an endpoint. Examples of socket numbers are shown in Table 1.8.

Table 1.8 Socket Examples

IP address	Port number	Socket number
10.155.22.99	1028	#10.155.22.99(1028)
172.16.16.10	21	#172.16.16.10(21)

FTP and Ports

When FTP is running on a server, it constantly monitors port 21, the FTP control port, for a request for service from the FTP server. To connect to the FTP server, the FTP client computer sends a request to TCP port number 21 on the server computer.

For example, assume that computer A is the FTP client, computer B is the FTP server, and that they have the following IP addresses.

Computer A (FTP client)	Computer B (FTP server)
IP address: 172.16.16.10	IP address: 10.155.22.99

The communication between the FTP client and FTP server follows this process.

1. At the command prompt on computer A, the user types the following information:

   FTP 10.155.22.99

2. The operating system assigns a TCP port number greater than 1023 (for example, 1028) to the FTP client application.
3. TCP creates a packet that includes the following information:

Source IP Address	172.16.16.10
Source TCP Port Number	1028
Destination IP Address	10.155.22.99
Destination TCP Port Number	21

4. The packet is sent across the network to IP address 10.155.22.99.
5. Computer B receives the packet and TCP forwards the packet to port 21 (FTP control).
6. The FTP service on computer B sends an acknowledgment (ACK) back to computer A by using both the IP address (172.16.16.10) and the port number (1028).

The packet cannot be accidentally delivered to a wrong port address on the server because the packet contains the correct port number before it leaves the client computer.

FTP Control and Data Connections

FTP uses two TCP connections to communicate between the client and the server. These connections are called the control connection and the data transfer connection. Connections can be ready in one of two states: passive open (waiting for a transmission) or active open (initiating the transmission).

The control connection starts the communication between the FTP client and the FTP server. The control connection is maintained for the duration of the FTP session. The control connection uses port 21 on the server and an open port that is greater than 1023 on the client.

The control connection is managed by a set of programs called the server Protocol Interpreter (server-PI) and the user Protocol Interpreter (user-PI).

The server-PI maintains a passive open state at port 21 waiting for the arrival of an FTP connection request from a client. When a request arrives, the server-PI establishes a control communication connection, receives standard FTP commands from the user-PI, sends replies, and governs the server Data Transfer Process (server-DTP).

The user-PI initiates the control connection (active open) from its TCP port to the server-PI, initiates FTP commands, and governs the user Data Transfer Process (user-DTP).

The data transfer connection exists only when there is data to be transferred between the client and the server. The data transfer connection closes each time a data transfer is completed. The control connection remains open.

Because of this, a new client data port must be opened each time a new data transfer begins. The server data port is always 20.

The data transfer connection is managed by a set of programs called the server Data Transfer Process (server-DTP) and the user Data Transfer Process (user-DTP). The server-DTP establishes the data connection (active open) with the user-DTP, sets up the parameters for transfer and storage, and transfers data on command from the server-PI. The user-DTP waits at its FTP port (passive open) for a connection from the server-DTP.

Using FTP

This section describes a typical FTP session.

▷ **To start an FTP session and connect to an FTP server**

1. Start a command prompt and type the following information:

   ftp *IPaddress*

   where *IPaddress* is a valid IP address. Then press ENTER.

   Note To test TCP/IP on your computer, you can always use the IP address 127.0.0.1. This address is known as the *loopback address* for your computer. The loopback address uses *loopback drivers* to reroute outgoing packets back to the source computer. By going through the loopback drivers, the packets can bypass the network adapter card completely and be returned directly to the computer that is performing the test.

2. When you are prompted to log on with a user name, log on as Anonymous.
3. When prompted for a password, press enter. An ftp> prompt appears.

At the ftp> prompt, you can enter FTP commands. Some of the common FTP commands are described in Table 1.9. (For a complete list of FTP client commands, see Appendix A, “TCP/IP Utilities Reference,” of the *Windows NT Server Resource Kit Networking Guide*.)

Table 1.9 Common FTP Commands

Command	Purpose
bye	Ends the FTP session with the remote computer and exits FTP.
delete	Deletes files on the remote computer; requires appropriate permissions.
dir	Lists the remote directory's files and subdirectories.
get	Copies a remote file to your computer.
help	Displays descriptions for FTP commands.
open	Connects to the specified FTP server.
put	Copies a file from your computer to the remote computer; requires appropriate permissions.
mkdir	Creates a directory on the remote computer, requires appropriate permissions.
!	Returns you to the Microsoft MS-DOS® shell. FTP is still active; type **exit** to return to the >ftp prompt.
!*command*	Executes an MS-DOS command on the local computer from the FTP session.

For example, to copy a file from the server computer, type the following command at the >ftp prompt.

get *filename*

This command copies the specified file from the server to the client.

After you enter a command, you receive a series of return codes from the FTP server on a number of lines. The return codes let you know the status of each command. Table 1.10 shows some of the common return codes listed in RFC 640. Information in italics is supplied by the server. (A complete list of return codes in RFC 640 can be found at **http://andrew2.andrew.cmu.edu/rfc/rfc640.html**.)

Table 1.10 FTP Server Return Codes

Code	Meaning
119	Terminal not available, will try mailbox.
120	Service ready in *nnn* minutes.
125	Data connection already open; transfer starting.
225	Data connection open; no transfer in progress.
150	File status okay; about to open data connection.
151	User not local; will forward to *user@host.*
152	User unknown; mail will be forwarded by the operator.
250	Requested file action okay, completed.
200	Command okay.
211	System status, or system help reply.
212	*Directory status.*
213	*File status.*
214	*Help message.*
220	Service ready for new user.
221	Service closing Telnet connection.
226	Closing data connection; requested file action successful (for example, file transfer or file abort).
227	Entering passive mode.
230	User logged in; proceed.
331	User name okay; need password.
332	Need account for login.
350	Requested file action pending further information.
450	Requested file action not taken: file unavailable (for example, file busy).
421	Service not available, closing Telnet connection. This can be a reply to any command if the service must shut down.
425	Cannot open data connection.
426	Connection closed; transfer aborted.
530	Not logged in.
532	Need account for storing files.
550	Requested action not taken.

Modifying FTP Ports

It is easy to modify the Well Known Port Number for FTP. However, to allow FTP clients access to your site, keep the FTP server port number set at 21 for most installations of Internet Information Server.

If you want to limit access to your FTP server, you can change the control connection (port 21) to a TCP port number greater than 1023 to "hide" your site.

You can change FTP server TCP port numbers by modifying the *Systemroot*\System32\Drivers\Etc\Services file or by changing their values in the Registry. The setting in the Services file takes precedence over the Registry setting in all cases. That is, by changing the Services file, you affect both the FTP client and the FTP server. By changing the Registry, you affect only the FTP server.

▷ To change the TCP port in the Services file

1. At a command prompt, change directories to *Systemroot*\System32\Drivers\Etc.
2. Use a text editor to search the Services file for the following two entries:

```
ftp-data            20/tcp
ftp                 21/tcp
```

3. Modify port 21 to a number greater than 1023. See the following example.

```
ftp-data            20/tcp          # The # sign designates a comment.
ftp                 1234/tcp        # FTP port changed to 1234, was 21.
```

4. Save and close the file. To implement the change, stop, then restart the FTP service.

Note This affects the default TCP ports on both the FTP client and the FTP server.

Your FTP server now waits at port 1234 for all FTP client requests and your FTP client connects only to an FTP server at port 1234.

▷ To verify the new FTP port settings

1. At a command prompt, type the command **ftp**.

   The ftp> prompt appears.

2. Type the command **open 127.0.0.1 21** and then press ENTER.

   The IP address 127.0.0.1 is the loopback address for your computer. You are specifying 21 as the destination port address. The following message appears:

```
-> ftp: connect:Connection refused
```

3. Type the command **open 127.0.0.1** and then press ENTER.

   The port now reverts to the default number specified in the Services file: 1234. You are prompted with the following logon message:

   ```
   User <127.0.0.1:<none>>:
   ```

   This verifies that both the FTP client and FTP server are using port 1234.

▹ To change the Registry entry for FTP

1. Start the Registry Editor, **Regedt32.exe.**
2. Click the HKEY_LOCAL_MACHINE window and locate the following key:

   ```
   \System
    \CurrentControlSet
     \Control
      \ServiceProvider
       \ServiceTypes
        \MSFTPSVC
   ```

3. Click MSFTPSVC and then double-click the **TcpPort** value.

   The **DWORD Editor** dialog box appears.
4. Click **Decimal** and enter **5678** in the **Data** box.
5. Click **OK** and close the Registry Editor.
6. At the command prompt, type the following information:

   cd %systemroot%\system32\drivers\etc

   ren services services.ok

   This prevents the FTP server from using the port address in the Services file after it has been restarted.
7. To implement the change, stop and restart the FTP service.

Note This situation affects the default port only on the FTP server.

If you have completed the preceding steps, your FTP server now monitors port 5678 for all FTP client requests and your FTP client connects to an FTP server at port 1234 only.

▷ To verify the new FTP port settings

1. At a command prompt, type **ftp**, then press ENTER.

   The ftp> prompt appears.

2. Type the following commands:

   open 127.0.0.1

   open 127.0.0.1 21

   open 127.0.0.1 1234

   The following message appears:

   ```
   -> ftp: connect: Connection refused
   ```

3. Type the command **open 127.0.0.1 5678** and then press ENTER.

   The port defaults to the number specified in the Registry: 5678. You are prompted with the following logon message:

   ```
   User <127.0.0.1:<none>>:
   ```

   This procedure verifies that both the FTP client and FTP server are using port 5678.

Customizing FTP Server

When a client connects to an FTP server, the user often lacks site information. Without site information, the user does not know if this is the correct FTP server, or what the files at the site contain. By adding a welcome message, exit message, and directory contents message, you can supply such information to visitors to your FTP site.

You can use two methods to add information about your FTP site. Both methods can enhance its usability.

You can use the Internet Service Manager to add default Welcome or Exit messages to the FTP server. Double-click the **FTP service**, then click **Messages** to add or change FTP service messages.

You can also add an FTP directory description file. For examples of this process, see Chapter 5, "Enterprise Scenarios."

▷ To enable the FTP directory description file

1. Click the **Start** button, then point to **Run.** In the **Open** box, type **regedt32.exe** and then click **OK.**

   The Registry Editor appears.

2. Click the HKEY_LOCAL_MACHINE window and locate the following key:

   ```
   \System
    \CurrentControlSet
     \Services
      \MSFTPSVC
       \Parameters
   ```

3. On the **Edit** menu, click **Add Value.**

   The **Add Value** dialog box appears.

4. In the **Value Name** text box, type **Annotate Directories.**
5. In the **Data Type** box, select REG_DWORD and then click **OK.**

   The **DWORD Editor** dialog box appears.

6. In the **Data** text box type **1** and click **OK.**

   The Registry Editor adds the new value to the Parameters key.

7. Close the Registry Editor.
8. To implement these changes, stop and restart the FTP service.

▷ To add an FTP directory description file

1. Using a text editor, create the file ~ftpsvc~.ckm
2. In the file, type the following lines:

   ```
   Directory for the Terra Flora FTP Server
   ----------------------------------------------------
   ```

3. Save the file in the root directory of the FTP server and close the editor.
4. At the command prompt in the root directory of the FTP server, type the following information and then press Enter.

   ```
   attrib +h ~ftpsvc~.ckm
   ```

   This step hides the file.

▷ **To verify the customized FTP server**

1. At the command prompt, type the following information.

   ftp 127.0.0.1

   This step uses the IP loopback address to start an FTP session on your local computer.

   The FTP client prompts you to log on.

2. Log on as Anonymous.

   The introductory message and the annotated directory listing appear.

3. At the ftp> command prompt, type the following information.

   BYE

   The exit message appears.

Monitoring FTP Sessions

You can monitor FTP, just like HTTP sessions, by using the **netstat** TCP/IP utility and the Performance Monitor.

The **netstat** utility shows static information at a given point in time. **Netstat** is best used to determine the status of connections. You can run **netstat** from a command prompt or inside an FTP session by using the **!** command. For examples of **netstat** command syntax, see Table 1.4, earlier in this chapter.

Performance Monitor shows events happening in real time. Performance Monitor is best used to check the status of users, file transfers, and byte transfers. For a listing of real-time statistics displayed by Performance Monitor for the FTP service, see Table 1.5, earlier in this chapter.

Gopher Service

Gopher is client/server–oriented software that uses a simple protocol to search for and retrieve files from Gopher servers on the Internet. The Gopher service was developed by the University of Minnesota in 1991 to overcome some limitations of the FTP service. Gopher has an easier-to-use interface and also allows administrators to create links to other computers or services, to annotate files and directories, and to create custom menus.

Gopher is not just an Internet tool. Many organizations use Gopher on their local area network to help people within the organization find the information they need quickly and efficiently.

The user of the Gopher client can download files, switch directories, or link to other Gopher servers by using a series of menus. The Gopher server generates menus, links, and annotations by using a series of tag files.

Gopher presents information in a hierarchical structure. Depending on which client software is used and what selections are available on the Gopher server, the user can choose how to view information—for example, as a text file, as a Microsoft Word for Windows document, or in a particular language.

A Gopher client presents the individual user with directory lists. If the user chooses a subdirectory from the displayed list, the listing for that subdirectory is displayed. If the user chooses a file, it is downloaded. Each directory and file can be on a different Gopher server.

You can also configure a Gopher server to search local Wide Area Information Server (WAIS) databases.

Gopher uses TCP as its transport protocol for all communication and data exchanges between the client and the server. Internet Information Server communicates with Windows Sockets, then Windows Sockets communicates with TCP.

TCP is a connection-oriented protocol (that is, the communications session is established between the client and the server before data is transmitted). However, unlike FTP, Gopher does not maintain the connection between requests; this is also known as a stateless connection.

For a description of TCP connection features, see Table 1.6, earlier in this chapter.

Gopher Ports and Connections

The Gopher protocol consists of a client and a server communicating through a TCP connection. The server waits at port 70 for a client request. The client, after initiating the connection, sends a *selector* to the server. A selector is a line of text that can consist of a series of characters or a null string. The server responds with a block of text terminated with a period on a line by itself. After receiving an acknowledgment from the client, the server closes the connection.

Similar to FTP, the Gopher client always communicates on a port whose number is greater than 1023. This port number changes each time a new transaction begins between the client and the server.

Designing a Gopher Site

Because most computer users are familiar with a hierarchical file system, you should design a Gopher site to resemble a directory tree structure. That is, the root directory contains names of subdirectories, links to other sites, and an explanation (Readme) file. The actual content is stored in subdirectories on the server.

When using Microsoft Internet Information Server, the default root directory is *Systemroot*\System32\Inetsrv\Gophroot.

Gopher Types

Gopher servers contain Gopher objects and each object has an associated Gopher type. The Gopher type signals the client what to do when that object is selected from the menu. Table 1.11 explains the Gopher types.

Table 1.11 Gopher Types and Client Behavior

Type	Description	Client action
0	Text file, typically an ASCII document	Usually displayed on the screen.
1	Directory listing	Expect another Gopher menu.
2	CSO phone book server	Expect to be queried for a person's name.
3	Error	
4	Macintosh® BinHex file	Expect the file to be transferred.
5	MS-DOS .zip or other archive file	Expect the file to be transferred.
6	UNIX UUENCODE file	Expect the file to be transferred.
7	Search item	Expect to be queried for a relevant search string.
8	Telnet session	Expect the Telnet program installed on your computer to start.
9	Binary file	Expect the file to be transferred.
T	3270 session	Expect the tn3270 program installed on your computer to start.
S	Sound file	Expect the file to be transferred and then played by a sound application on your computer.
g	Graphics file	Expect the file to be transferred and then displayed by a graphics application on your computer.
M	MIME file	Expect the file to be transferred and then displayed by an application on your computer.
h	HTML file	Expect the file to be transferred and then displayed by an application on your computer.
I	Image file	Expect the file to be transferred and then displayed by an application on your computer.
i	In-line text type	Used to suppress item numbers in text-only clients.

Gopher Tag Files

You use Gopher tag files to set up links to other Gopher servers and resources, and to give descriptive names to files and directories on Gopher servers. Gopher tag files are configured by using the **gdsset** utility. This utility creates hidden tag files (*.gtg) in the \Inetsrv\Gophroot directory. The examples in the following three sections demonstrate how to use tag files to customize the Gopher site.

Changing Filename Display

In this example, you have two Readme files and a subdirectory in the \Inetsrv\Gophroot directory on your server. When a Gopher client accesses your computer, the following menu displays.

```
1 README1.TXT
2 README2.TXT
3 SUBDIR
```

Readme1.txt describes the mission of this Gopher site. Readme2.txt describes how to contact the site administrator. And Subdir is a subdirectory that contains the content of this Gopher site.

To change these filenames to a descriptive name format, type the following **gdsset** commands at a command prompt.

```
gdsset -c -g0 -f "The Mission of this Gopher Site" README1.TXT
gdsset -c -g0 -f "Contact the Site Administrator" README2.TXT
gdsset -c -g0 -f "Contents of this Gopher Site" SUBDIR
```

These commands create three hidden tag files in the \Inetsrv\Gophroot directory: Readme1.txt.gtg, Readme2.txt.gtg, and Subdir.gtg. The tag files set up an association between the descriptive name and the filename. The next time a Gopher client accesses your computer, the following menu displays.

```
1 The Mission of this Gopher Site
2 Contact the Site Administrator
3 Contents of this Gopher Site
```

When a user clicks The Mission of this Gopher Site, the Gopher client displays the contents of Readme1.txt. Clicking Contact the Site Administrator displays the contents of Readme2.txt, and clicking Contents of this Gopher Site displays the contents of the directory Subdir. The original filenames and directory names are hidden from the Gopher client.

Creating Links to Directories

In this example, you have five subdirectories under the root Gopher directory (\Inetsrv\Gophroot) on your server.

\Inetsrv\Gophroot\Subdir1\Subdir2\Subdir3\Subdir4\Subdir5

When a Gopher client accesses your machine, the user sees the following menu display.

```
SUBDIR1
```

If a user wants to access files in Subdir5, the user must access four additional subdirectories to access Subdir5.

To establish a link to Subdir5 from the root directory and provide a descriptive name format for Subdir5, use the following **gdsset** commands at a command prompt.

gdsset -c -l -g1 -f "Microsoft Windows Printer Drivers Location" -s \Subdir1\Subdir2\Subdir3\Subdir4\Subdir5 link.subdir5

This command creates a hidden tag file, called Link.Subdir5.gtg, in the \Inetsrv\Gophroot directory.

Note All link files must start with the prefix "link"; however, do not use the prefix "link" for any other tag files.

The next time a Gopher client accesses your computer, the following menu is displayed.

```
SUBDIR1
Microsoft Windows Printer Drivers Location
```

Clicking Microsoft Windows Printer Drivers Location brings the user directly to Subdir5.

Creating Links to Other Gopher Sites

To link to another Gopher site, add the host name or IP address to the **gdsset** command. For example, to link to the Greater London, England Gopher Server, you issue the following command from an >ftp command prompt.

gdsset -c -l -g1 -f "Link to the Greater London, England Gopher Server" -s -hgopher.london.com link.london

The links, files, friendly names, and directories that appear on the server are in alphabetical order.

Using Gopher

Internet Explorer works as a Gopher client. To connect to a Gopher server, start Internet Explorer and enter a Gopher address in the address box. For example, you can enter

gopher://gopher.college.edu/

If the name or IP address of the Gopher server is known, but the server is not using the standard TCP port address (70), you can alter the address on the client to match the server. For example, if the Gopher server is monitoring port 1938, use the following command.

gopher://gopher.college.edu:1938

Modifying Gopher Ports

For most installations of Internet Information Server, you keep the Gopher server port number set to the default 70 to allow other Gopher clients access to your site. However, if you want to limit access to your Gopher server, you can change the control connection (port 70) to a port number greater than 1023 to "hide" your site.

You can change Gopher server port numbers by modifying the *Systemroot*\System32\Drivers\Etc\Services file or by modifying their values in the Registry. The setting in the Services file takes precedence over the Registry setting in all cases. By changing the Services file or the Registry, you affect only the Gopher server.

Note By changing the port number, you can break some or all of your tags and links. You must rebuild these by using the **-p** option of the **gdsset** command to change the port number. For example, if you change the port number to 2345, you rebuild the new tag by typing the following line:

gdsset -c -g0 -f "The Mission of this Gopher Site" Readme1.Txt -p2345

▷ To change the Gopher port in the Services file

1. At a command prompt, change directories to *Systemroot*\System32\Drivers\Etc.
2. Use a text editor to search the Services file for the following entry.

```
gopher          70/tcp
```

3. Modify port 70 to a number greater than 1023 and add a comment (#) to show the default. For example, if you change to port 2345, add the following line.

```
gopher          2345/tcp        #  gopher      70/tcp
```

4. Save and close the file.
5. To implement the change, stop then restart the Gopher service.

Note This affects the default ports on the Gopher server.

Your Gopher server now waits at port 2345 for all Gopher client requests.

▷ To verify the new Gopher port settings

1. Start Internet Explorer. In the address box, type **gopher://127.0.0.1** and then press ENTER.

   The following message appears.

```
The attempt to load 'gopher:127.0.0.1' failed.
```

2. Click **OK** to dismiss the message.
3. In the address box, type **gopher://127.0.0.1:2345** and then press ENTER.

   The Gopher menu appears on your screen.

▷ To change the Registry entry for Gopher

1. Start the Registry Editor, **Regedt32.exe.**
2. Click the HKEY_LOCAL_MACHINE window and locate the following key.

```
\System
 \CurrentControlSet
  \Control
   \ServiceProvider
    \ServiceTypes
     \GOPHERSVC
```

3. Click GOPHERSVC and then double-click the **TcpPort** value.

   The **DWORD Editor** dialog box appears.

4. Click **Decimal** and enter **6789** in the **Data** box.
5. Click **OK** and close the Registry Editor.
6. At the command prompt, type the following information:

   ```
   cd %systemroot%\system32\drivers\etc
   ren services services.ok
   ```

   This step prevents the Gopher server from using the port address in the Services file after it has been restarted.
7. To implement the change, stop and restart the Gopher server.

   Note This affects the default port only on the Gopher server.

Your Gopher server now monitors port 6789 for all Gopher client requests and your Gopher client connects to a Gopher server at port 6789 only.

▷ To verify the new Gopher port settings

1. Start Internet Explorer. In the address box, type **gopher://127.0.0.1** and then press ENTER.

   The following message appears.

   ```
   The attempt to load 'gopher:127.0.0.1' failed.
   ```

2. Click **OK** to dismiss the message.
3. In the address box, type **gopher://127.0.0.1:6789** and then press ENTER.

   The Gopher menu appears.

Monitoring Gopher Sessions

You can monitor Gopher sessions by using the Performance Monitor and, to a lesser extent, **netstat**.

The **netstat** utility can be difficult to use with Gopher because Gopher sessions are very short and you cannot always activate **netstat** in time to receive any meaningful data. **Netstat** shows static information at a given point in time. **Netstat** is best used to determine the status of connections.

You can run **netstat** from a command prompt. For an explanation of **netstat** command syntax, see Table 1.4, earlier in this chapter.

Performance Monitor shows events happening in real time. Performance Monitor is best used to check the status of users, file transfers, and byte transfers. For a listing of real-time statistics displayed by Performance Monitor for Gopher, see Table 1.5, earlier in this chapter.

CHAPTER 2

Connecting Windows NT Server to the Internet

In the near future, it might be as common and simple to connect to the worldwide Internet as it is to connect to the worldwide telephone system. However, it is now a complex endeavor to connect servers or networks to the Internet. This chapter presents an overview of the concepts you use in connecting a server or network to the Internet. The chapter explains:

- The basic process of connecting a server to the Internet.
- Typical requirements for the server.
- Where to find more detailed information about procedures.
- Example network scenarios for connecting a computer or network to the Internet.

You can find extensive information on these topics by searching the Internet itself. It is recommended you seek resources on the Internet for more information on any topic. In addition, Table 2.1 lists references you can find in the Windows NT documentation and in the *Microsoft Windows NT Server Resource Kit*, version 4.0.

Table 2.1 Additional Information about Using Windows NT on the Internet

For information about	See
Connecting to the Internet as a client	*Microsoft Windows NT Workstation Resource Kit: Windows NT Workstation Resource Guide*
NetBIOS names	*Windows NT Server Networking Supplement* and *Microsoft Windows NT Server Resource Kit: Windows NT Server Networking Guide*
TCP/IP networking, including IP addresses and subnet masks, and DHCP and WINS servers	*Windows NT Server Networking Supplement* and *Microsoft Windows NT ServerResource Kit: Windows NT Server Networking Guide*
Securing a server on the Internet	*Windows NT Server Internet Guide*, Chapter 3, "Server Security on the Internet"

Table 2.1 Additional Information about Using Windows NT on the Internet *(Continued)*

For information about	See
Creating Internet Information Server sites	*Windows NT Server Internet Guide*, Chapter 4, "Desktop Scenarios," and Chapter 5, "Enterprise Scenarios"
Specific Internet server services or client applications included in the *Windows NT Server Resource Kit*	*Windows NT Server Internet Guide*, Chapter 7, "Internet Tools"
Troubleshooting Internet Information Server	*Windows NT Server Internet Guide*, Chapter 8, "Troubleshooting an Internet Information Server Installation"

Establishing an Internet Connection

You must establish an Internet connection to enable worldwide access to your site. Before you establish an Internet connection, you should:

- Understand your network and how TCP/IP operates.
- Select an Internet service provider (ISP) and determine what Internet services you will use.

This section explains network protocols and intranets, the formal requirements and procedures for participating in the Internet, Internet service providers, and how to choose the right connection.

When you connect a computer to the Internet, you must do a thorough security review and implement measures to protect your computer and network (if the computer is also connected to a private network) from intruders. For more information about securing computers and networks connected to the Internet, see Chapter 3, "Server Security on the Internet."

Network Protocols and Intranets

The Internet is a group of interconnected networks. When you create an Internet server, you are adding another network to the network of networks. The network you add to the Internet can be one computer, a small workgroup, or your entire corporation's local area network.

Network protocols are similar to language. Languages have different words, word patterns, and punctuation. A network protocol serves a similar role for computers attempting to communicate. The network protocol used on a network determines how *packets* (units of data) are configured and sent over the network cable. For more information about network protocols, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

The Internet primarily uses the TCP/IP (Transmission Control Protocol/Internet Protocol) network protocol. That means your computer must use the TCP/IP network protocol to participate. (TCP/IP is actually a suite of protocols. Internet Protocol is one of the protocols in the suite of protocols.) You can install TCP/IP during or after installation of Windows NT.

If you use TCP/IP on your internal network, as shown in Figure 2.1, your computer can act as a gateway to the Internet. By configuring Windows NT as a TCP/IP router you can pass packets of information in both directions—to the Internet from the intranet, and from the Internet into your intranet.

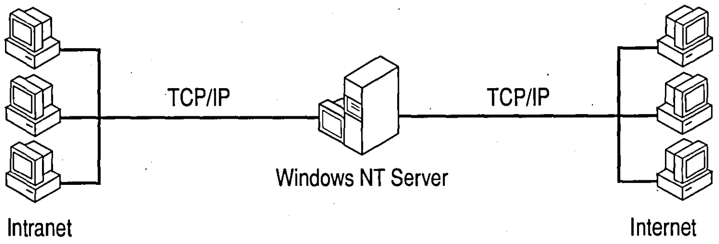


Figure 2.1 Windows NT–based computer connected to two networks

For more information about TCP/IP and the routing capabilities in Windows NT Server, see the *Windows NT Server Networking Supplement*, the *Windows NT Server Networking Guide*, and Chapter 3 in this book, "Server Security on the Internet."

IP Addresses and Domain Names

Each computer on the Internet has a unique address (the *IP address*). An IP address is in the form of four period-delimited octets consisting of up to 12 numerals—such as 172.16.16.189. Information is transmitted on the Internet in data packets. Each packet is addressed to a specific computer's IP address.

Because IP addresses are difficult to remember, the Domain Name System (DNS) was created for the Internet to pair a specific IP address, such as 172.16.16.189, with a "friendly" domain name, such as microsoft.com. When you use a domain name in an Internet browser, the browser first must contact a DNS server to resolve the domain name to an IP address, then contact the computer with that address.

This has two implications for your server running Internet Information Server (IIS server):

- You must have a permanent IP address assigned to a server on the Internet.
- You must register a domain name in the Domain Name System for your permanent IP address.

To establish a World Wide Web (WWW) server, you need a permanent IP address. To connect a TCP/IP network to the Internet, you need a valid IP address for each computer or device you want to be accessible from the Internet.

You must use a domain name if you want Internet users to be able to reach your Internet server or servers by the friendly domain name, such as microsoft.com. Both a registered domain name and an IP address are required for your Internet service to be seen and used by others on the Internet.

Most Internet service providers assign your IP addresses and can also register your domain names. Contact the Internet Network Information Center (InterNIC) or your ISP for more information about DNS registration.

To contact the InterNIC to register domain names and obtain IP addresses, connect to the Internet address **http://internic.net**.

If you must apply for your own domain name or IP addresses, you must have a good understanding of DNS and of TCP/IP networking. For more information about DNS and TCP/IP networking, see the *Windows NT Server Networking Supplement* and *Windows NT Server Networking Guide*.

Internet Service and Providers

You establish a connection to the Internet by leasing a line from an Internet service provider (ISP) or a telephone company. Your provider installs a cable at your site that is plugged into the network interface card (NIC) in your computer. Usually, a router is also installed between your computer and the ISP.

The services available on the Internet vary widely. The basic services required by Internet clients and servers are:

- An Internet gateway (default gateway).
- IP addresses and subnet mask.

An Internet service provider must provide the required services and often provides optional Internet services, such as DNS name resolution, domain name registration, electronic mail, and Internet news.

It is important to note that not all ISPs are alike; you need to find out their capabilities. Some questions to ask an ISP can include:

- How are you connected to the Internet (backbone)? (For example, a T1, multiple T1s, or a T3 connection.)
- What type of dedicated access do you offer? (For example, Frame Relay or shared T1.) Do you guarantee a minimum bandwidth?
- Do you offer dial-up access to allow connections through telephone modems?
- Do you offer Integrated Services Digital Network (ISDN) access?
- What type of security do you offer?
- What are your installation costs for each type of connection?
- What are your monthly costs for each type of connection?

Internet service providers are local, regional, or national providers. Local ISPs are connected to the Internet through larger ISPs or through a regional network. Local ISPs usually have only one location. The larger regional and national ISPs have multiple locations. If your site has enough traffic to require a high-speed T3 line (45 megabits per second) to your ISP, consider connecting directly to a regional network.

Regional networks are sites selected by the National Science Foundation (NSF) to provide a common connection point to the Internet. Regional networks connect to other regional networks at 155 megabits per second through a backbone carrier—such as US Sprint, MCI MAIL, or AT&T.

Companies that require a large bandwidth for their Internet sites can connect directly to a regional network. Requirements vary by regional network provider, but usually a T3 line is the minimum bandwidth of a connection. For more details, contact the vendor who operates your local regional network.

The Microsoft Network (MSN™) is an Internet service provider. You can find other Internet service providers listed in your local phone book (usually under "computer network services"). Internet service providers also frequently advertise in local newspapers or computer magazines.

How to Choose the Right Internet Connection

You connect to the Internet through a network adapter card or other network device, such as a modem or ISDN card. Internet bandwidth is measured in bits per second (bps).

Your Internet bandwidth determines how fast data gets to your computer and also how many requests can be serviced simultaneously. As more computers get data through your Internet connection simultaneously, delays or failures can occur if you do not have enough bandwidth.

When you lease an Internet connection, your ISP installs a network cable to your site. Leased connection speeds range from 56,000 bps (or 56 kilobytes per second) with Frame Relay to 45,000,000 bps (or 45 megabytes per second) with a T3 connection. A dial-up ISDN line can offer speeds up to 128,000 bps (or 128 kilobytes per second).

The connection types described in Table 2.2 represent typical levels of service for full Internet connections in North America and Japan. The Internet services offered through Internet service providers in your country might differ significantly.

Table 2.2 Common Internet Service Connection Types

Connection type	Maximum bandwidth	Approximate number of users supported
Dedicated PPP/SLIP	Modem speed	2-3
56K (Frame Relay)	56,000 bps	10-20
ISDN (using PPP)	128,000 bps	10-50
T1	1,540,000 bps	100-500
Fractional T1	Varies as needed	Varies as needed
T3	45,000,000 bps	5,000+

To understand these speeds in practical terms, assume a page of text is 42,240 bits. (One character is 8 bits. Therefore, 8 bits x 80 characters in a line x 66 lines per page = 42,240 bits per page.) A 28.8 Kbps modem can transfer .67 pages per second. A 128,000 bps ISDN line can transfer three pages per second. A 1,500,000 bps T1 line can transfer 35.5 pages per second.

For example, a light-duty server can use a 56 Kbps link or ISDN. A server with medium traffic might have a T1 line or some fraction of a T1 line installed. Large businesses that expect heavy Internet traffic might need fractional or multiple T1 lines or even T3 service in order to handle thousands of users.

Modem connections to the Internet are available, but are typically used for individual client browsing and are not recommended for servers. A connection to the Internet that uses a phone line and modem can service only two or three users simultaneously. (Modem connections might be used for text-only Internet servers with only a small number of potential users.) Modem connections are often called "slow links" because data is transmitted at the speed of the modem, typically from 9600 to 28,800 bps. This is far too slow for efficient operation of a World Wide Web server, for example.

Selecting Hardware and Software to Run Internet Information Server

Many variables influence hardware and software selection. The guidelines and case studies in this section are presented to help you determine the best choices for your situation.

Internet Information Server Hardware Guidelines

The type of processor and the amount of RAM you choose for your system can affect the performance of your server. For example, in laboratory conditions an 80486DX/50 computer with 52 MB of RAM running Microsoft Windows NT Server and Internet Information Server can handle more than 100 simultaneous users or sessions.

The number of simultaneous users your server can handle varies according to the type of session that is open and other factors. A server is able to accommodate more users when they are running sessions that are not processor-intensive, such as electronic mail (e-mail), Telnet, and FTP. Sessions that are processor-intensive include those that run Common Gateway Interface (CGI) scripts, make database queries, and download Hypertext Markup Language (HTML) files.

Table 2.3 lists the minimum and recommended hardware needed to run Microsoft Windows NT Server 4.0 and Internet Information Server.

Table 2.3 Hardware Requirements and Recommendations

Hardware requirement	Minimum	Recommended
Processor	50 MHz 486	90 MHz Pentium®
RAM	16 MB	32 to 64 MB
Free hard disk space	50	200
Monitor	VGA	Super VGA
CD-ROM drive	3X	6X

RAM

The amount of RAM needed by your server is dependent on a number of factors, including:

- The number of simultaneous users.
- The number of Hypertext Transfer Protocol (HTTP) users (high memory use) versus Gopher and FTP users (lower memory use).
- The amount of RAM used for cache.

- The size of swap file.
- The amount of free disk space.
- The amount of RAM used for video.
- The number of services running.
- The type of processor.
- The SQL database searches.

Taking into consideration all of these variables, a general guideline is to allow about 256K of RAM per simultaneous user.

www.microsoft.com

The Web site for Microsoft, www.microsoft.com, handles three million requests a day. In a 24-hour time period, this averages more than 2,000 hits per minute.

The www.microsoft.com Web site consists of two computers running Internet Information Server on Microsoft Windows NT Server. Each computer has multiple 66-MHz Intel Pentium processors, 8 GB of usable hard disk space, and 128 MB of RAM. One computer uses four Pentium processors and the other uses two.

Internet Information Server Software Requirements

Internet Information Server runs on Windows NT Server 4.0. You should install the latest service pack. Windows NT 4.0 service packs are available through The Microsoft Network (MSN), CompuServe, and on the Internet at **http://www.microsoft.com**.

Table 2.4 shows a typical software configuration for your Internet server.

Table 2.4 Software Requirements and Recommendations

Software	Description
Operating system	Windows NT Server 4.0 or later, with the latest service pack
Server software	Internet Information Server (included with Windows NT Server 4.0)
HTML creation	Microsoft Word for Windows® 95 and Microsoft Internet Assistant for Word

Internet Networking Scenarios

This section describes Internet and intranet scenarios that use Windows NT Server. The components used on the Internet or to connect to the Internet are identified and explained. The components are applied to Internet scenarios. And finally, an intranet is defined and scenarios for connecting your intranet to the Internet are illustrated.

Networking Software for the Internet

Windows NT Server provides all the networking software necessary to connect an information server or network to the Internet. The Windows NT software used is defined in Table 2.5.

Table 2.5 Networking Software Used for Connecting to the Internet

Windows NT software component	Function
Infrastructure	
TCP/IP protocol	Is required to communicate with other computers on the Internet.
DHCP server	Dynamically assigns TCP/IP configuration to computers on a network.
WINS server	Provides name resolution for NetBIOS names.
DNS server	Provides name resolution for Domain Name System names.
HOSTS file	Provides name resolution for DNS names.
LMHOSTS file	Provides name resolution for NetBIOS names.
Connectivity	
Remote Access Service	Enables incoming connections from remote clients that are using Dial-Up Networking or other PPP or Serial Line Internet Protocol (SLIP) dial-up software.
Dial-Up Networking	Provides low-speed connections to the Internet. Primarily used by clients connecting to a Remote Access Service server or Internet service provider.
RIP (routing information protocol) for Internet Protocol	Provides routing for high-speed connections to the Internet (or other networks). Primarily used on small to medium-size networks.
Publishing	
Internet Information Server	Enables file and application sharing by using the HTTP, FTP, and Gopher protocols. Requires a computer running Windows NT Server.
Peer Web Services	Enables file and application sharing by using the HTTP, FTP, and Gopher protocols. Requires a computer running Windows NT Workstation.
Internet Explorer	Enables access to shared files and applications by using Internet protocols.

To complement these primary tools, you can also use tools in the *Windows NT Resource Kit* (see Chapter 7, "Internet Tools"), public domain programs available on the Internet, or commercial products that include more features and technical support.

You also need a connection to the Internet. Depending on your needs, the connection can be a 28.8 Kbps modem and dial-in Point-to-Point Protocol (PPP) account, or a dedicated high-volume line supplied by an Internet service provider for an Internet server or providing an Internet gateway for an intranet.

For information about	See
The physical connection to the Internet	"Establishing an Internet Connection," earlier in this chapter
The Internet tools in this Resource Kit	Chapter 7, "Internet Tools"

Using Windows NT Server on the Internet

This section explains typical Internet scenarios with Windows NT Server .

Internet Client

The simplest way to connect to the Internet is as a client. As a client you use Internet Explorer or other tools to search for information.

This configuration allows outbound traffic to the Internet only, as illustrated in Figure 2.2. (For more information about client connections to the Internet, see the *Windows NT Workstation Resource Guide*, Chapter 35, "Using Windows NT Workstation on the Internet.")

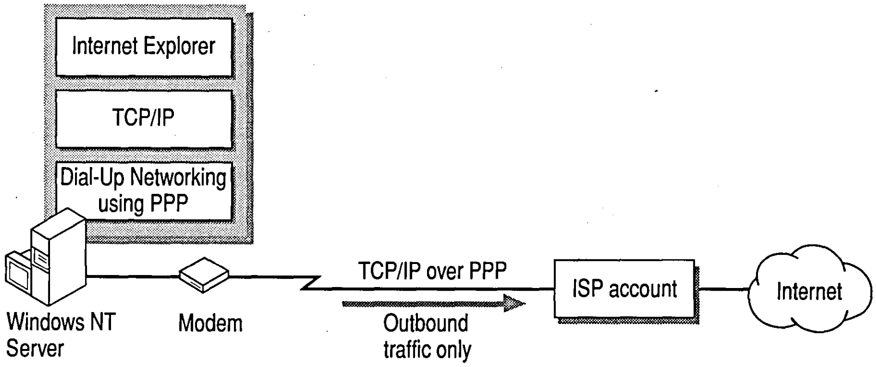


Figure 2.2 Windows NT as Internet client

In this scenario, the computer running Windows NT Server (or Windows NT Workstation) uses Dial-Up Networking and a modem to connect to an Internet service provider. After successful connection to the Internet service provider, the user can start and use any TCP/IP–based applications, such as Internet Explorer or the command-prompt FTP client.

For this type of scenario, you need to install and configure the following hardware or services:

- Internet client tools, such as Internet Explorer, FTP, or Telnet
- TCP/IP networking protocol
- Dial-Up Networking
- A modem
- PPP or SLIP dial-in account to an Internet service provider

Internet Web Server

Expanding the preceding configuration, you ~~can~~ create two-way communication with the Internet as illustrated in Figure 2.3.

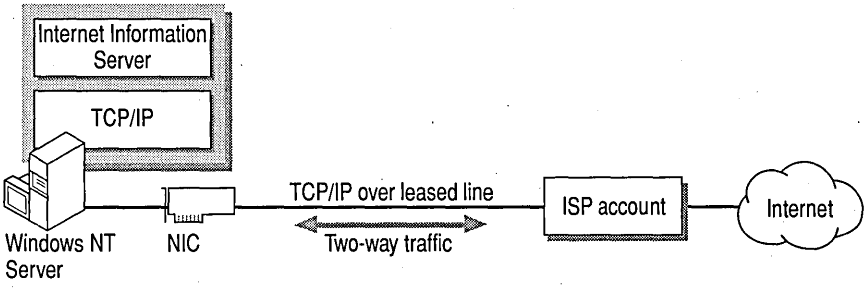


Figure 2.3 Windows NT Internet Information Server and client

In this scenario, the computer running Windows NT Server has a leased line to an Internet service provider. You install Internet Information Server and make information available to remote users on the Internet. In addition, the computer running Windows NT Server can use any TCP/IP–based applications, such as Internet Explorer or the command-prompt FTP client.

For this scenario, you need to install and configure the following hardware or services:

- Internet Information Server
- TCP/IP networking protocol
- Network interface card
- Leased line to an Internet service provider
- Domain name registration, as described in the section, "Establishing an Internet Connection"

For more information about Internet servers, see Chapter 4, "Desktop Scenarios," and Chapter 5, "Enterprise Scenarios."

Note Security becomes an important issue when you are connected to the Internet. This section describes only basic Internet scenarios. Many options that are not mentioned in this chapter exist to protect your computer or intranet from external intruders. For more information on security, see Chapter 3, "Server Security on the Internet."

Using Windows NT Server on an Intranet

An *intranet* is a private local area network that uses Internet technology. The functions on an intranet are identical to the functions on the Internet. You can install Internet Information Server on any computer on your intranet that runs Windows NT Server, and it can be accessed by Internet Explorer or any other client that supports the HTTP, FTP, and Gopher protocols.

To operate on an intranet, you need to provide a networkwide name resolution system by using WINS servers, DNS servers, or a HOSTS or LMHOSTS file. (For more information about using HOSTS and LMHOSTS for name resolution in an Internet scenario, see Chapter 5, "Enterprise Scenarios." For more information on using HOST and LMHOSTS in general, see the *Windows NT Server Networking Supplement.*)

Heterogeneous clients can use all the resources on your network, such as Internet Information Server, databases, DHCP servers, and WINS servers, as shown in Figure 2.4.

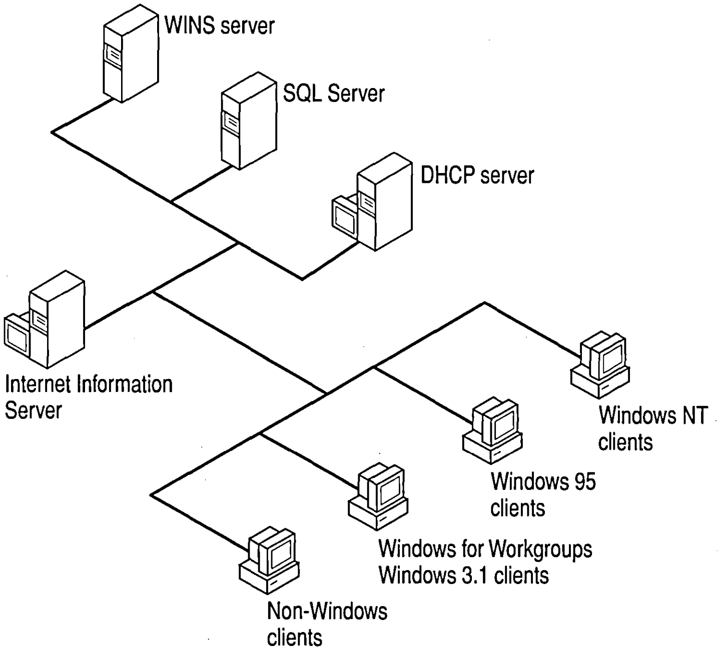


Figure 2.4 Typical intranet components

In this scenario, you install Internet Information Server and make information available to local users on the network.

For any intranet scenario, you need to install and configure the following hardware or services:

- A computer running Internet Information Server
- TCP/IP networking protocol on every computer that will use the IIS server
- Network interface cards on all computers
- An Internet browser, such as Internet Explorer, on every computer that will access the IIS server
- Domain name resolution, as described in the section, "Establishing an Internet Connection"

Connecting Your Intranet to the Internet

You can configure your network to allow intranet clients to be able to access the Internet. You create two-way communication with the Internet by configuring Windows NT and configuring RIP for Internet Protocol routing as shown in Figure 2.5.

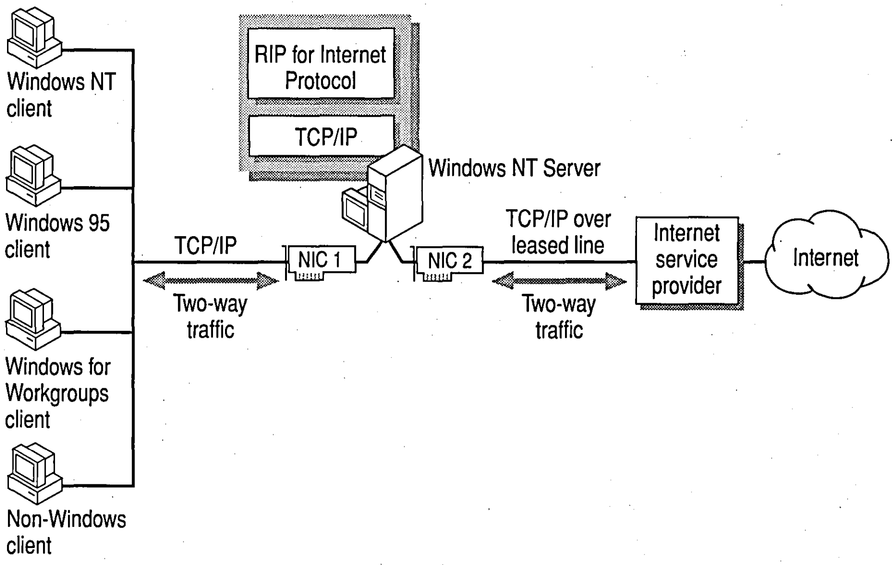


Figure 2.5 Intranet access to the Internet by using Windows NT

In this scenario, the computer running Windows NT Server has a leased line to an Internet service provider. The RIP for Internet Protocol service is installed. An Internet service provider router uses the routing information protocol (RIP) to communicate with the computer running Windows NT Server RIP for Internet Protocol service. By using RIP, the Internet service provider's router learns the IP address of all computers on the private network. This enables traffic from the Internet to be routed to computers on the private network, and traffic from private network computers to be routed to the Internet.

For this scenario, you need to install and configure the following hardware or services:

- A computer running the RIP for Internet Protocol service
- TCP/IP networking protocol on every computer that will use the Internet
- Network interface cards on all computers
- An Internet browser, such as Internet Explorer, on every computer that will access the Internet
- Internet-wide domain name resolution, as described in the section, "Establishing an Internet Connection"

For more information about the RIP for Internet Protocol service (part of Windows NT Server multiprotocol routing functionality), see the *Windows NT Server Networking Supplement* and *Windows NT Server Networking Guide.*

Connecting Intranet Clients to the Internet with Remote Access Service

The Windows NT Server Remote Access Service (RAS) can be added to the above configuration to provide remote clients with an Internet gateway. This type of configuration expands your intranet configuration as illustrated in Figure 2.6.

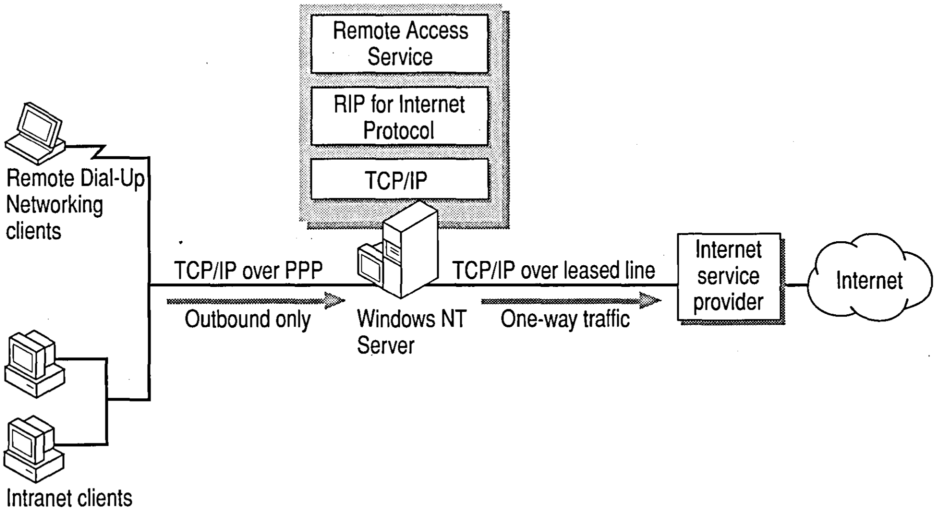


Figure 2.6 Remote client Internet gateway

In this scenario, the computer running Windows NT Server has a leased line to an Internet service provider. The RIP for Internet Protocol service and Remote Access Service are installed on this server. An Internet service provider router uses the routing information protocol to communicate with the computer running Windows NT Server RIP for Internet Protocol service. By using RIP, the Internet service provider's router learns the IP address of all computers on the private network. This enables traffic from the Internet to be routed to computers on the private network, and traffic from private network computers to be routed to the Internet.

By using the Remote Access Service, Windows Dial-Up Networking clients or other dial-up clients can connect to the RAS server and the local network. Because the RIP for Internet Protocol service is also on the network and routes packets to and from the Internet, remote clients also have access to the Internet. Thus, local network clients and remote RAS clients can use the local network and the Internet.

For this scenario, you need to install and configure the following hardware or services:

- A computer running the RIP for Internet Protocol service and the Remote Access Service
- TCP/IP networking protocol on every computer that will use the Internet
- A multiport adapter, which allows multiple remote clients to dial in to the computer running RAS
- Network interface cards on all computers
- An Internet browser, such as Internet Explorer, on every computer that will access the Internet
- Dial-Up Networking on remote clients that will dial in to the RAS server
- Internet-wide domain name resolution, as described in the section, "Establishing an Internet Connection"

For more information about the RIP for Internet Protocol service and the Remote Access Service, see the *Windows NT Server Networking Supplement* and *Windows NT Server Networking Guide.*

On a small intranet (that is, an intranet with less than 20 computers), the RAS server can use Dial-Up Networking, simple TCP/IP routing, and a PPP connection to its Internet service provider in place of a leased line and the RIP for Internet Protocol service. In this configuration you can connect both intranet clients and remote Dial-Up Networking clients to the Internet, as shown in Figure 2.7.

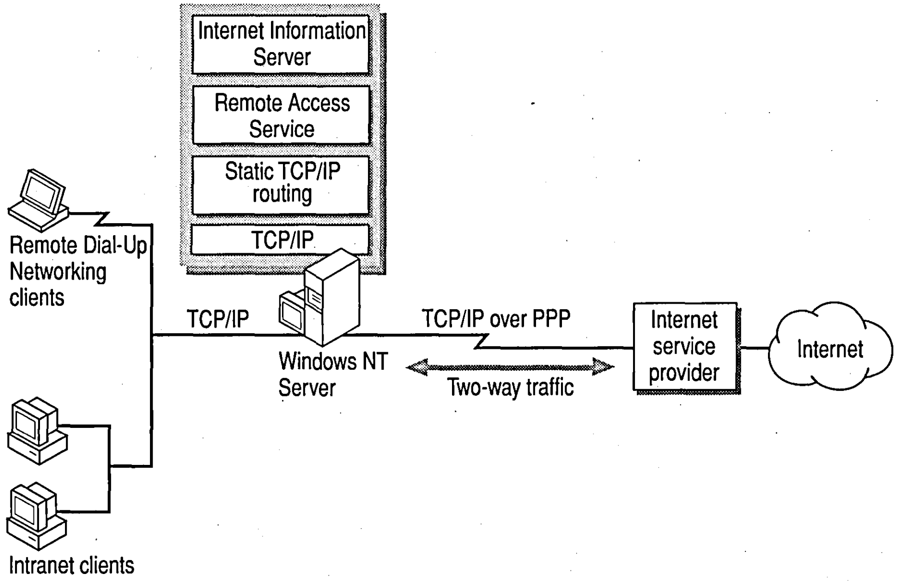


Figure 2.7 Internet gateway for a small intranet with remote clients

In this scenario, the computer running Windows NT Server has a Dial-Up Networking connection to an Internet service provider. Simple TCP/IP routing is enabled, and a static routing table is created for the computers on the private network. You must also provide routing information to the Internet service provider because simple TCP/IP routing does not use the routing information protocol to communicate with the Internet service provider's router. The routing information you supply enables the routing of Internet traffic to and from the computers on the private network.

The Remote Access Service, installed on the server, accepts incoming calls from remote clients that use Dial-Up Networking or other dial-up client software. The Remote Access Service enables Windows Dial-Up Networking clients or other dial-up clients to connect to the RAS server and the local network. This configuration can also support a light-duty IIS server.

For this scenario, you need to install and configure the following hardware or services:

- A computer running simple TCP/IP routing and a static routing table
- TCP/IP networking protocol on every computer that will use the Internet
- The Remote Access Service
- A multiport adapter, which allows multiple remote clients to dial in to the computer running Remote Access Service
- Network interface cards on all computers
- An Internet browser, such as Internet Explorer, on every computer that will access the Internet
- Dial-Up Networking on remote clients that will dial in to the RAS server
- Internet-wide domain name resolution, as described in the section, "Establishing an Internet Connection"

For more information about simple TCP/IP routing and the Remote Access Service, see the *Windows NT Server Networking Supplement* and *Windows NT Server Networking Guide*.

For more information about creating an Internet gateway, see Chapter 6, "Internet Connectivity Scenarios Using the Remote Access Service."

CHAPTER 3

Server Security on the Internet

You must provide a secure base to use Internet Information Server (IIS) and participate in the Internet. In this chapter, security refers to providing selective access to documents through Internet Information Server and preventing Internet users from maliciously tampering with your intranet.

This chapter presents:

- Authentication and security controls in Internet Information Server.
- Scenarios for connecting an intranet to the Internet.
- Suggestions on using monitoring tools to detect, monitor, and prevent security breaches.

For information about	See
Windows NT security	*Windows NT Server Concepts and Planning* or the *Microsoft Windows NT Workstation Resource Kit: Windows NT Workstation Resource Guide*
Windows NT security integration with Internet Information Server	Windows NT Server *Microsoft Internet Information Server Installation and Administration Guide* online HTML book, Chapter 6, "Securing Your Site Against Intruders"

Note The *Microsoft Windows NT Administrator's Security Guide* gives you the information you need to set up your Windows NT–based system to be eligible for C2-level security certification. Along with general topics on high-security installations for system administrators, the *Administrator's Security Guide* contains the "Microsoft Report on C2 Evaluation of Windows NT," which describes the evaluation process and gives directions for duplicating the computer systems that were evaluated by the National Computer Security Center (NCSC).

The NCSC evaluated version 3.5 of the Windows NT operating systems, but you will need the information in *Administrator's Guide* as well as the resource kits for version 4.0 of Windows NT Server and Windows NT Workstation when setting up a system for C2 certification.

Internet Information Server Authentication

Internet Information Server enables you to control access to your information site by using Windows NT user accounts. The following sections describe:

- The user account created by Internet Information Server.
- The effect of a server's role on the IUSR_*computername* account and the effect of domain-based security on user accounts used by Internet Information Server.
- Typical security scenarios for intranet and Internet sites that use Internet Information Server. The security scenarios include anonymous access, Basic authentication, and Windows NT challenge/response (secure) authentication.

Domain Accounts and Local Accounts

During installation, Internet Information Server creates IUSR_*computername*, a standard user account, as the user name for all anonymous access. A random password is generated for IUSR_*computername*. Just like any user account, the account is added to the local or domain directory database and can be modified by using User Manager.

The role of a server—as a primary domain controller (PDC), backup domain controller (BDC), or stand-alone server—influences how IUSR_*computername* user accounts are created and used by Internet Information Server.

If Internet Information Server is installed on a primary domain controller or backup domain controller, the IIS server user account is automatically added to the domain directory services database. All computers in that domain have access to validated users listed in the domain directory services database. The IUSR_*computername* account automatically becomes a domainwide account and can access resources across the domain.

If Internet Information Server is installed on a stand-alone member server, the IUSR_*computername* account is a local account. Computers in its domain cannot validate user accounts created on the stand-alone server. To enable access to resources on other servers in the domain if you have installed Internet Information Server on a stand-alone member server, change the default IUSR_*computername* account to an account with domainwide permissions.

The server role of the computer on which Internet Information Server is installed affects the authority of the IUSR_*computername* account created during setup. Table 3.1 summarizes these effects.

Table 3.1 Effect of Server Role on IUSR_*computername* Account Authority

Server role	Anonymous user account created	Account authority
Member server	*Local_computer*\IUSR_*computername*	Local only
BDC	*Domain*\IUSR_*computername*	Domain
PDC	*Domain*\IUSR_*domainname*	Domain

Log On Locally User Right

You must use User Manager or User Manager for Domains to assign the Log On Locally user right to all accounts used for access by Internet Information Server. The accounts used by Internet Information Server include:

- The anonymous access account (the IUSR_*computername* account).
- The account specified when creating virtual directories.
- The accounts specified in .idc files for access to databases.
- The user accounts specified by clients.

Anonymous Access

Internet Information Server permits anonymous access in the WWW, FTP, and Gopher services by default. There are no differences between an anonymous intranet site and an anonymous Internet site.

But even when you use anonymous access, all activity on a system running Internet Information Server determines permissions by user name. Associating a user name with every action is fundamental to Windows NT security.

During installation, Internet Information Server creates IUSR_*computername*, a standard user account, as the user name for all anonymous access. A random password is generated for IUSR_*computername*. The account is added to the local directory services database on stand-alone systems or to the domain directory services database on primary or backup domain controllers. You modify this account by using User Manager.

Internet Explorer and most other Web browsers do not provide a user name and password when connecting to a Web server, so Internet Information Server uses the IUSR_*computername* account, as shown in Figure 3.1.

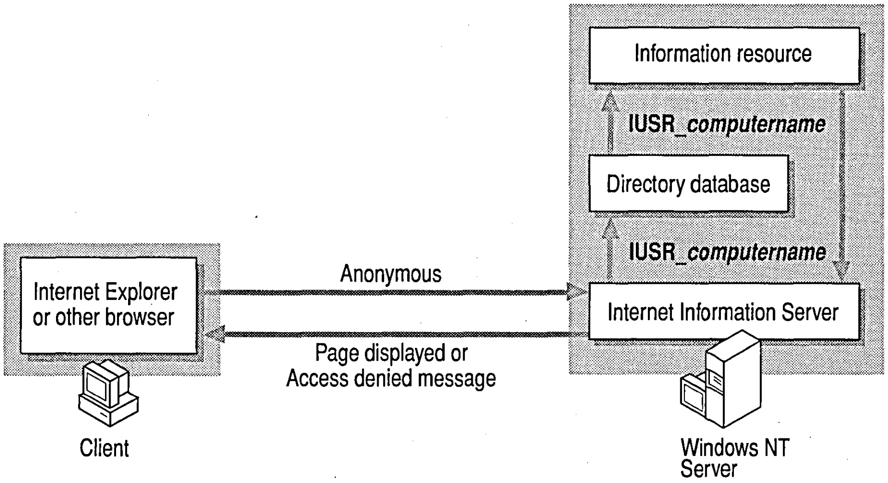
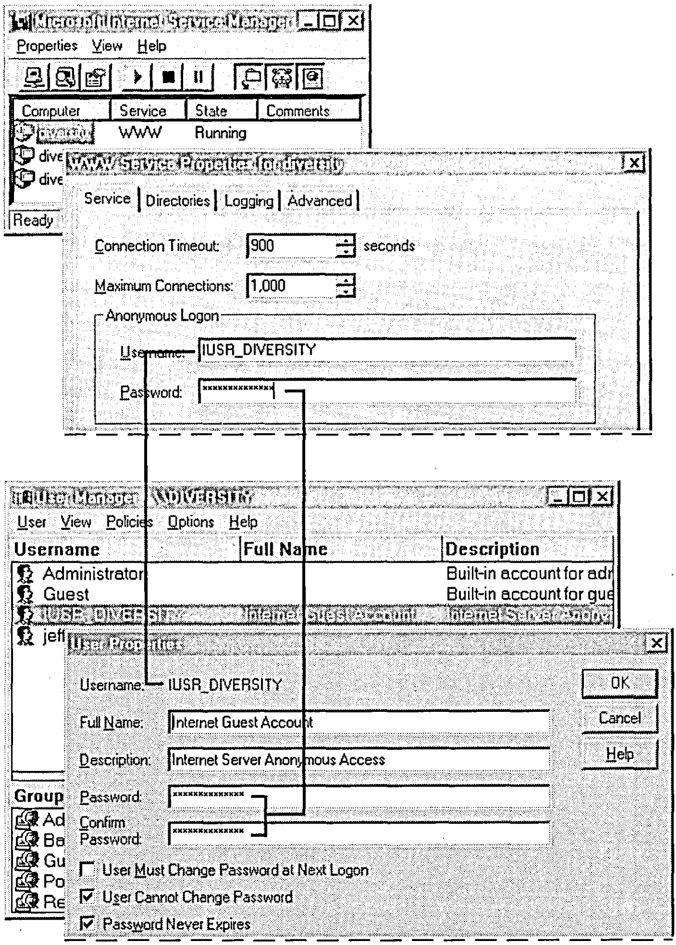


Figure 3.1 Anonymous access process

Anonymous access is enabled by default. You set anonymous access by using the **Service** property sheet for each service. The account information for the IUSR_*computername* or other account specified in the **Service** property sheet must also agree with the settings in User Manager for the same account, as shown in Figure 3.2. Users are denied access if the user name and password do not match.



Microsoft Internet Service Manager
Properties View Help
Computer Service State Comments
diversity WWW Running
dive
dive
Ready
WWW Service Properties for diversity
Service Directories Logging Advanced

Connection Timeout: 900 seconds

Maximum Connections: 1,000

Anonymous Logon

Username: IUSR_DIVERSITY

Password: **************

User Manager - \\DIVERSITY
User View Policies Options Help

Username	Full Name	Description
Administrator		Built-in account for adr
Guest		Built-in account for gue
IUSR_DIVERSITY	Internet Guest Account	Internet Server Anony
jeff		

Group
Ad
Ba
Gu
Po
Re
User Properties
OK
Cancel
Help

Username: IUSR_DIVERSITY

Full Name: Internet Guest Account

Description: Internet Server Anonymous Access

Password: **************

Confirm Password: **************

□ User Must Change Password at Next Logon

☑ User Cannot Change Password

☑ Password Never Expires

Figure 3.2 Matching user names and passwords in Internet Service Manager and User Manager

To provide *only* anonymous access—which is preferable for most installations—you clear the **Basic (clear text)** and **Windows NT Challenge/Response** boxes. If you provide anonymous access only, no one can use a Windows NT account maliciously. For example, anonymous-only settings prevent anyone from gaining access by using the Administrator account or any other account with sufficient permissions to alter your computer.

User Authentication

You can use Windows NT user accounts to control access to your entire server or to control access to certain files or directories. When the **Anonymous** check box on the **Service** property sheet is cleared, every initial request from a client causes an authentication dialog box to appear. If **Anonymous** is selected, and **Basic (clear text)** or **Windows NT Challenge/Response** is also selected, the user is prompted for a user name and password only if the user tries to gain access to a resource on a Windows NT File System (NTFS) drive and if that resource's properties do not allow the IUSR_*computername* account access.

Accounts used by Internet Information Server must be granted the Log On Locally user right—whether you specify that account in Internet Service Manager or the user supplies the user name and password. By default, user accounts on a Windows NT Server domain controller are not granted the Log On Locally user right. Be sure that any account on a domain controller that is used for access by Internet Information Server is granted the right to log on locally.

How you configure and use Windows NT user accounts is determined by the authentication method your clients support and whether you use authentication over your intranet or the Internet.

Intranet User Authentication

User authentication is easiest to use on an intranet with an existing Windows NT user account system. Because Internet Information Server uses Windows NT user accounts, you can use your network's existing accounts and domain structure, and administer the user accounts with the familiar User Manager. Figures 3.3 through 3.5 show Maria Gonzales (mariag) logging on by using her password (KamInop8).

If all of your clients run Internet Explorer version 2.0 or later, you can use Windows NT challenge/response authentication, which provides secure authentication, as illustrated in Figure 3.3. If you select **Windows NT Challenge/Response**, all requests from Internet Explorer version 2.0 or later use challenge/response authentication. All other browsers can connect only by using Basic authentication, and the **Basic** authentication check box must be selected.

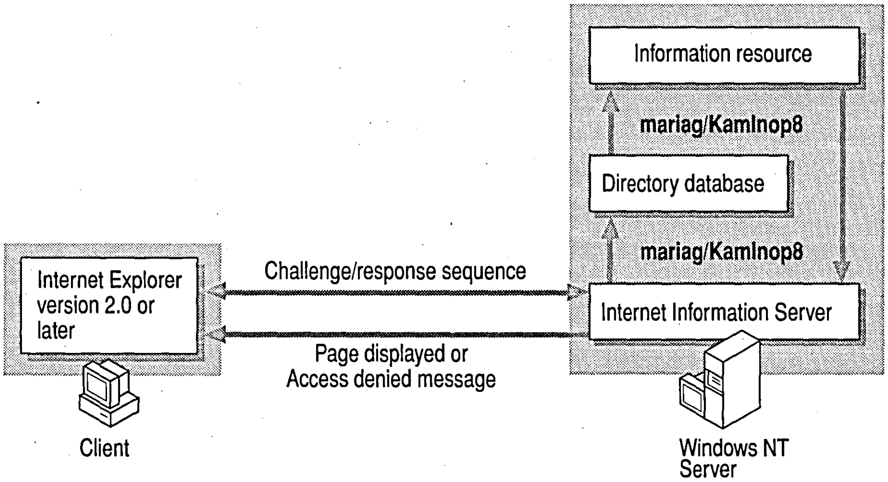

Information resource
mariag/Kamlnop8
Directory database
mariag/Kamlnop8
Internet Explorer version 2.0 or later
Challenge/response sequence
Internet Information Server
Page displayed or Access denied message
Client
Windows NT Server

Figure 3.3 Challenge/response process

Internet Explorer version 1.5 does not support Windows NT challenge/response authentication. If your clients run Internet Explorer version 1.5 or earlier, or any other Web browser (for example, Netscape Navigator), you cannot use challenge/response authentication. You can, however, use Basic (clear-text) authentication, as shown in Figure 3.4.

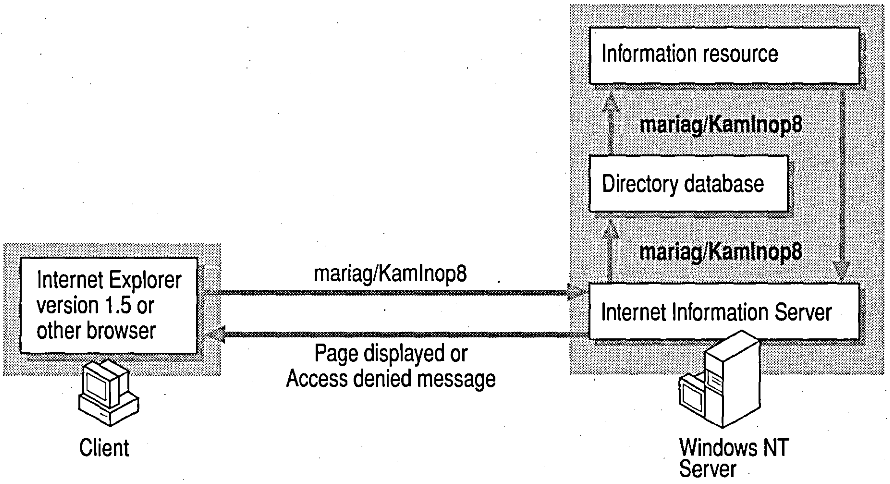

Information resource
mariag/Kamlnop8
Directory database
mariag/Kamlnop8
Internet Explorer version 1.5 or other browser
mariag/Kamlnop8
Internet Information Server
Page displayed or Access denied message
Client
Windows NT Server

Figure 3.4 Basic authentication process

Warning Basic (clear-text) authentication sends your Windows NT user name and password over the network unencrypted. User names and passwords sent by using Basic authentication can be learned and then used maliciously.

Basic authentication encodes the user name and password by using a base-64 algorithm—so it is not completely clear text. To intercept the user name and password, a network monitor must intercept the packet, then decode the packet containing the user name and password. With base-64 encoding, the user name or password can also contain characters that cannot be used inside a Hypertext Transport Protocol (HTTP) header.

If you are concerned about security on your intranet, you can use Basic authentication in conjunction with Secure Sockets Layer (SSL), as described in "Encrypting Private Data with SSL," later in this chapter. SSL encrypts the authentication process, as shown in Figure 3.5. However, in this scenario all transmissions are encrypted, which has a significant impact on server performance.

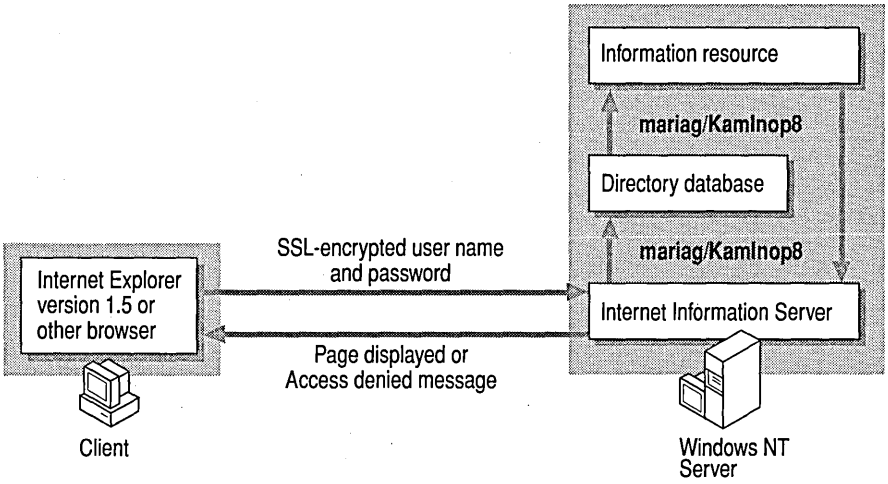

Information resource
mariag/Kamlnop8
Directory database
mariag/Kamlnop8
SSL-encrypted user name and password
Internet Explorer version 1.5 or other browser
Internet Information Server
Page displayed or Access denied message
Client
Windows NT Server

Figure 3.5 Basic SSL authentication process

Internet User Authentication

The principles just discussed in the intranet section apply to user authentication over the Internet. However, because you cannot assume everyone uses Internet Explorer version 2.0 or later to access your server, you must use Basic authentication in conjunction with SSL for secure authentication.

If you expect to create thousands of user accounts for clients on the Internet, you need to investigate the hardware requirements for maintaining a large number of user accounts. Table 3.2 outlines hardware requirements for domain controllers.

Table 3.2 Domain Controller Hardware Requirements

Approximate number of user accounts	User account database file size[1]	Minimum processor needed	Required RAM[2]
Up to 3,000	5 MB	486DX/33	32 MB
3,001-7,500	10 MB	486DX/66	32 MB
7,501-10,000	15 MB	Pentium, MIPS® Rx4000, Digital Alpha™	48 MB
10,001-15,000	20 MB	Pentium, MIPS Rx4000, Digital Alpha	64 MB
15,001-30,000	30 MB	Pentium, MIPS Rx4000, Digital Alpha	128 MB
30,001-40,000	40 MB	Pentium, MIPS Rx4000, Digital Alpha	166 MB

[1] User account numbers are approximate. The exact file size of the directory services database depends on the number of user accounts, machine accounts, and group accounts.

[2] RAM must be at least 2.5 times the size of the directory services database.

For more information about establishing large numbers of user accounts, see the white paper, *Microsoft Windows NT Server Domain Planning for Your Enterprise*, available on www.microsoft.com.

Encrypting Private Data with SSL

The Secure Sockets Layer protocol provides communications privacy over networks by using a combination of public key cryptography and bulk data encryption for data privacy. By using this protocol, clients and servers can communicate in a way that prevents eavesdropping, tampering, or message forgery.

Simplified Overview of SSL

Cryptography is a complex topic based on mathematics. To fully explain public key cryptography is outside the scope of this book. However, the following simplified explanation allows some basic understanding of SSL and public key cryptography. For more information about cryptography, consult the Internet or your local library.

Cryptographic keys are created at the same time in pairs: a public key and a private key. The public key is given to anyone (and is often made available though a public agency, such as a certificate authority). The private key is kept and safeguarded by you. Both keys are required for any exchange of information.

Internet Explorer encrypts data—such as a Hypertext Markup Language (HTML) form with private information—by using your server's public key. The encrypted data is sent to the server. The data is decrypted by the server, which uses its private key. The data can be decrypted only with the private key, held by the server.

Key Manager is used to generate the key pair and to activate the generated key. A key is not active until you send the certificate request file generated by Key Manager to your certificate authority.

For more information about using Key Manager, see the *Internet Information Server Installation and Administration Guide.*

Using SSL

Secure Sockets Layer is most effectively used by encrypting only communication that contains private data, such as credit card numbers, addresses, or company records. Because SSL uses your computer's processor to encrypt data, it takes much longer to retrieve and send data from SSL-enabled directories.

In your SSL-enabled directory, place only those pages that have or will receive sensitive information. Also, keep the content of pages in an SSL-enabled directory free from unnecessary elements because every item on the page will be encrypted, including simple graphics. Every element on the page increases the time it takes to transmit the data.

FTP Security

The File Transfer Protocol (FTP) is a legacy protocol. However, FTP remains a useful service because it can accept files from remote users or users of a different file system.

FTP Anonymous Access

FTP always uses user-level security, meaning the user must log on to gain access to the FTP server. The Internet Information Server FTP service can use the Windows NT user account database to authenticate users logging on. However, all FTP transmissions are in clear text, thus exposing user names and passwords.

The problem of exposed passwords is eliminated when an FTP server is configured to permit anonymous logons. Anonymous logon requires the user to type **anonymous** as their user name and their Internet e-mail address as their password. Anonymous users get access to files under the IUSR_*computername* account.

You can also allow anonymous-only logons to the Windows NT Internet Information Server FTP service. Anonymous-only logon is useful because it prevents real passwords from being revealed on a public network. FTP is configured for anonymous access by default.

For more information about configuring FTP for anonymous access, see the *Internet Information Server Installation and Administration Guide.*

Drop Box

You can create a drop box for your Internet customers to leave files in. The drop box must be on a drive formatted with NTFS. To create a drop box, right-click the folder that will become a drop box. Click **Properties**, click **Security**, and then click **Permissions**. Set the permissions for all users to write-only. After you have set write-only permissions, Internet users can put files in the drop box directory, but cannot see or copy any of the files left there. Only internal users with appropriate permissions can read the files.

Connecting Intranets to the Internet

Although you might want the users on your intranet to use the Internet, and want to give users from the Internet access to certain information, you probably do not want Internet users to have full access to your intranet.

When you connect an intranet to the Internet, you can use physical isolation, protocol isolation, third-party routers, and Windows NT routing in your network to provide security. The topology you choose affects the service you provide to intranet users.

Figure 3.6 illustrates the different network topology scenarios you can implement and how each scenario influences security and service for intranet users. The sections that follow in this chapter give more information about the benefits of each security topology illustrated in Figure 3.6. (Note that third-party Internet security devices and software are available, but are not discussed in detail in this chapter.)

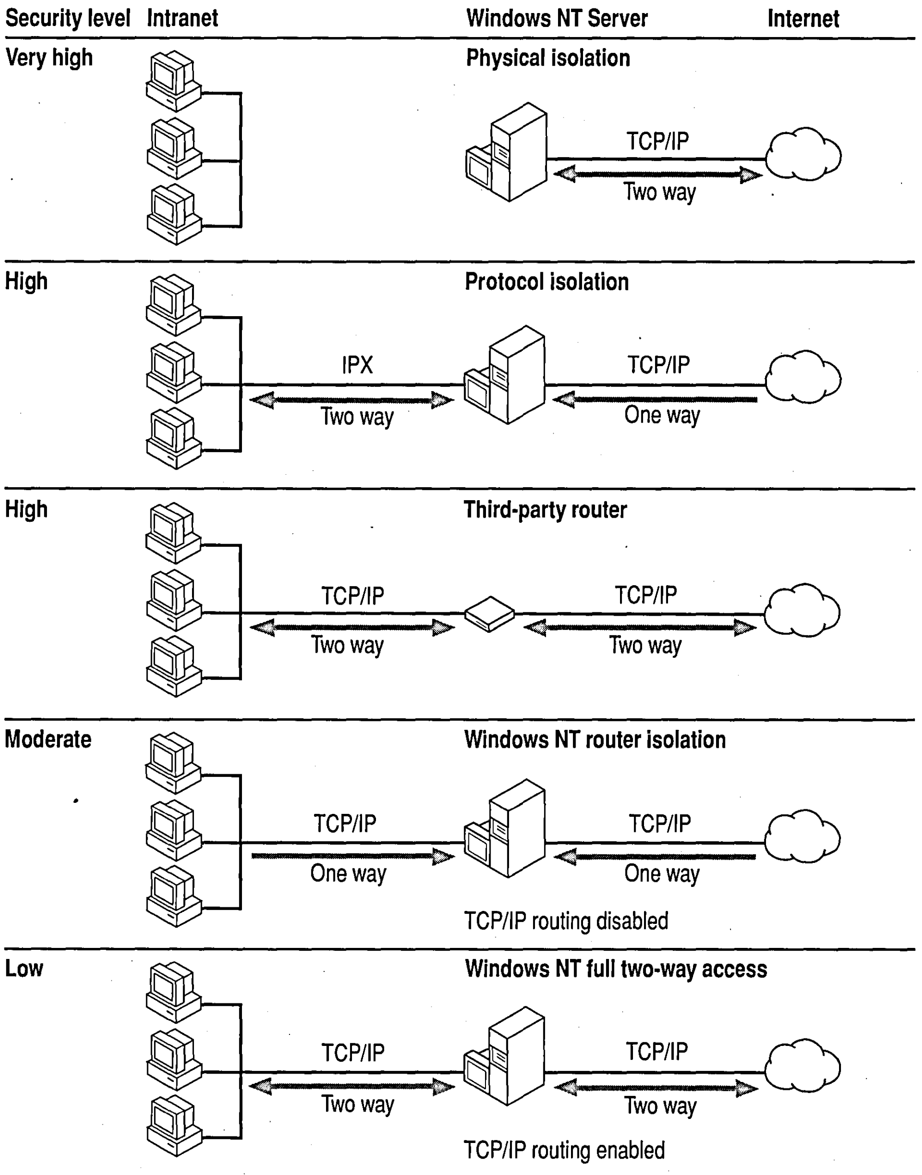


Figure 3.6 How network topology affects security levels

Physical Isolation

A computer physically isolated from your intranet is the safest way to have Internet access, and the easiest to plan and configure. You can install Internet Information Server on it and use Internet Explorer to see and be seen by the Internet. Even the most clever hacker cannot browse your intranet without physical access. Of course, the computer running Internet Information Server is still open to attack and should be securely configured as described in the *Internet Information Server Installation and Administration Guide.*

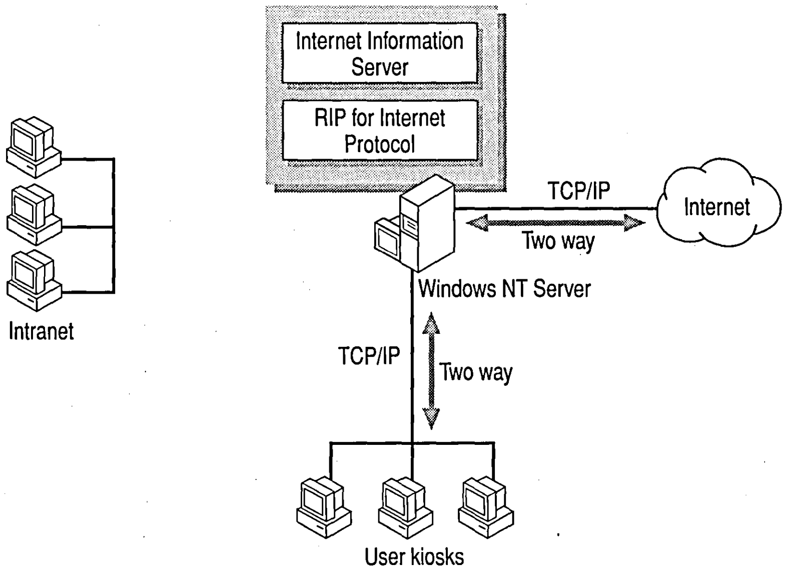


Figure 3.7 Physical isolation security model

A limitation to this configuration is that you cannot share files between the intranet and the Internet. You have to use floppy disks or temporary network connections to share information between the two systems.

You can expand this scenario to create a small intranet of user kiosks and IIS servers connected to the Internet server by installing the RIP for Internet Protocol service.

The type of configuration you choose depends on the size of your organization and on how much Internet access you want to give to your users. For example, if you have a single computer connected to the Internet, it runs Internet Information Server. IIS provides information to share with Internet users, and (optionally) serves as an Internet client that uses Internet Explorer or other Internet software. For this computer to serve as an Internet client, however, it must be physically accessible to employees because it is not on the intranet.

To give users in your organization easier access to the Internet, you can set up a physically separate network. This network consists of the Internet server, additional Internet servers (such as additional IIS servers used as mirrors of the primary IIS installation), and individual workstations, or *kiosks*. The kiosks can be located in conference rooms, hallways, libraries, or in special offices throughout the company. Individuals who are heavy users of the Internet can have kiosks in their offices. The kiosks can be used to retrieve information from your Internet server, to place new information on the server, and to gather information from the Internet at large. This type of scenario, however, requires additional cable installation because all Internet-connected computers are physically separate from your intranet.

Protocol Isolation

If you want both Internet and intranet computers to communicate with the computer running Internet Information Server, you can use protocol isolation security. In this model, the Internet server has two network adapters. The network adapter connected to the Internet is bound to Transmission Control Protocol/Internet Protocol (TCP/IP). The network adapter connected to the intranet runs IPX (the transport protocol used in Novell® NetWare® networks) or any other network protocol except TCP/IP. Intranet users can copy files and maintain the server. However, they cannot access the IIS server because access requires TCP/IP. Internet users can "see" the IIS server, but cannot reach the intranet because reaching it requires IPX.

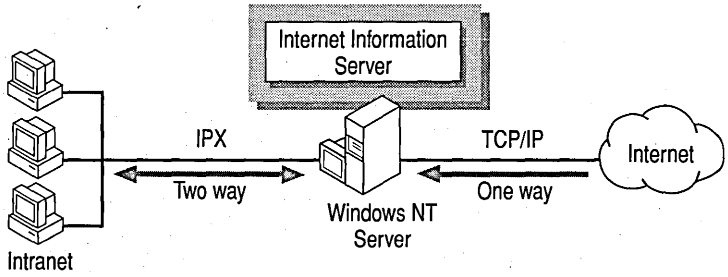


Figure 3.8 Protocol isolation security model

The protocol isolation security model works best for users who spend most of their time making information available to Internet users and who want to copy files directly from the intranet to the Internet server. Or, some users need to frequently download information that is left in a drop box by Internet users, and then integrate that material with information from corporate electronic mail and other resources on the intranet.

The resources on this server are accessible from either direction, but data cannot be passed through. Because of this, there is a virtual barrier to passing packets through the server. Such barriers are often referred to as *firewalls.*

The advantage of the protocol isolation security model is that your users can share information with Internet users from their workstations on the intranet without exposing the intranet to unauthorized use.

One disadvantage of using this model is that your users cannot directly access the Internet or Internet Information Server. The users cannot search for or retrieve Internet resources, only those resources on the computer running Windows NT Server. Users also cannot exchange mail with other Internet users unless you have provided the necessary Internet mail server services on the server.

Another disadvantage is that, theoretically, an Internet user can maliciously penetrate this security model. However, it is very challenging since the server does no protocol conversion.

Replicating the Internet Server on Your Network

A variation on the protocol isolation security model is to replicate the data on the Internet server onto another computer on the internal intranet by using the Windows NT Replication service.

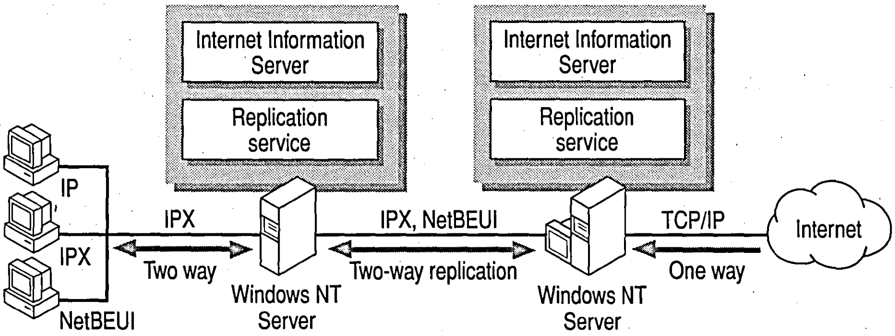


Figure 3.9 Using the Windows NT Replication service for security

For example, if you use the Internet server as a drop box for customer questions and suggestions, Internet users leave information on the Internet server, and then the Windows NT Replication service replicates the contents of the Internet server to the intranet computer. Conversely, if your intranet users need to post information to the public, users on your corporate net copy the information to be shared to the intranet intermediary computer, and then that information is replicated to your Internet server. The intermediary computer can also run Internet Information Server to provide an internal version of your Internet site. This is a scenario used in the Microsoft corporate intranet.

A replication scenario also allows more control over what is brought into the intranet and permitted out of the intranet. Files can be checked for viruses or other problems. You can also use TCP/IP on your intranet because the IPX segment between your intranet and the Internet provides protocol isolation.

For more information about replication, see Chapter 4 of the *Windows NT Server Concepts and Planning* guide.

Third-Party Router Security on TCP/IP-Based Intranets

If you use TCP/IP on a large intranet with high volume or multiple subnets, you probably use a third-party router and a leased-line connection to the Internet. If your third-party routers create a firewall by filtering packets, you can use the router as an Internet gateway.

You can specify exactly which packets are routed from the intranet to the Internet and vice versa. Typically, you do not permit any unrequested packets to enter your intranet and you specify the intranet users who are permitted access to the Internet. Router configuration and topology for this type of application is often provided by the router vendor.

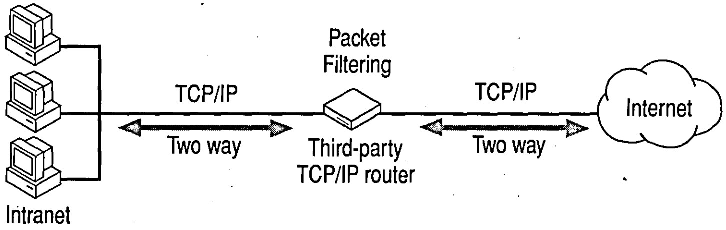


Figure 3.10 Third-party TCP/IP router security

For more information about third-party router capabilities, see your third-party vendor or third-party router documentation. For more information about using routing with Windows NT Server, see Chapter 4 in the *Windows NT Server Networking Supplement.*

Windows NT Router Security on TCP/IP-Based Intranets

If you use TCP/IP on your intranet, you can create a firewall in the computer running Windows NT Server by disabling internal TCP/IP routing. And you can still provide Internet Information Server services to both intranet and Internet users.

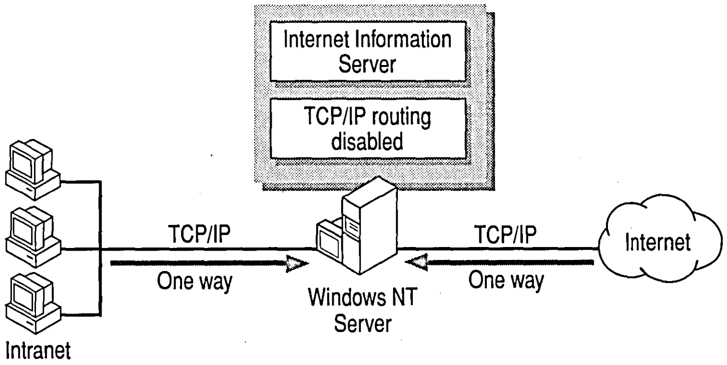


Figure 3.11 Disabled TCP/IP router security

TCP/IP routing controls whether data is passed to and from the intranet through the computer running Windows NT Server; that is, it controls whether the computer acts as a gateway, as shown in Figure 3.11.

The router feature works both ways. Either traffic can pass in both directions or traffic cannot pass through the server at all. This security model has all the advantages and disadvantages of the protocol isolation model.

A major concern with this model is that the separation between the Internet and your intranet depends on a single option in the TCP/IP configuration (or in the associated Registry entry). An intruder who somehow enters through your computer running Windows NT Server needs to change only one Registry value to expose your internal TCP/IP-based intranet.

If you use this security model, you need to be especially careful to control physical and administrative access to the computer that runs Internet Information Server. An individual familiar with Windows NT configuration tools and administrative permissions can find and change the **Router** check box in a matter of minutes.

Full Internet Access

Some organizations need to provide an unrestricted Internet gateway for their users. For example, researchers need to scan the Internet directly as a major part of their work, and then combine information gleaned from the Internet with information that is on the intranet. Each of these users does not need to connect to the Internet through a modem. Instead, one computer running Windows NT Server can serve as a simple gateway to the Internet, as shown in Figure 3.12.

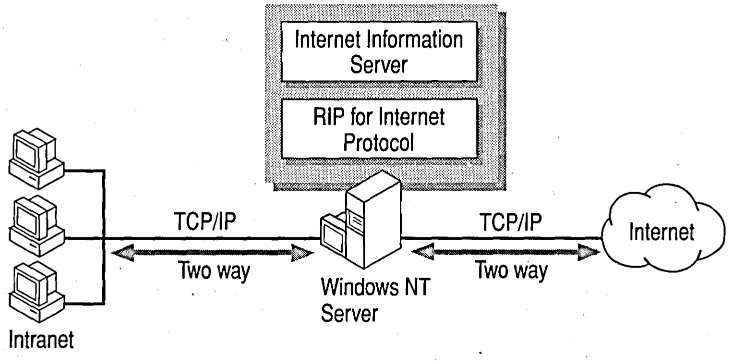


Figure 3.12 A Windows NT–based computer serving as a gateway to the Internet

The computer that serves as a gateway must have:

- A connection to the Internet.
- TCP/IP protocol.
- The RIP for Internet Protocol service.

Internet Information Server can run on the gateway computer, but it is optional.

For information on configuring TCP/IP routing and the RIP for Internet Protocol service, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit: Windows NT Server Networking Guide.*

Routing works both ways. Either traffic can pass in both directions or traffic cannot pass through the server at all. If you enable the RIP for Internet Protocol service, you need to protect all sensitive data on your intranet by other means, such as access control on NTFS drives.

Make sure that the users who have direct Internet access are aware of the security issues. In fact, you should periodically remind them of these issues.

It is most convenient to run Internet Information Server on the computer that serves as the Internet gateway. It is an ideal place for shared directories where Internet users and users of the intranet can deposit and retrieve files, and for indexes of those files.

Also note that Internet users running Windows NT, Windows for Workgroups, LAN Manager, or MS-DOS networking clients can connect to resources on any computer connected to the Internet by issuing **net use** commands. An Internet user running Windows NT, Windows for Workgroups, LAN Manager, or an MS-DOS networking client can issue a **net view** command and then see a list of your corporate servers. Standard Windows NT security controls this method of access.

For more information about Windows NT security, see *Windows NT Server Concepts and Planning*, the *Internet Information Server Installation and Administration Guide*, and the *Microsoft Windows NT Resource Kit: Windows NT Server Resource Guide.*

Additional Security Methods

You can use methods other than network topology to secure and monitor your network. The rest of this chapter explains these methods, which include:

- Using third-party router packet filtering to prevent unwanted access.
- Configuring user account security to control access through the IUSR_*computername* account.
- Using file system security to prevent access to portions of a disk (or partition) and audit file use.
- Using the security log in Event Viewer to audit access to the computer running Internet Information Server and to all NTFS files available through Internet Information Server.
- Using Internet Information Server logs to track use of your IIS services.

For more information about Windows NT security as it relates to Internet Information Server, see the *Internet Information Server Installation and Administration Guide.*

Using Firewalls and Other Inbound Security

Third-party products can create firewalls between the Internet and your intranet. Most of these products are based on *packet filtering*. Packet filtering takes place when the computer examines the source and destination IP addresses of a packet and forwards only those packets that have been granted access.

Many third-party routers that connect your intranet to the Internet can be configured to filter packets based on the source or destination IP address. You can specify which IP addresses are allowed or denied access into your intranet.

For more information about the packet filtering products available, consult dedicated router vendors.

Windows NT User Account Security

A primary security measure to observe at all times is to guard the Administrator account and administrative permissions on computers connected to the Internet. Give the passwords for these accounts only to employees with appropriate security clearances.

External Internet users can get access to your intranet through the Guest or IUSR_*computername* account. To ensure that the permissions for these accounts on your Internet gateway and Internet Information Server are configured to prevent intrusion, restrict the accounts to read-only access on public directories.

Using File System Security

If you create an Internet gateway or run Internet Information Server on one of your networked computers, use NTFS security settings to control access to specific files and directories and to configure the behavior of files and directories. This security method requires the disk or disk partition to be formatted as NTFS. It is a good idea to keep all files that are available through Internet Information Server on a disk or disk partition separate from your operating system, application, or personal files.

Auditing System Activity

You can use auditing to track selected activities of users and the system. Windows NT can record a range of event types—from a systemwide event, such as a user logging on, to an attempt by a particular user to read a specific file on an NTFS drive. Both successful and unsuccessful attempts to perform an action can be recorded.

To open the **Audit Policy** dialog box, click **Audit** on the **Policies** menu in User Manager for Domains. The audit policy determines the amount and type of security logging that Windows NT performs. When an audited event occurs, an entry is added to the Windows NT security log. The security log is viewed by using Event Viewer. Use the settings shown in Table 3.3 to specify what events will be audited.

Table 3.3 Auditing Options

For this event	Select	To audit
Log on and log off	**Success**	A user successfully logged on or off the workstation, or the user made an over-the-network connection to the local computer.
	Failure	A user attempted, but was not allowed, to log on or off the workstation, or the user attempted and failed to make an over-the-network connection to the local computer.
File and object access	**Success**	A user successfully accessed a directory, printer, or file that is set for auditing.
	Failure	A user attempted, but failed, to access a directory, printer, or file that is set for auditing.
Use of user rights	**Success**	A user successfully used a user right. (Rights relating to log on and log off are not included.)
	Failure	A user attempted, but failed, to use a user right.
User and group management	**Success**	A user or group account was successfully created, modified, or deleted, or a password was successfully set or changed.
	Failure	There was an unsuccessful attempt to: • Create, modify, or delete a user or group account. • Set or change a password.
Security policy changes	**Success**	A change was successfully made to the user rights or audit policies.
	Failure	A change was attempted to the user rights or audit policies, but failed.
Restart, shutdown, and system security	**Success**	A user successfully restarted or shut down the computer; or an event has occurred that affects system security.
	Failure	A user attempted, but failed, to restart or shut down the computer.
Process tracking	**Success**	Detailed tracking information for events such as successful program activation, some forms of handle duplication, indirect object access, and process exit.
	Failure	Detailed tracking information for events such as failed program activation, some forms of handle duplication, indirect object access, and process exit.

Before auditing can be established on objects, auditing for the events shown in Table 3.3 must be enabled through User Manager for Domains by a user with Administrator permissions. When auditing files, you must also use Windows NT Explorer to specify which files to audit and which type of file access events to audit. To do this, right-click a file or directory to display its properties, then click **Security** and click **Auditing** to specify auditing attributes.

You view audited events in Event Viewer. Internet Information Server generates entries in all three Event Viewer logs (System, Security, and Application). You can use Event Viewer entries to identify attempts to break into your intranet through your gateway or to detect attempted tampering with your Internet Information Server system.

For more information about auditing, see *Windows NT Server Concepts and Planning*.

Auditing Access with Internet Information Server Logs

You can use Internet Information Server logs to track use of your IIS services.

Logging is very flexible. You can configure it to suit your site's needs. For example, two or more IIS servers can log to the same network file or network database. This is useful for large sites or for sites that use duplicate servers for load balancing. Conversely, if you also run the FTP or Gopher service, you can specify separate files or databases to track access by each service.

By logging to a database, you can use database reporting tools or the Internet Database Connector to query and analyze the log files to detect suspicious activity.

Suspicious activity can include:

- Multiple failed commands, especially to the /Scripts directory or another directory configured for executable files.
- Attempts to upload files to the /Scripts directory or another directory configured for executable files.
- Attempts to access .bat or .cmd files and subvert their purpose.
- .Bat or .cmd commands maliciously sent to the /Scripts directory or another directory configured for executable files.
- Excessive requests from a single IP address attempting to overload or cause a denial of service to other users.

Logs are generated in CERN (European Laboratory for Particle Physics) format but can be converted to Common Log File (National Center for Supercomputing Applications [NCSA] or European Microsoft Windows NT Academic Center [EMWAC]) formats. Conversion is often necessary to use third-party log analysis tools.

For more information about logging, see the *Internet Information Server Installation and Administration Guide.*

CHAPTER 4

Desktop Scenarios

Internet technology offers new ways to communicate and do business. However, you do not need a connection to the public Internet to benefit from technology developed for the Internet. Peer Web Services (Windows NT Workstation) or Internet Information Server (Windows NT Server) and Internet Explorer (an Internet client) can bring the ease of use and rich content of the Internet to your intranet.

The scenarios in this chapter demonstrate single-computer implementations on a corporate desktop computer or small department server. In the first scenario, a desktop computer running Windows NT Workstation and Peer Web Services provides employees timely information about the corporation's recent network merge. The second scenario demonstrates a departmental production server running Windows NT Server and Internet Information Server (IIS). The departmental IIS server provides employees access to Human Resources information.

The scenarios are based on Terra Flora, a fictitious international floral company described in this chapter's first section, "Terra Flora—A Case History." The scenarios show you how to use Windows NT Server Internet Information Server to solve business needs from team communication to global enterprise networking. In Chapter 5, "Enterprise Scenarios," you will find additional scenarios that use or simulate multiple servers. The chapters use scenarios that are presented as if an administrator were implementing a staged rollout of Internet Information Server in a corporation.

You can find more information about Terra Flora, including how this fictitious company used Windows NT Server to achieve networking interoperability, in the *Microsoft Windows NT Server Resource Kit: Windows NT Server Networking Guide*.

Terra Flora — A Case History

Terra Flora, a retail floral corporation, began selling flowers in the 1970s. Over the next 25 years, Terra Flora expanded to include a nursery business and a terra cotta manufacturing plant that produces pots and vases for the retail outlets. Now, in the mid-1990s, these three semiautonomous businesses employ more than 40,000 employees in eight locations, as shown in Figure 4.1.

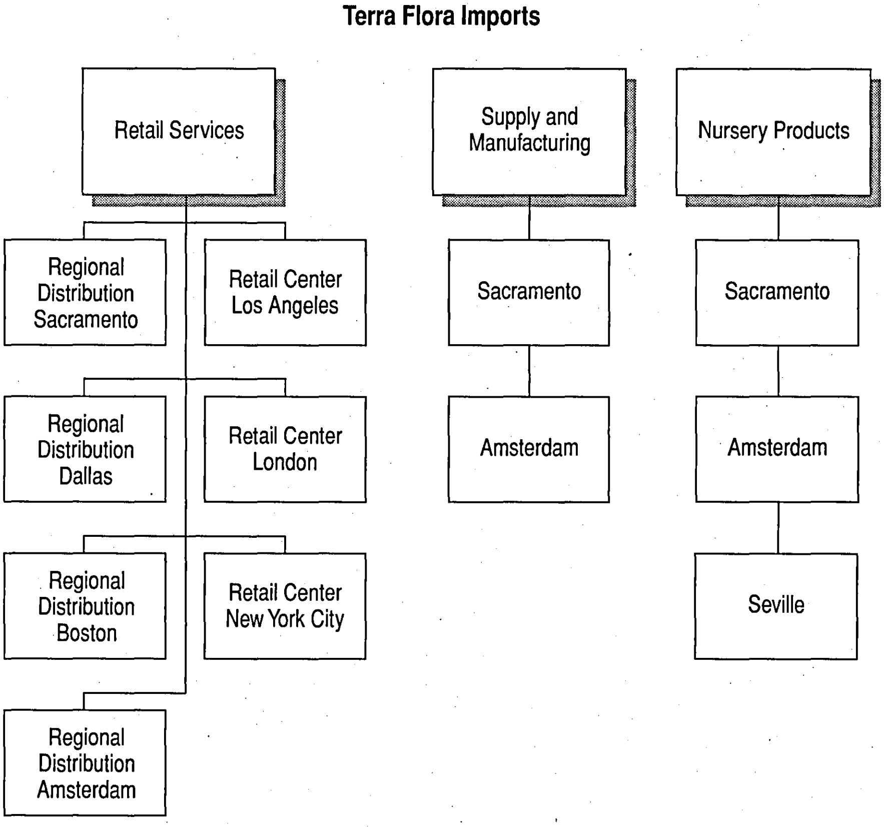

Terra Flora Imports
Retail Services
Supply and Manufacturing
Nursery Products
Regional Distribution Sacramento
Retail Center Los Angeles
Regional Distribution Dallas
Retail Center London
Regional Distribution Boston
Retail Center New York City
Regional Distribution Amsterdam
Sacramento
Amsterdam
Sacramento
Amsterdam
Seville

Figure 4.1 Terra Flora organization

Terra Flora recently physically combined the networks of all divisions, resulting in the network shown in the diagram on the inside back cover of this book.

This diagram represents the significant elements that are present in the Terra Flora network. The size and complexity of a multinational corporate network cannot be represented in a single diagram. References in this book use the computer names on this diagram to provide the network context of a particular scenario. In some scenarios, the actual computer shown in the diagram is used, such as domain controllers or DNS servers. Other scenarios include references to computers that are not illustrated in the diagram; however, the computer's relative position in the network is shown.

Within this network, each of Terra Flora's three divisions has its own autonomous network and information sources, as shown in Table 4.1.

Table 4.1 Terra Flora Systems

Information stored	Format	Computer system
Retail Division		
Retail order database, Accounting database, Employee database	ORACLE database	Sun® Solaris
Corporate and employee information	Word and other documents	Intel-based servers running Windows NT and NetWare
Manufacturing Division		
Parts and price lists	Microsoft Excel worksheets	Intel-based servers running Windows NT and NetWare
Raw materials tracking database	DB2 database	AS/400 running VMS
Wholesale terra cotta gifts catalog	Microsoft Publisher	Intel-based computers running Windows NT Workstation
Nursery Division		
Inventory and wholesale order database	RPG/400	DECpc150 running DEC PATHWORKS
Wholesale flower catalog	ORACLE database	Sun Solaris

The network was made to interoperate by using Windows NT as the integrating platform. Additionally, Terra Flora centralized administration tasks at corporate headquarters in Sacramento, California.

Now that the entire corporation is interconnected, Terra Flora is faced with the challenge of making its information available on the network to everyone in the company—and to customers around the world.

Microsoft Internet Information Server has been selected as the tool to bring Terra Flora's information to its employees and customers. The scenarios in this book explain how Internet Information Server makes information accessible internally and to customers around the world.

You can find more information about the Terra Flora example, including extensive information about how Windows NT Server can be used to achieve networking interoperability, in the *Windows NT Server Networking Guide.*

Accessing Information at Terra Flora

To create an intranet, you need to evaluate your network architecture, review your information needs, and develop an information deployment plan.

Network Architecture

Terra Flora standardized on Transmission Control Protocol/Internet Protocol (TCP/IP) as its single network protocol. It chose TCP/IP as its primary protocol because all of the network operating systems in use at Terra Flora support TCP/IP. Also, TCP/IP routing minimizes network traffic both on the local network and across wide area network (WAN) links.

With TCP/IP, Terra Flora can use applications that have been developed to comply with the standards put forth in requests for comment documents (RFCs) created by the Internet Engineering Task Force (IETF). These international standards, such as the Hypertext Transport Protocol (HTTP) and the TCP/IP protocol suite, enabled the global Internet to develop.

Reviewing Information Needs

Before its merged network was created, Terra Flora's information was contained in different databases and file formats across three separate networks. The information needed to be accessible to customers on those networks and on networks around the world. It was clear to the information officer that a single technology was required to effectively consolidate and deliver that information. Internet technology, based on HTTP, provides a single system that can deliver information to users around the world.

First, the formats and users of each existing information type were identified. Next, the Internet technology that could serve the information to the largest number of people was identified. Table 4.2 summarizes this information.

Table 4.2 Terra Flora Information Consolidation

Information stored	Format	Users	New access method
Retail Division			
Retail order database, Accounting database, Employee database	ORACLE database	Internal, external	HTML forms
Corporate and employee information	Word and other documents	Internal	WWW directory listings
Manufacturing Division			
Parts and price lists	Text files	Internal, external	FTP and Gopher
Raw materials tracking database	DB2 database	Internal	None
Wholesale terra cotta gifts catalog	Microsoft Publisher	External	HTML
Nursery Division			
Inventory and wholesale order database	RPG/400	Internal, external	None
Wholesale flower catalog	ORACLE database	External	HTML forms

Planning Content Strategy and Deployment

The information officer, Maria Gonzales, has the task of integrating disparate information sources. Internet technology offers the easiest, most cost-effective method to access the information.

Three groups of content users were identified:

- Workgroup users
- Division users
- Enterprise users

Each group of users has a specific goal and uses a particular kind of content, as identified in Table 4.3.

Table 4.3 Content Strategy

Users	Goal	Content
Workgroup	Team communication and collaboration	Plans development, document sharing
Division	Division communication and collaboration	Internal supply, part number listing, employee directory, employee handbook
Enterprise	Corporatewide communication and collaboration; migrating mission-critical applications to Internet technology	Plant and products catalog, retail ordering system

Maria has chosen to phase in the integration of components, building on the success of each step, as shown in Table 4.4.

Table 4.4 Terra Flora Implementation Phases for Information Servers

Phase	Goal	Method
1	Team communication	Peer Web Services on an intranet desktop (see this chapter)
2	Division communication	Internet Information Server as a single intranet server (see this chapter)
3	Corporate collaboration	Creating virtual servers by using Internet Information Server (see Chapter 5)
4	Migrate mission-critical applications to Internet Information Server	Internet Information Server as a front end to a database (see Chapter 5)
5	Support heterogeneous clients on the network	FTP and Gopher servers (see Chapter 5)

You can find related scenarios and more information about the Terra Flora example, including extensive information about how Windows NT Server can be used to achieve networking interoperability, in the *Windows NT Server Networking Guide*.

Peer Web Services on an Intranet Desktop

Maria Gonzales needs to communicate with her staff and with network users.

The recent interconnection of three networks has given the Terra Flora information services department the ability to reach any computer in the company, but no tool exists on all the platforms to allow easy communication with every client. The lack of communication is hampering the adoption and use of the newly interconnected networks.

To provide a central communication center, Maria Gonzales announces in e-mail the address of a network directory from which network users can install Internet Explorer, and the address for her computer running Peer Web Services, **http://mariag**.

Peer Web Services Hardware Configuration

Because Peer Web Services is easy to use and is integrated with Windows NT Workstation, Maria installs it on her personal computer running Windows NT Workstation version 4.0. The computer has the following equipment.

- Intel 486 processor with clock speed of 66 MHz
- 32 MB of RAM
- 1 GB of hard disk space

Peer Web Services Network Configuration

The advantage of using Peer Web Services for workgroup communication is that it needs little configuration to start operating in the network. Once Peer Web Services is installed and running, no manual network configuration is necessary.

The computer used to run Peer Web Services (see Figure 4.2) is similar to the computer CANTW40DSK01 in the Terra Flora network diagram.

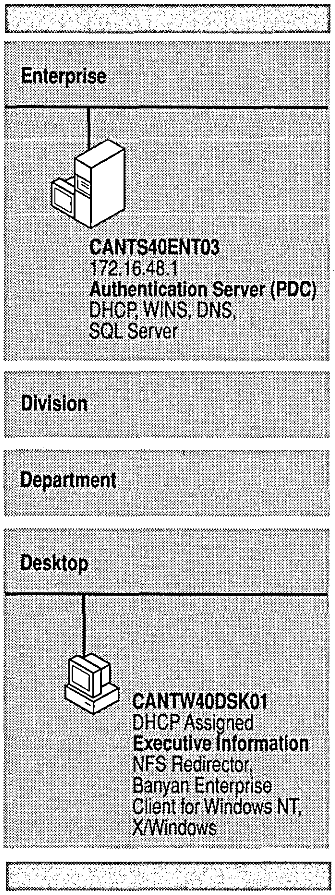


Figure 4.2 Network overview of Peer Web Services

TCP/IP Properties

The IP address and all TCP/IP properties for this computer are dynamically assigned by the network DHCP server CANTS40ENT03 during computer startup. The WINS server, also on CANTS40ENT03, is also notified of the IP address and of the computer name, MARIAG. (For more information about DHCP and WINS, see the *Windows NT Server Networking Supplement* and the *Windows NT Server Networking Guide*.)

Name Resolution

All Internet Explorer users address the Peer Web Services computer by using the NetBIOS name of the information officer's computer. The client's TCP/IP protocol automatically queries the Windows Internet Name Service (WINS) server when a NetBIOS computer name (for example, **http://mariag**) is used to address a Peer Web Services site. The WINS server provides the IP address currently assigned by Dynamic Host Configuration Protocol (DHCP) to that computer name. The DHCP assignment and WINS registration process is dynamic, so regardless of the IP address currently assigned to MARIAG, Internet Explorer users can always resolve **http://mariag** to the current IP address by using the WINS server.

Peer Web Services Configuration

The default installation of Peer Web Services does not need to be changed for immediate use of the information server. Default settings work for most installations.

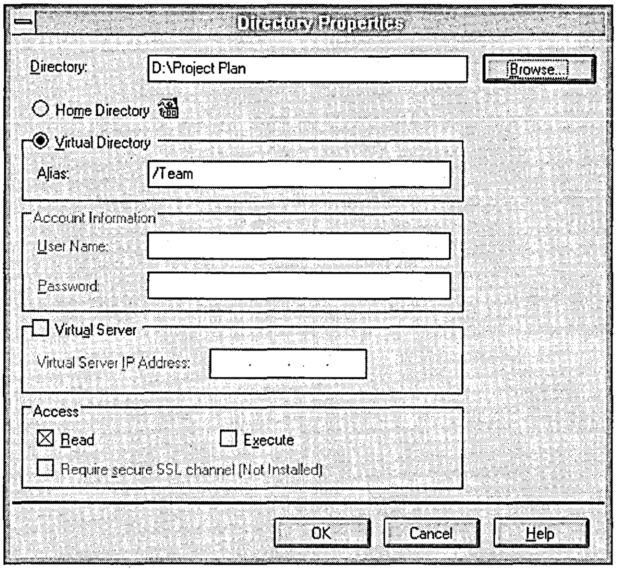
Anonymous Access and Challenge/Response Authentication

Some of the information made available through Terra Flora's World Wide Web (WWW) service pilot project needs to be accessible to all employees, so Maria keeps the default selection—**Allow Anonymous**. Because anonymous access is configured by default, it requires no additional configuration. Maria uses the default home directory (Wwwroot) for content available by anonymous access.

Maria also makes available content that needs to be accessible only to team members. Because all team members are running Windows NT Workstation version 4.0, they have on their desktops Internet Explorer version 2.0, which uses the Windows NT challenge/response password method. Maria uses this authentication method to limit access to team information. Basic authentication is available, but is used only when authenticated clients do not support challenge/response.

For more information about Basic and challenge/response authentication, see Chapter 3, "Server Security on the Internet."

First, Maria creates a virtual directory (/Team) on a Windows NT File System (NTFS) drive for the team information, as shown in Figure 4.3.


Directory Properties

Directory: D:\Project Plan

○ Home Directory

● Virtual Directory

Alias: /Team

Account Information

User Name:

Password:

□ Virtual Server

Virtual Server IP Address:

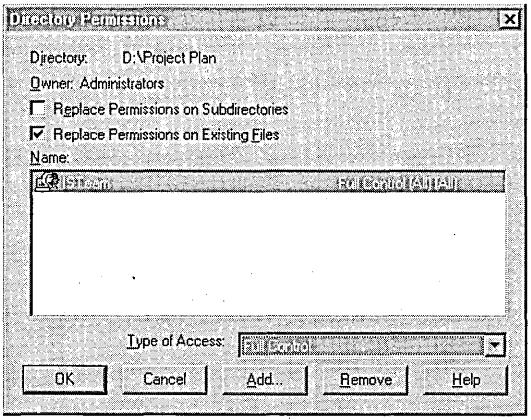
Access

☒ Read □ Execute

□ Require secure SSL channel (Not Installed)

Figure 4.3 Adding a virtual directory in Peer Web Services

Next, Maria sets the properties for that directory to allow access by team members only. She removes the group Everyone. She adds access for the team members by giving the local group ISTeam full control over the directories, as shown in Figure 4.4.


Directory Permissions

Directory: D:\Project Plan

Owner: Administrators

□ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

ISTeam Full Control (All) (All)

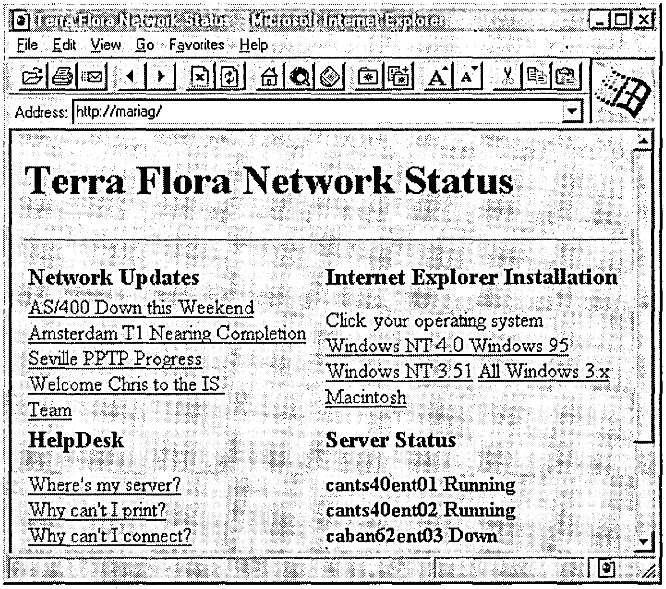
Type of Access: Full Control

Figure 4.4 Setting directory permissions

Now, only members of ISTeam are granted access to the Project Plan directory (shared in Peer Web Services as /Team). All existing Windows NT security and groups can be integrated and used with Peer Web Services and Internet Information Server.

Providing Static Content

Maria uses Internet Assistant to create the Hypertext Markup Language (HTML) file Wwwroot\Default.htm. This file is the *home page* or initial page of information for the site. (See Figure 4.5.) The home page is for the network users and contains information about network status.


Terra Flora Network Status - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://mariag/

Terra Flora Network Status

Network Updates

AS/400 Down this Weekend
Amsterdam T1 Nearing Completion
Seville PPTP Progress
Welcome Chris to the IS Team

Internet Explorer Installation

Click your operating system
Windows NT 4.0 Windows 95
Windows NT 3.51 All Windows 3.x
Macintosh

HelpDesk

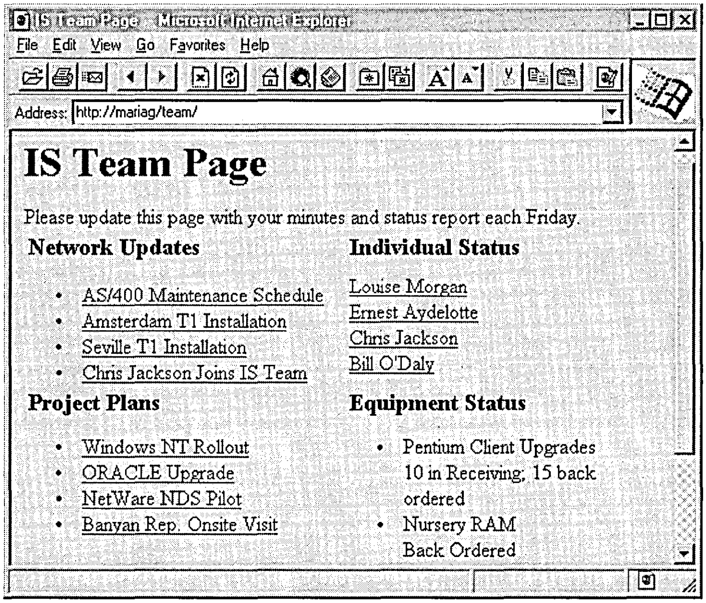
Where's my server?
Why can't I print?
Why can't I connect?

Server Status

cants40ent01 Running
cants40ent02 Running
caban62ent03 Down

Figure 4.5 Terra Flora network integration home page

Next, Maria creates D:\Project Plan\Default.htm as the home page for her team. On this page, Maria also includes links to non-HTML files, such as the Microsoft Project file for the network integration plan, and to historical data in text files. (See Figure 4.6.)


IS Team Page - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://mariag/team/

IS Team Page

Please update this page with your minutes and status report each Friday.

Network Updates

- AS/400 Maintenance Schedule
- Amsterdam T1 Installation
- Seville T1 Installation
- Chris Jackson Joins IS Team

Individual Status

Louise Morgan
Ernest Aydelotte
Chris Jackson
Bill O'Daly

Project Plans

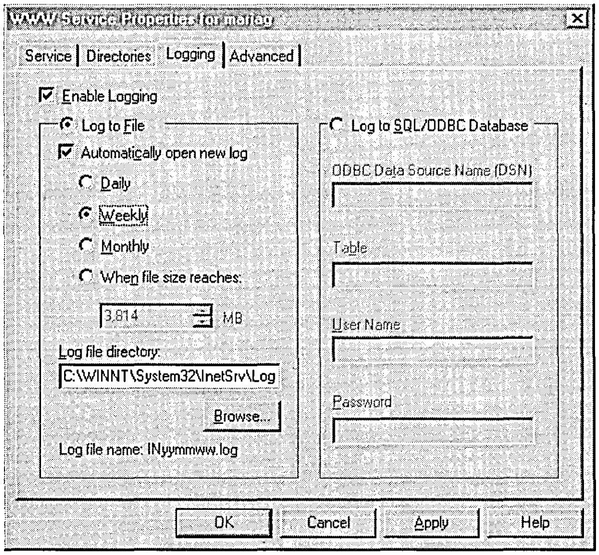
- Windows NT Rollout
- ORACLE Upgrade
- NetWare NDS Pilot
- Banyan Rep. Onsite Visit

Equipment Status

- Pentium Client Upgrades 10 in Receiving; 15 back ordered
- Nursery RAM Back Ordered

Figure 4.6 IS team home page

Finally, to determine who is using the files, Maria configures logging to create weekly log files. (See Figure 4.7.) Later, Maria will use the **convlog** program to convert the log to National Center for Supercomputing Applications (NCSA) format, and will then import the log files into a Microsoft Access database to analyze the use statistics and to generate reports.



☑ Enable Logging

● Log to File

☑ Automatically open new log

○ Daily
● Weekly
○ Monthly
○ When file size reaches:

3.814 MB

Log file directory:
C:\WINNT\System32\InetSrv\Log

Log file name: INyymmww.log

○ Log to SQL/ODBC Database

ODBC Data Source Name (DSN)

Table

User Name

Password

Figure 4.7 Logging to a file

Peer Web Services Internet Considerations

This same configuration works on the Internet without modification. Standard security issues apply, as described in the Peer Web Services *Installation and Administration Guide* HTML documentation and in Chapter 3 of this book.

Peer Web Services is optimized for use as a personal information server for light duty, such as in a workgroup. It does not support the heavy use that can occur on the Internet.

Internet Explorer version 2.0 or later is the only HTTP browser that supports the Windows NT challenge/response authentication system. To accommodate other browsers, you must use the Basic authentication system, which is not secure. You must either use Basic authentication, which sends user names and passwords by using base-64 encoding (and can be decoded easily), or you must implement SSL (Secure Sockets Layer) on your entire site.

Internet Information Server as a Single Intranet Server

The Terra Flora employee handbook is several years out of date and the Human Resources department has requested that an online version be provided to employees as soon as possible.

To meet the goal of a common information source, easily accessible by a variety of clients, Maria chose to install an IIS server. Internet Information Server does not require dedicated hardware, so Maria installed it on an existing file and print server that runs Windows NT Server.

Internet Information Server Intranet Server Hardware Configuration

The existing file and print server is two years old. The low system demands of Internet Information Server will not significantly impact file and print performance, so running Internet Information Server on older hardware is practical, but the following configuration is optimal.

- Intel 486 processor with clock speed of 66 MHz
- 32 MB of RAM
- 1 GB of hard disk space

Internet Information Server Intranet Server Network Configuration

The computer used for the intranet server is similar to the computer CANTS40DPT01 in the Terra Flora network diagram. (See Figure 4.8.)

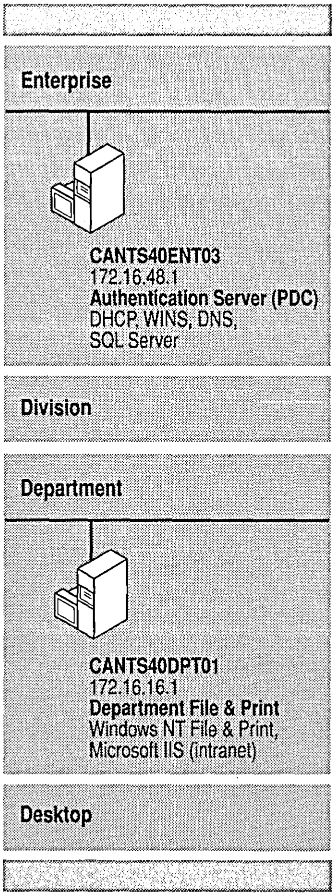


Figure 4.8 Internet Information Server intranet server network overview

TCP/IP Properties

The IP address and all TCP/IP properties for this computer are dynamically assigned by the network DHCP server CANTS40ENT03 during computer startup. The WINS server, also on CANTS40ENT03, is also notified of the IP address for the computer and of the computer name, HR.

Name Resolution

The computer name for the Human Resources server is HR. All Internet Explorer users automatically query the WINS server when using the name of the computer, for example, **http://hr/**. The WINS server provides the IP address currently assigned by DHCP to that computer name. The DHCP assignment and WINS registration process is dynamic, so regardless of the IP address currently assigned to HR, Internet Explorer users can always resolve **http://hr** to the current IP address.

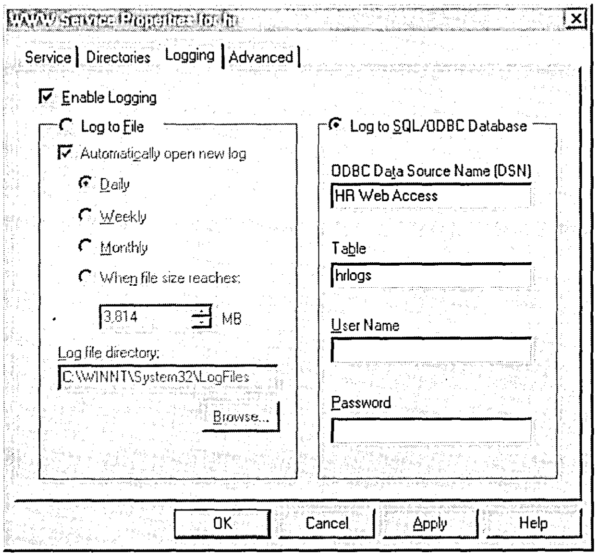
Internet Information Server Configuration

The default installation of Internet Information Server does not need to be changed for immediate use of the information server. Default settings work for most installations.

Anonymous Access

All the information made available through this WWW service pilot project must be accessible to all employees. Anonymous access is enabled by default in Internet Information Server. By clearing the **Windows NT Challenge/Response** check box, Maria allows only anonymous access.

Because this is a pilot project, it is important to collect statistics to determine who is using the files. Maria configures logging to a Microsoft Access database. (See Figure 4.9.) Although logging to a database requires processing time, internal use is expected to be light so the overhead will be minimal. In addition, instant access to the Microsoft Access custom reports based on the Internet Information Server logs is a real benefit for the information officer.



WWW Service Properties for hr

Service | Directories | Logging | Advanced

☑ Enable Logging

○ Log to File

☑ Automatically open new log

● Daily

○ Weekly

○ Monthly

○ When file size reaches:

3.814 MB

Log file directory:

C:\WINNT\System32\LogFiles

● Log to SQL/ODBC Database

ODBC Data Source Name (DSN)

HR Web Access

Table

hrlogs

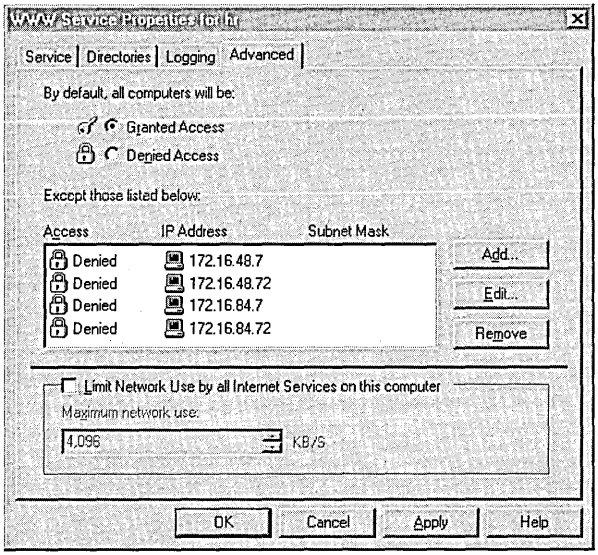
User Name

Password

Figure 4.9 Logging to a database

Excluding Computers by DNS Name

Retail outlet point-of-sale computers should not be able to access the IIS server. To prevent the retail stores from accessing the IIS server, the IP addresses of the point-of-sale computers are excluded from access to the information server by using the **Advanced** property sheet, as shown in Figure 4.10.



By default, all computers will be:

● Granted Access

○ Denied Access

Except those listed below:

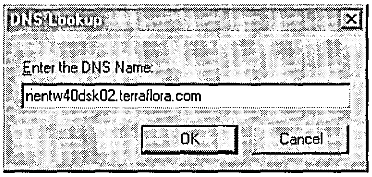
Access	IP Address	Subnet Mask
Denied	172.16.48.7	
Denied	172.16.48.72	
Denied	172.16.84.7	
Denied	172.16.84.72	

□ Limit Network Use by all Internet Services on this computer

Maximum network use: 4,096 KB/S

Figure 4.10 Excluding computers on the Advanced property sheet

It is not necessary to know the IP address of the computers to be denied. Because a DNS server is available (CANTS40ENT01), after you click **Add** you can click the ellipsis (**...**) button next to the IP address box and enter the DNS name of the computer. Internet Information Server queries the DNS server to resolve the name for you, as shown in Figure 4.11.



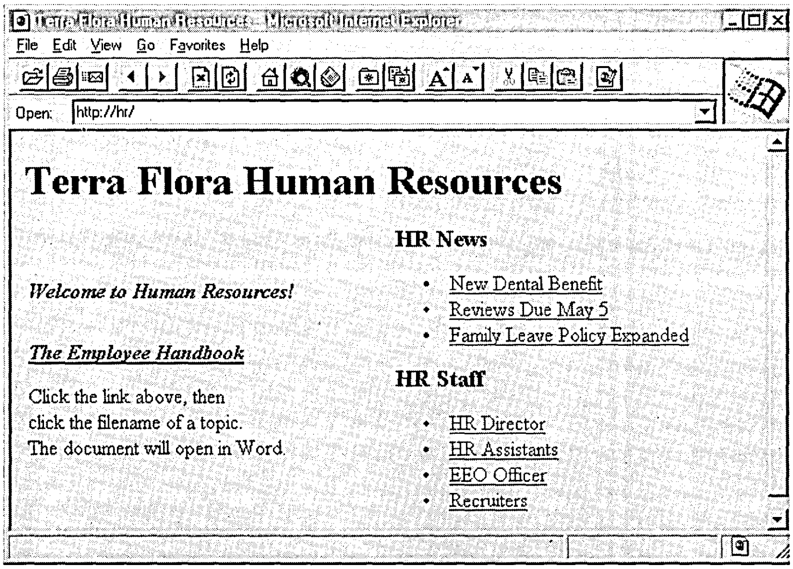
Enter the DNS Name: nentw40dsk02.terraflora.com

Figure 4.11 Resolving DNS names for exclusion

Directory Listings to Provide Content

It is not necessary to use the HTML format for the content on Internet Information Server or Peer Web Services. You can use directory listings to automatically display the contents of directories, similar to the Windows NT Explorer display.

New information about Terra Flora's Human Resources department will be written in HTML by using Internet Assistant for Microsoft Word. The files will be placed in the default directory, Wwwroot. The home page for the Human Resources department will be Wwwroot/Default.htm. Because the home page is named Default.htm, users need only specify **http://hr/** to view the Human Resources home page, as shown in Figure 4.12.


Terra Flora Human Resources - Microsoft Internet Explorer
File Edit View Go Favorites Help
Open: http://hr/

Terra Flora Human Resources

Welcome to Human Resources!

The Employee Handbook

Click the link above, then click the filename of a topic. The document will open in Word.

HR News

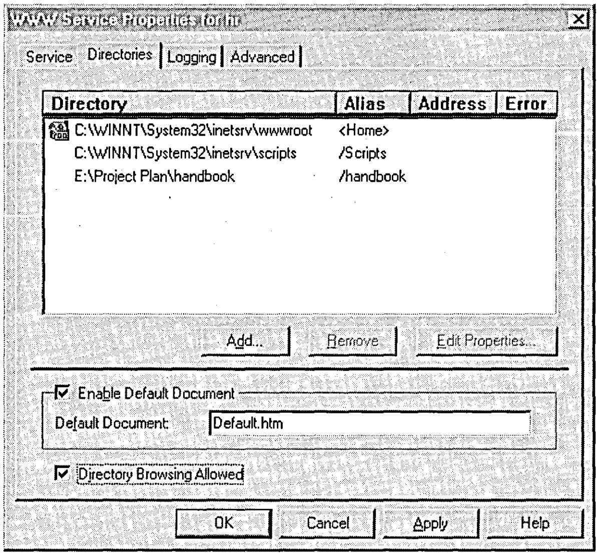
- New Dental Benefit
- Reviews Due May 5
- Family Leave Policy Expanded

HR Staff

- HR Director
- HR Assistants
- EEO Officer
- Recruiters

Figure 4.12 Human Resources home page

From the HTML home page, users can view existing Human Resources information that exists in multiple formats, including Microsoft Word documents. Rather than convert all the documents to HTML format, the existing documents are presented by using WWW directory listings. On the **Directories** tab of the **WWW Service Properties** dialog box, directory browsing is enabled, as shown in Figure 4.13.



WWW Service Properties for hr

Directory	Alias	Address	Error
C:\WINNT\System32\inetsrv\wwwroot	<Home>		
C:\WINNT\System32\inetsrv\scripts	/Scripts		
E:\Project Plan\handbook	/handbook		

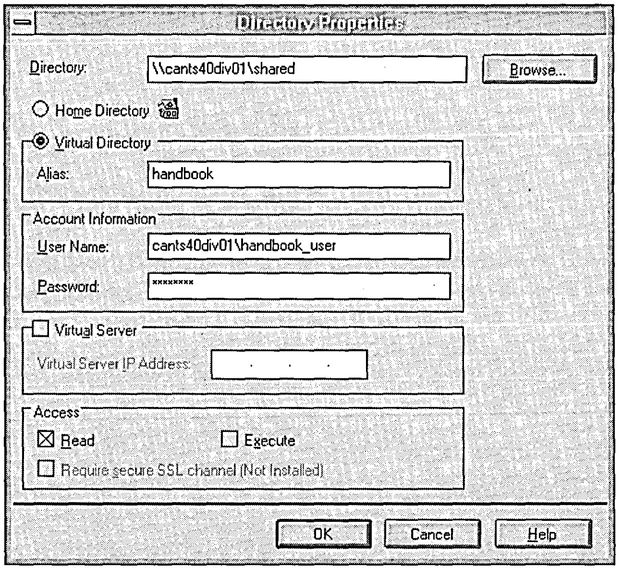
☑ Enable Default Document

Default Document: Default.htm

☑ Directory Browsing Allowed

Figure 4.13 Enabling directory browsing

The employee handbook files were created and are maintained by using Microsoft Word. The handbook resides on another Windows NT–based file and print server. A virtual directory called "handbook" is created that points to the network directory on the Terra Flora computer CANTS40DIV01, as shown in Figure 4.14.



Directory Properties

Directory: \\cants40div01\shared

○ Home Directory

● Virtual Directory

Alias: handbook

Account Information

User Name: cants40div01\handbook_user

Password: ********

☐ Virtual Server

Virtual Server IP Address: . . .

Access

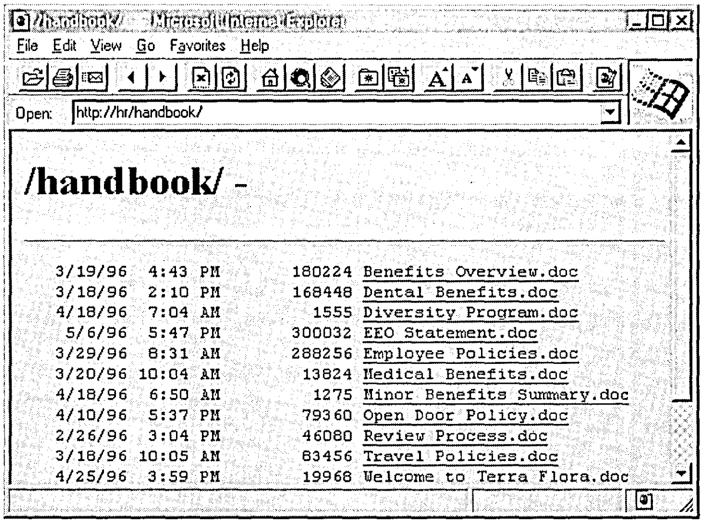
☒ Read ☐ Execute

☐ Require secure SSL channel (Not Installed)

Figure 4.14 Creating a virtual directory

Because the default document, Default.htm, does not exist on the network directory, but directory browsing is enabled, when users connect to **http://hr/handbook** (or click the link on the HTML home page), they see a listing of the handbook files.

Twenty files are combined to make up the handbook and are named according to the contents of the file. For example, the information about medical benefits is in the file Medical Benefits.doc, as shown in Figure 4.15.


/handbook/ - Microsoft Internet Explorer
File Edit View Go Favorites Help
Open: http://hr/handbook/

/handbook/ -

```
  3/19/96  4:43 PM       180224 Benefits Overview.doc
  3/18/96  2:10 PM       168448 Dental Benefits.doc
  4/18/96  7:04 AM         1555 Diversity Program.doc
   5/6/96  5:47 PM       300032 EEO Statement.doc
  3/29/96  8:31 AM       288256 Employee Policies.doc
  3/20/96 10:04 AM        13824 Medical Benefits.doc
  4/18/96  6:50 AM         1275 Minor Benefits Summary.doc
  4/10/96  5:37 PM        79360 Open Door Policy.doc
  2/26/96  3:04 PM        46080 Review Process.doc
  3/18/96 10:05 AM        83456 Travel Policies.doc
  4/25/96  3:59 PM        19968 Welcome to Terra Flora.doc
```

Figure 4.15 WWW directory listings

When Internet Explorer users double-click a filename in the listing, such as Medical Benefits.doc, Word automatically starts and displays the selected file. All employees in the company have access to the files by using directory browsing.

To prevent anyone from tampering with the handbook, the files are accessed by using the user account handbook_user, an account local to the CANTS40DIV01 server, as shown in Figure 4.14. This account was created specifically to provide read-only access to the handbook files. When an account is specified in the **Directory Properties** dialog box, this account overrides any account information provided by the user.

Internet Considerations

This same configuration works on the Internet without modification. Standard security issues apply, as described in the *Internet Information Server Installation and Administration Guide* and in Chapter 3 of this book.

CHAPTER 5

Enterprise Scenarios

An enterprise network is a network for an organization that has several thousand employees and that operates at multiple sites. Typically, large networks have several different standards in use across the network. Interoperability and communication are constant challenges for the information staffs of enterprise networks.

The diagram inside the back cover of this book illustrates the enterprise network for Terra Flora, a fictitious international floral company.

The Terra Flora enterprise network was created in Microsoft laboratories to demonstrate Windows NT interoperability features for an enterprise network. *The Windows NT Server Resource Kit: Windows NT Server Networking Guide* contains chapters that show you how Windows NT Server solved the interoperability challenges posed by the Terra Flora enterprise network.

Chapters 4 and 5 in this book show you how to use Windows NT Server Internet Information Server (IIS) to meet business communication needs—from team communication to mission-critical applications. The chapters use scenarios that are presented as if an administrator were implementing a staged rollout of Internet Information Server to the company. See Chapter 4, "Desktop Scenarios," for a complete description of the Terra Flora company and its network.

The scenarios in this chapter use or simulate multiple servers. The scenarios covered are:

- A single production server using virtual servers to host "multiple" web sites on a single computer.
- Database access for a mission-critical application.
- File Transfer Protocol (FTP) and Gopher servers for access to the same set of Human Resources information.
- Multiple computers running Windows NT Server and Internet Information Server demonstrates a large-scale Internet implementation of IIS.

Creating Virtual Servers by Using Internet Information Server

In this scenario, Terra Flora has successfully deployed Internet Information Server on a department-level server (see Chapter 4) and is setting up an IIS server for each division.

This scenario assumes that dedicated hardware is not available for each division's IIS server. Therefore, Terra Flora installs Internet Information Server on an existing computer running Windows NT Server, then creates a virtual server for each division, as shown in Table 5.1.

Table 5.1 Computer Names for Terra Flora Divisions

Division	Computer name URL
Retail	**http://retail**
Supply and Manufacturing	**http://supply**
Nursery	**http://nursery**

These servers will provide information—such as project plans and employee services—to new members or to other division employees. For examples of how Terra Flora will distribute information, see the section "Information Distribution," later in this chapter.

Ideally, each division operates a separate server. Automatic IP address administration by Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS) name resolution works on separate servers that are each addressed with a single Internet Protocol (IP) address. After you install Internet Information Server, name resolution on the network automatically "finds" the IIS server; no additional network configuration is required for name resolution. DHCP and WINS are designed to work together for automatic name resolution on a network, as explained in Chapter 2.

For example scenarios that use automatic DHCP configuration and WINS resolution, see "Peer Web Services on an Intranet Desktop" and "Internet Information Server as a Single Intranet Server" in Chapter 4, "Desktop Scenarios."

Virtual Server Hardware Configuration

The virtual servers are installed on a new file and print server. The new server provides adequate resources for the three IIS servers, in addition to its primary role as a file and print server and a messaging server.

Here is the hardware configuration for the IIS server that will host the virtual servers:

- Pentium dual processor with clock speed of 100 MHz
- 64 MB of RAM
- 10 GB disk

Virtual Server Network Configuration

Terra Flora uses virtual servers for its division-level IIS servers because it does not want the expense of dedicated IIS servers for the initial rollout. The network configuration of a virtual server on an intranet requires multiple IP addresses and name resolution for each IP address assigned. Figure 5.1 highlights the components in the Terra Flora network that are involved in creating enterprise virtual servers by using Internet Information Server.

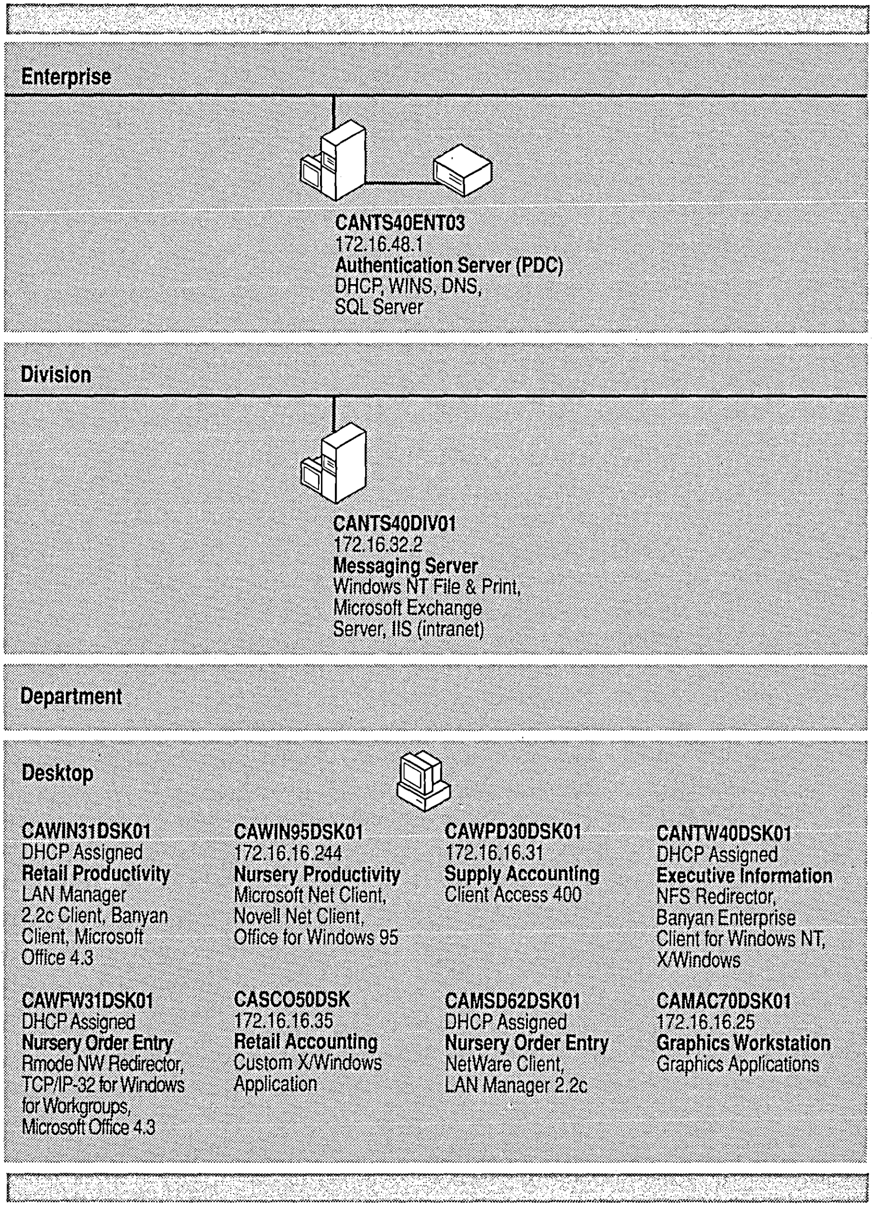


Figure 5.1 Virtual server network overview

The virtual servers are hosted on the computer CANTS40DIV01, which also is a file and print server and a messaging server. Name resolution is provided by CANTS40ENT03. All clients in the network except MS-DOS-based clients can access the virtual servers.

If you use DHCP servers and WINS servers on your network, as Terra Flora does, it is best to avoid using IIS virtual servers.

Virtual servers require you to manually configure Transmission Control Protocol/Internet Protocol (TCP/IP) properties on the computer running Internet Information Server and also to manually configure the name resolution system in use on your network.

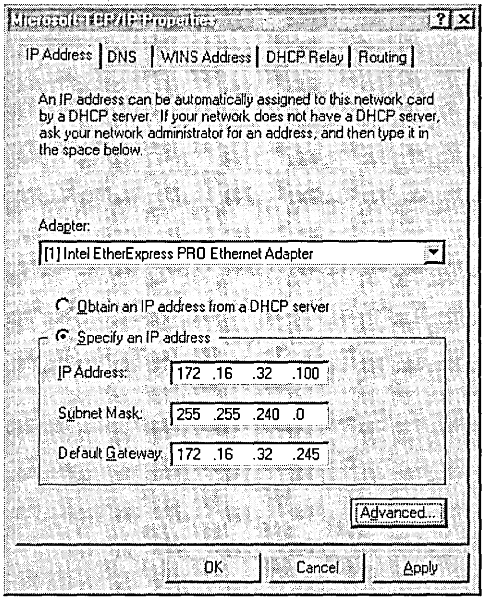
DHCP and WINS are designed to work together for automatic name resolution on a network, as explained in Chapter 2. Automatic administration means that name resolution on the network is completely automated. Every time the IIS server starts, it is automatically given an IP address and its name is registered on the WINS servers used throughout the network. This method is demonstrated in "Peer Web Services on an Intranet Desktop" and "Internet Information Server as a Single Intranet Server" in Chapter 4, "Desktop Scenarios."

If you do not use DHCP or WINS servers on your network, installation of Internet Information Server requires manual configuration. Because virtual servers require little additional manual configuration, they are ideal for a network that does not use DHCP or WINS.

Virtual Server TCP/IP Properties

One IP address must be added to the network interface card (NIC) of CANTS40DIV01 for each virtual server. When you assign more than one IP address to a single network interface card , you must disable automatic DCHP configuration. The DHCP server cannot assign multiple IP addresses to the same network interface card.

You enter the IP addresses and all TCP/IP properties for this computer by using the configuration options available when you double-click **Network** in Control Panel. On the **Protocol** tab, select **TCP/IP protocol** and click **Properties**. Type the first IP address, subnet mask, and the computer's default gateway under **Specify an IP Address** on the **IP Address** tab. (See Figure 5.2.)



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[1] Intel EtherExpress PRO Ethernet Adapter

○ Obtain an IP address from a DHCP server

● Specify an IP address

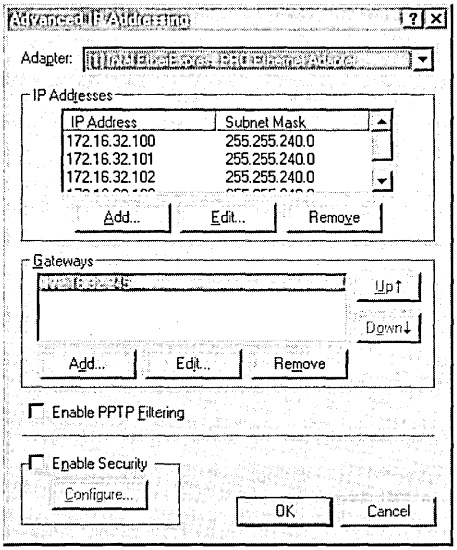
IP Address: 172 .16 .32 .100

Subnet Mask: 255 .255 .240 .0

Default Gateway: 172 .16 .32 .245

Figure 5.2 Setting TCP/IP properties for virtual servers

After you type the first IP address, subnet mask, and default gateway, click **Advanced** to display the **Advanced IP Addressing** dialog box, as shown in Figure 5.3. To add IP addresses to your network interface card, click the **Add** button under **IP Addresses**.



Advanced IP Addressing

Adapter: [illegible]

IP Addresses

IP Address	Subnet Mask
172.16.32.100	255.255.240.0
172.16.32.101	255.255.240.0
172.16.32.102	255.255.240.0

Gateways: [illegible]

□ Enable PPTP Filtering

□ Enable Security

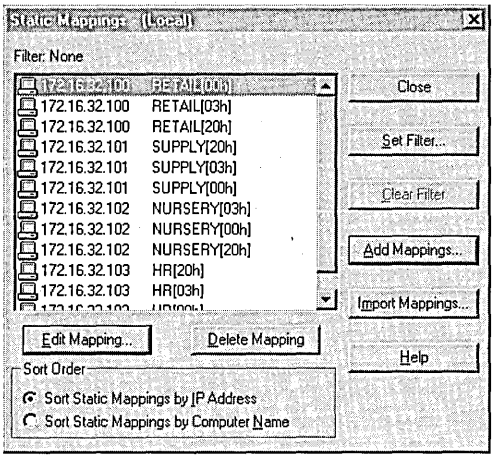
Figure 5.3 Adding more than one IP address

Virtual Server Name Resolution

The computer name of the computer hosting the IIS virtual servers is CANTS40DIV01 (see diagram inside the back cover of this book). When you use multiple computer names with multiple IP addresses on the same network interface card, you must configure the WINS server with the computer name/IP address pairs that you will use. Thus, when clients consult a WINS server, the server provides the computer name and IP address for your virtual server. (You can also configure the WINS server to override the default computer name/IP address pair used if only a single IP address is assigned to the network interface card of a computer running Internet Information Server.)

You use the WINS server (CANTS40ENT03 in the Terra Flora diagram) to assign three computer names (NetBIOS computer names) to the three static IP addresses configured on the computer running Internet Information Server. The names in the WINS database will be used by Windows-based clients for name resolution.

Use WINS Manager in the Administrative Tools folder to assign the NetBIOS names to the IP addresses you added to the network interface card of your computer running Internet Information Server. On the **WINS Manager Mappings** menu, click **Static Mappings**. In the **Static Mappings** dialog box, click **Add Mappings** and add each virtual server's IP address/NetBIOS name pair. After you have added the IP address/NetBIOS name pairs, the mappings appear as shown in Figure 5.4.



Static Mappings - (Local)

Filter: None

172.16.32.100	RETAIL[00h]
172.16.32.100	RETAIL[03h]
172.16.32.100	RETAIL[20h]
172.16.32.101	SUPPLY[20h]
172.16.32.101	SUPPLY[03h]
172.16.32.101	SUPPLY[00h]
172.16.32.102	NURSERY[03h]
172.16.32.102	NURSERY[00h]
172.16.32.102	NURSERY[20h]
172.16.32.103	HR[20h]
172.16.32.103	HR[03h]
172.16.32.103	HR[00h]

Sort Order

● Sort Static Mappings by IP Address

○ Sort Static Mappings by Computer Name

Figure 5.4 Virtual server WINS mapping

When an Internet Explorer client (or other browser) requests a Uniform Resource Locator (URL) that uses a NetBIOS name—such as **http://retail**—TCP/IP networking on the client automatically consults the WINS server to discover IP addresses. This is illustrated as step 1 in Figure 5.5. The WINS server notifies the client of the IP address assigned to that NetBIOS name (step 2). The client then uses the IP address to make the request to the computer running Internet Information Server (step 3).

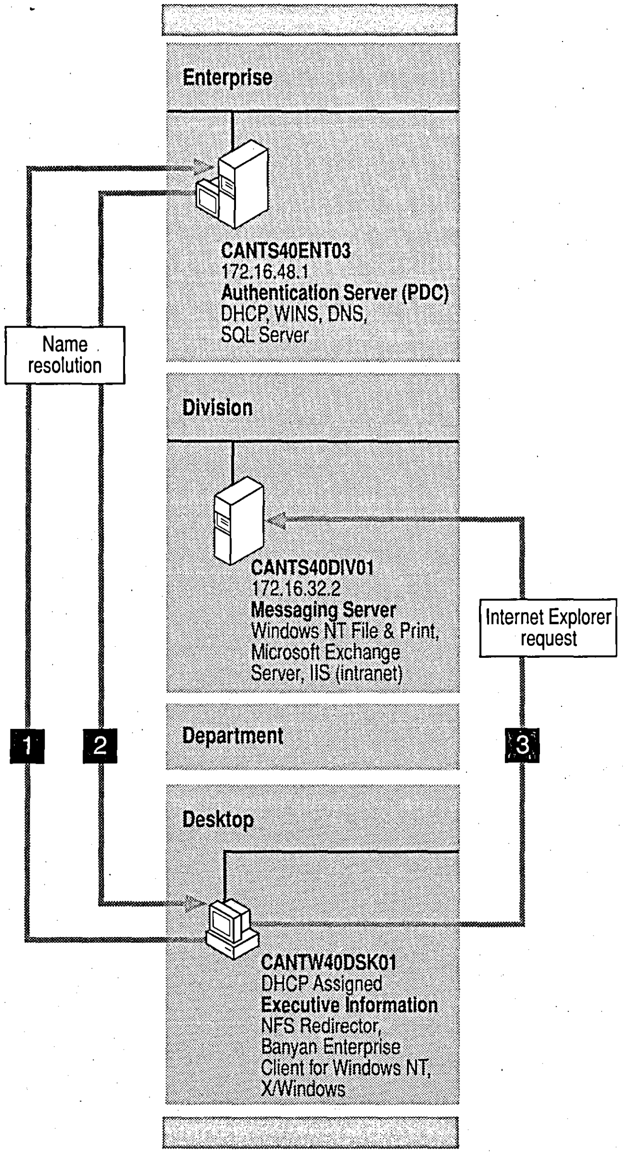


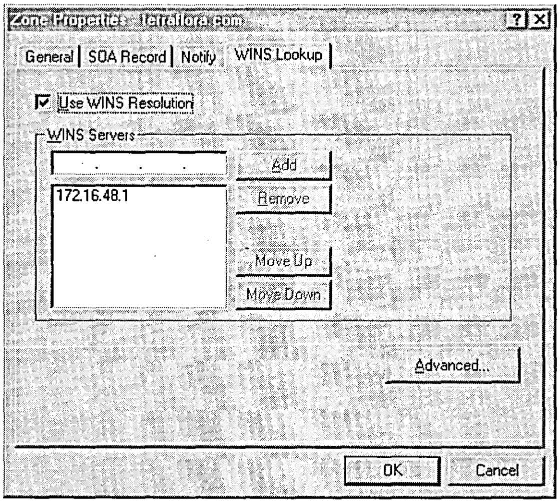
Figure 5.5 WINS resolution for URL that uses NetBIOS computer name

Networks that do not use WINS can use an alternative name resolution system, usually Domain Name System (DNS) servers. DNS servers resolve a domain name—such as retail.terraflora.com—to an IP address.

If you use third-party DNS servers, you manually add a DNS A-type resource record to the zone data file for each virtual server IP address/DNS domain name pair. For more information about DNS resource records and their formats see RFC 883 and RFC 973 or the documentation for your DNS server.

Terra Flora uses both Windows NT WINS servers and Windows NT DNS servers. For example, both a WINS server and a DNS server are on CANTS40ENT03 on the Terra Flora network diagram. Because Terra Flora uses both WINS and DNS, there is no need to create actual DNS database entries for the new servers. Instead, you can provide a form of dynamic DNS by directing the Windows NT Server DNS server to query WINS for name resolution of the terraflora.com domain.

In DNS Manager, right-click the zone that will consult the WINS database for name resolution, and then click **Properties**. Click the **WINS Lookup** tab and enter the IP address of the WINS server, as shown in Figure 5.6.



☑ Use WINS Resolution

WINS Servers

172.16.48.1

Figure 5.6 Using WINS with DNS for name resolution

The DNS server automatically consults the WINS server to discover the IP address. For example, a UNIX computer requests the DNS server to resolve retail.terraflora.com to an IP address. Because the DNS server does not have an explicit record for retail.terraflora.com, it queries the WINS server for the name "retail." The WINS server has a static mapping for the NetBIOS name "retail" to the IP address 172.16.32.100 and returns that IP address to the DNS server. The DNS server then resolves the DNS name retail.terraflora.com based on the NetBIOS name mapping in WINS. This NetBIOS-name-to-DNS-name mapping is automatic for all names in the WINS server, including WINS mappings based on automatic IP address assignment by DHCP.

After you finish these configurations, users can then access the Internet Information Server virtual server by using either the NetBIOS name (if WINS is supported on the client) or the domain name (if DNS is supported on the client), as shown in Table 5.2.

Table 5.2 Virtual Server Computer Names Used in URLs

NetBIOS name	Computer name used in URL with WINS name resolution	Domain name URL used by DNS name resolution
RETAIL	**http://retail**	**http://retail.terraflora.com**
SUPPLY	**http://supply**	**http://supply.terraflora.com**
NURSERY	**http://nursery**	**http://nursery.terraflora.com**

For more information on WINS and DNS interoperability, see the *Windows NT Server Networking Guide.*

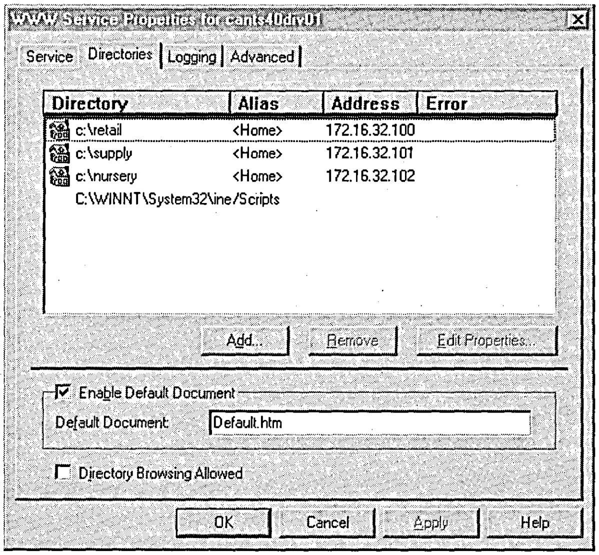
If your network contains non-Microsoft DNS servers, you must add a record in the DNS database for each IP address/domain name pair you add. The name resolution process is similar to WINS name resolution. For information about adding a computer to a domain, see your DNS server documentation.

You can also use HOSTS or LMHOSTS files on client computers for name resolution. On frequently accessed servers, this is slightly faster that consulting a WINS or DNS server, and also reduces network traffic. For more information on name resolution by using HOSTS and LMHOSTS files, see the *Windows NT Server Networking Supplement.*

To complete the creation of the virtual servers, you must now create a home directory for each virtual server, as described in the next section.

Internet Information Server Configuration to Create Virtual Servers

You use Internet Service Manager to create virtual servers. You will not see virtual server names in the main Internet Service Manager window. Virtual servers are created on the **Directories** tab of the **WWW Service Properties** dialog box, as shown in Figure 5.7.



Directory	Alias	Address	Error
c:\retail	<Home>	172.16.32.100	
c:\supply	<Home>	172.16.32.101	
c:\nursery	<Home>	172.16.32.102	
C:\WINNT\System32\ine/Scripts			

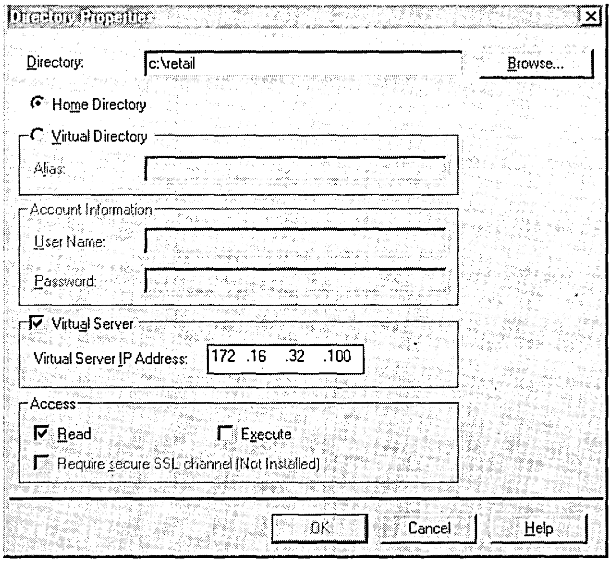
☑ Enable Default Document

Default Document: Default.htm

□ Directory Browsing Allowed

Figure 5.7 Virtual server directories listed

To create a virtual server, click **Add** and, in the **Directory Properties** dialog box, specify a directory for each IP address configured on your server. (See Figure 5.8.) A virtual server is not "created" until a directory is created that uses the IP address of that virtual server.



Directory Properties

Directory: c:\retail

● Home Directory

○ Virtual Directory

Alias:

Account Information

User Name:

Password:

☑ Virtual Server

Virtual Server IP Address: 172 .16 .32 .100

Access

☑ Read ☐ Execute

☐ Require secure SSL channel (Not Installed)

Figure 5.8 Specifying the IP address for a virtual server directory

If a single IP address is used on a computer running Internet Information Server, all directories created apply to that IP address. If two or more IP addresses are added to a computer running Internet Information Server, you must then select the **Virtual Server** check box and type an IP address in the **Virtual Server IP Address** box for each IIS directory you create. If you fail to select the **Virtual Server** check box and to specify an IP address, that directory will be available through all IP addresses assigned to the computer.

The default home directory (wwwroot) and the /Scripts directory created during installation are not assigned to a specific IP address. Because no IP address is assigned to the directories, the default home directory becomes the default home directory for all TCP/IP addresses assigned to that server.

The /Scripts directory is a good example of a case that calls for using a common directory between virtual servers by not specifying an IP address. You can locate the scripts for all virtual servers on the computer in the same common directory. For example, **http://retail/scripts/order.dll** and **http://supply/scripts/update.exe** both use files in the same physical directory.

Using Groups for Selective Access

This section discusses how Internet Information Server authentication and Windows NT user accounts and global groups are used at Terra Flora to provide selective access to files served through Internet Information Server.

An overview of Terra Flora's use of Windows NT groups to provide selective access is shown in Figure 5.9.

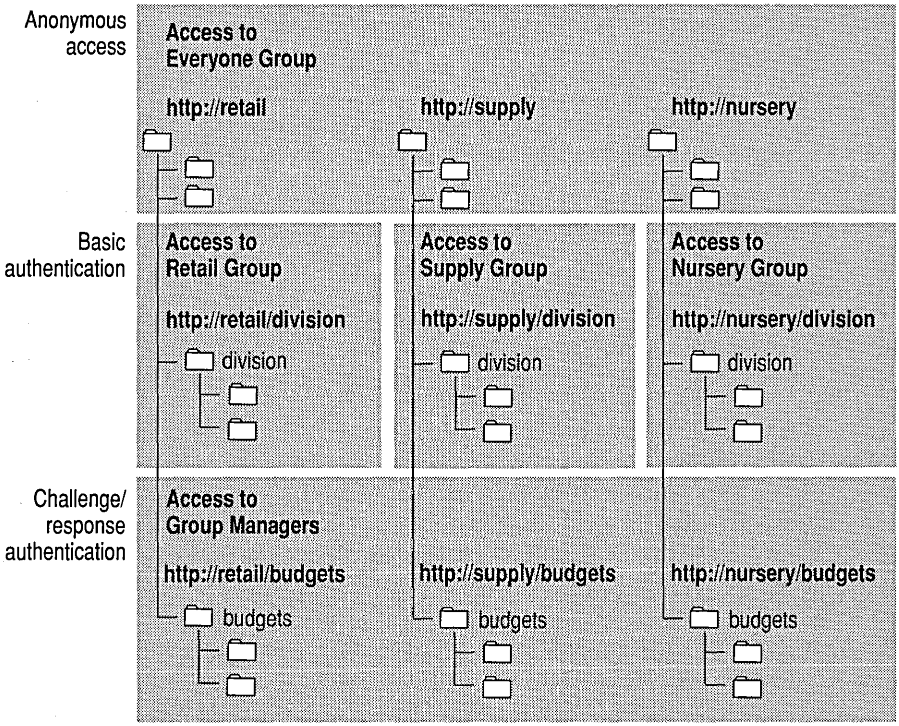


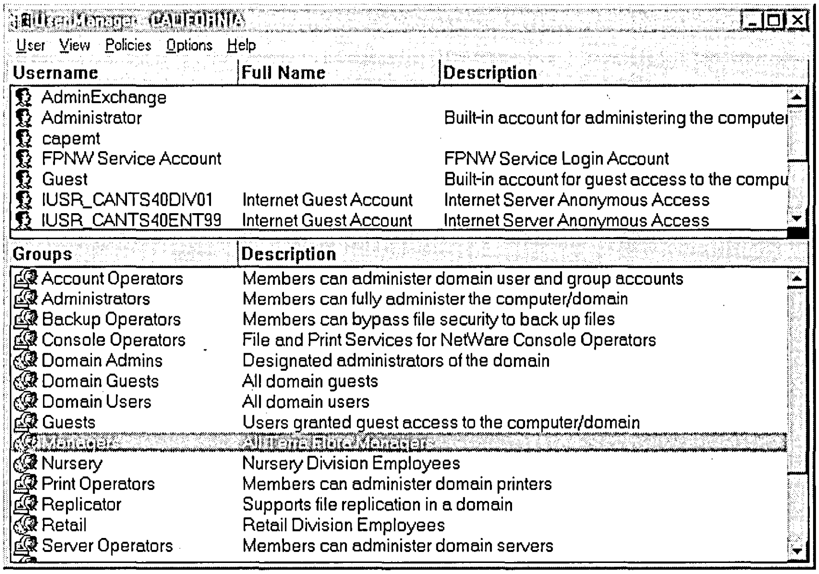
Figure 5.9 Controlling access to files by using Windows NT groups

Although Figure 5.9 depicts a single directory structure for simplicity, directories can reside on other disks or even on other network shares.

Domainwide Anonymous Access

The Anonymous access layer of Figure 5.9 demonstrates anonymous access to the root directories provided by using the anonymous account specified on the **Service** tab in the **WWW Service Properties** dialog box.

In this Terra Flora scenario, Internet Information Server is installed on a stand-alone member server, CANTS40DIV01. The default anonymous account, IUSR_CANTS40DIV01, is a local user account. Because the server will access directories on network computers in the California domain, the account is added to the California domain by using User Manager for Domains, as shown in Figure 5.10. Adding the local account IUSR_CANTS40DIV01 to the California domain enables computers in that domain to authenticate access by Internet Information Server.



Username	Full Name	Description
AdminExchange		
Administrator		Built-in account for administering the computei
capemt		
FPNW Service Account		FPNW Service Login Account
Guest		Built-in account for guest access to the compu
IUSR_CANTS40DIV01	Internet Guest Account	Internet Server Anonymous Access
IUSR_CANTS40ENT99	Internet Guest Account	Internet Server Anonymous Access

Groups	Description
Account Operators	Members can administer domain user and group accounts
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Console Operators	File and Print Services for NetWare Console Operators
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Guests	Users granted guest access to the computer/domain
Managers	All Terra Flora Managers
Nursery	Nursery Division Employees
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
Retail	Retail Division Employees
Server Operators	Members can administer domain servers

Figure 5.10 Accounts and global groups used at Terra Flora in User Manager

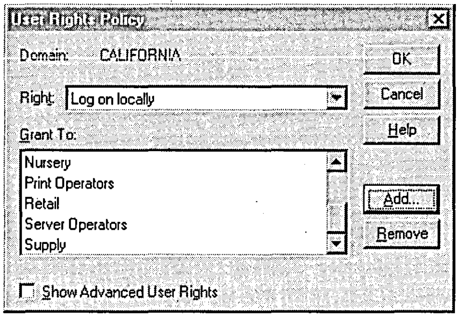
Alternatively, you can create a new account in the California domain for anonymous access and specify that account in Internet Service Manager on the **Service** tab in the **WWW Service Properties** dialog box.

Basic Authentication and Global Groups

The Basic authentication layer of Figure 5.9 demonstrates using Basic authentication and Windows NT groups to control access to subdirectories.

In Terra Flora, each department provides some information to the entire company, such as current project plans or an employee directory. However, each division or department also uses material that only its members should have access to.

To provide selective access, global groups are created for each division (Nursery, Retail, and Supply) by using User Manager on the primary domain controller, CANTS40ENT03. The Log On Locally user right is added to every user or group that will use the IIS server, as shown in Figure 5.11.


User Rights Policy

Domain: CALIFORNIA

Right: Log on locally

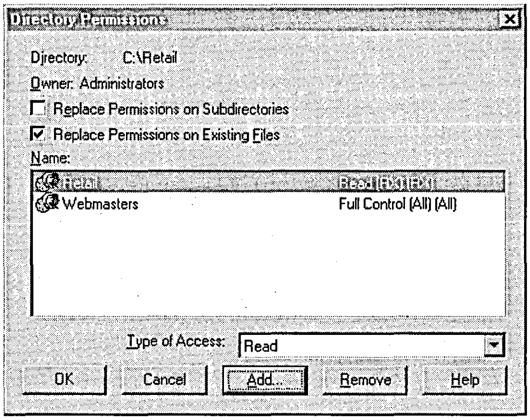
Grant To:

Nursery
Print Operators
Retail
Server Operators
Supply

□ Show Advanced User Rights

Figure 5.11 Assigning rights to groups in User Manager

You must also give the division groups read access to the directories. To do this, right-click the folder in Windows NT Explorer, then click **Properties** to specify group permissions in the **Directory Permissions** dialog box shown in Figure 5.12.


Directory Permissions

Directory: C:\Retail
Owner: Administrators
□ Replace Permissions on Subdirectories
☑ Replace Permissions on Existing Files
Name:

Retail	Read (RX) (RX)
Webmasters	Full Control (All) (All)

Type of Access: Read

Figure 5.12 Designating the security properties for a directory

To complete the security configuration, Terra Flora appoints a webmaster in each division to control content on the servers. The Webmasters group is created and populated with the three division webmasters. Only the Webmaster group is given full control to the entire directory structure.

For more information about adding global groups to a domain and adding user rights to user accounts and groups, see *Windows NT Server Concepts and Planning*.

Challenge/Response Authentication and Global Groups

The Challenge/response authentication layer in Figure 5.9 demonstrates access that is granted to managers only by using Windows NT challenge/response authentication. A global group named Managers is created and populated with the user accounts of individual managers.

Read permission on all the budget information files is granted to the group named Managers. Full Control permission on individual files is granted to the individual manager responsible for the file.

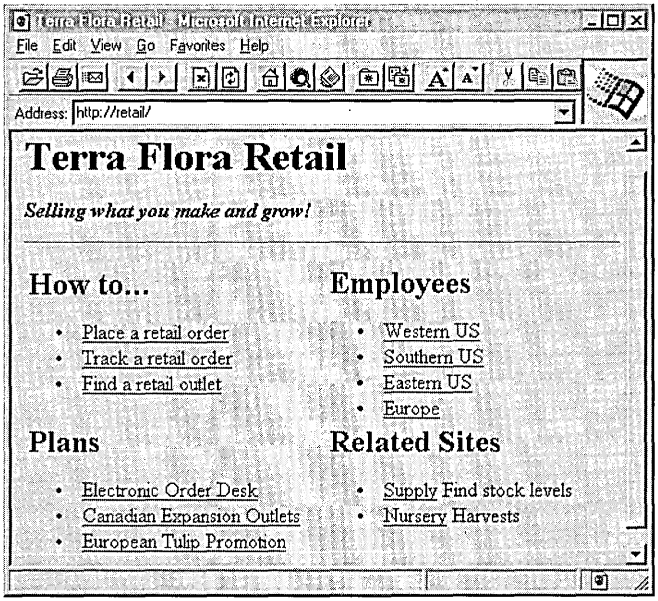
The use of Windows NT groups demonstrated in this section is scalable and can be expanded to suit your business.

For more information about domain user accounts, local accounts, and the IUSR_*computername* account, see Chapter 3, "Server Security on the Internet."

Information Distribution

This section shows how to handle typical content on a division server and presents useful strategies for your business.

The division servers provide all employees access to process documents (how-to documents), current project plans, employee home pages, and links to related pages on other division servers, as shown in Figure 5.13.


Terra Flora Retail - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://retail/

Terra Flora Retail

Selling what you make and grow!

How to...

- Place a retail order
- Track a retail order
- Find a retail outlet

Employees

- Western US
- Southern US
- Eastern US
- Europe

Plans

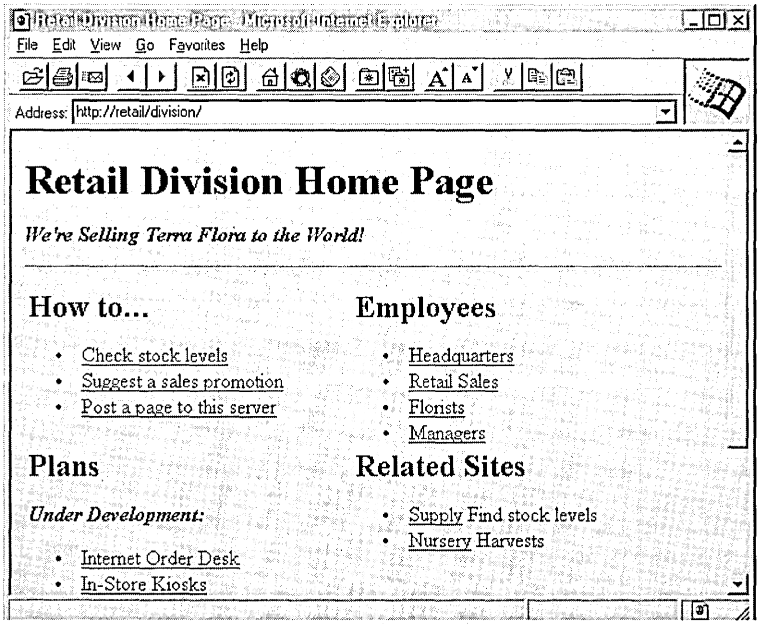
- Electronic Order Desk
- Canadian Expansion Outlets
- European Tulip Promotion

Related Sites

- Supply Find stock levels
- Nursery Harvests

Figure 5.13 Retail Division home page for entire company

Only employees in the division have access to that division's project templates, plans in development, and budgets. The Retail Division home page (Figure 5.14) shows what the employees in that division have access to.


Retail Division Home Page - Microsoft Internet Explorer
File Edit View Go Favorites Help

Address: http://retail/division/

Retail Division Home Page

We're Selling Terra Flora to the World!

How to...

- Check stock levels
- Suggest a sales promotion
- Post a page to this server

Employees

- Headquarters
- Retail Sales
- Florists
- Managers

Plans

Under Development:

- Internet Order Desk
- In-Store Kiosks

Related Sites

- Supply Find stock levels
- Nursery Harvests

Figure 5.14 Retail Division home page for Retail Division employees only

Retail employees collaborate on files in the \Division\Plans directory to create final project plans. When the plans are complete and approved, the webmaster copies the plan files to the root directory and creates links on the appropriate Hypertext Markup Language (HTML) pages so that all Terra Flora employees can read the plans.

Parallel directory structures enable you to copy entire directory structures to other servers without changing hard-coded relative links within the files. Parallel directory structures also simplify navigation, as shown in Figure 5.15.

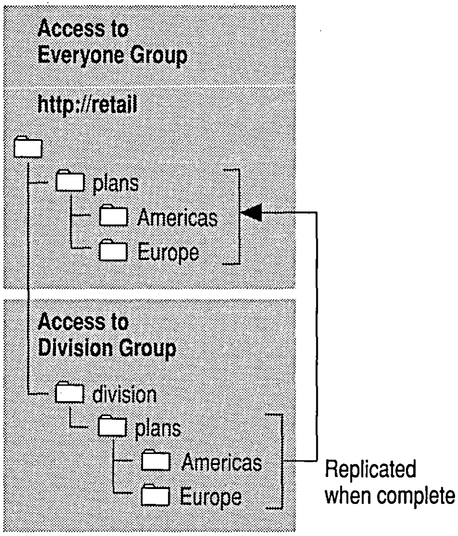


Figure 5.15 Directory structure for Retail Division

Creating Virtual Servers on the Internet

Virtual servers on the Internet are the same as virtual servers on an intranet. You must register your domain names in the worldwide Domain Name System through the *InterNIC*. The InterNIC is a cooperative activity between the National Science Foundation, Network Solutions, Inc., and AT&T to provide DNS registration services to the worldwide Internet community. You can reach the InterNIC at **http://internic.net**. Some Internet service providers register domain names with the InterNIC for you.

If your Internet clients use Internet Explorer version 2.0 or later, you can use Windows NT groups for secure authentication by using challenge/response authentication. Netscape Navigator and other browsers do not support secure authentication by using challenge/response. They use Basic authentication, which transmits user names and passwords by using base-64 encoding. Base-64 encoding can be decoded easily. Because anyone monitoring the network can decode these user names and passwords, using Basic authentication on public networks is not recommended.

Once authenticated, either by challenge/response or Basic authentication, all data is transmitted in clear text. You can use Secure Sockets Layer (SSL) to encrypt all data, but SSL uses a lot of processor time to encode and decode every shred of data passed through Internet Information Server. Therefore, SSL is usually reserved for small amounts of private information, such as credit card numbers or addresses.

For more information about SSL, see Chapter 3, "Server Security on the Internet."

Database Application Using Internet Information Server

This scenario explains how the Internet Database Connector is used to create a core-business application that streamlines Terra Flora's internal processes and eventually will accommodate an expanded customer base.

The flower arrangement order desk is the heart of Terra Flora's business. By using Internet Information Server to post to and query the retail order Oracle database, anyone in the company can use the data. This scenario establishes an internal ordering system that uses Hypertext Transport Protocol (HTTP). The internal system will serve as a pilot for an Internet ordering system, which will expand Terra Flora's market to the entire world.

This section assumes that an Oracle database already exists.

For more details on using the Internet Database Connector and related control files (.idc and .htx), see the *Windows NT Server Microsoft Internet Information Server Installation and Administration Guide.*

Database Connector Hardware Configuration

Two computers—the computer running Internet Information Server and the computer running the Oracle database—must be configured for the network.

The computer running Internet Information Server has the following hardware configuration:

- Intel 486 processor with clock speed of 50 MHz
- 24 MB of RAM
- 2 GB of free disk space

Database Connector Network Configuration

As the previous section mentioned, you must configure two computers for the network. Figure 5.16 highlights the components in the Terra Flora network that are involved in using the IIS Internet Database Connector.

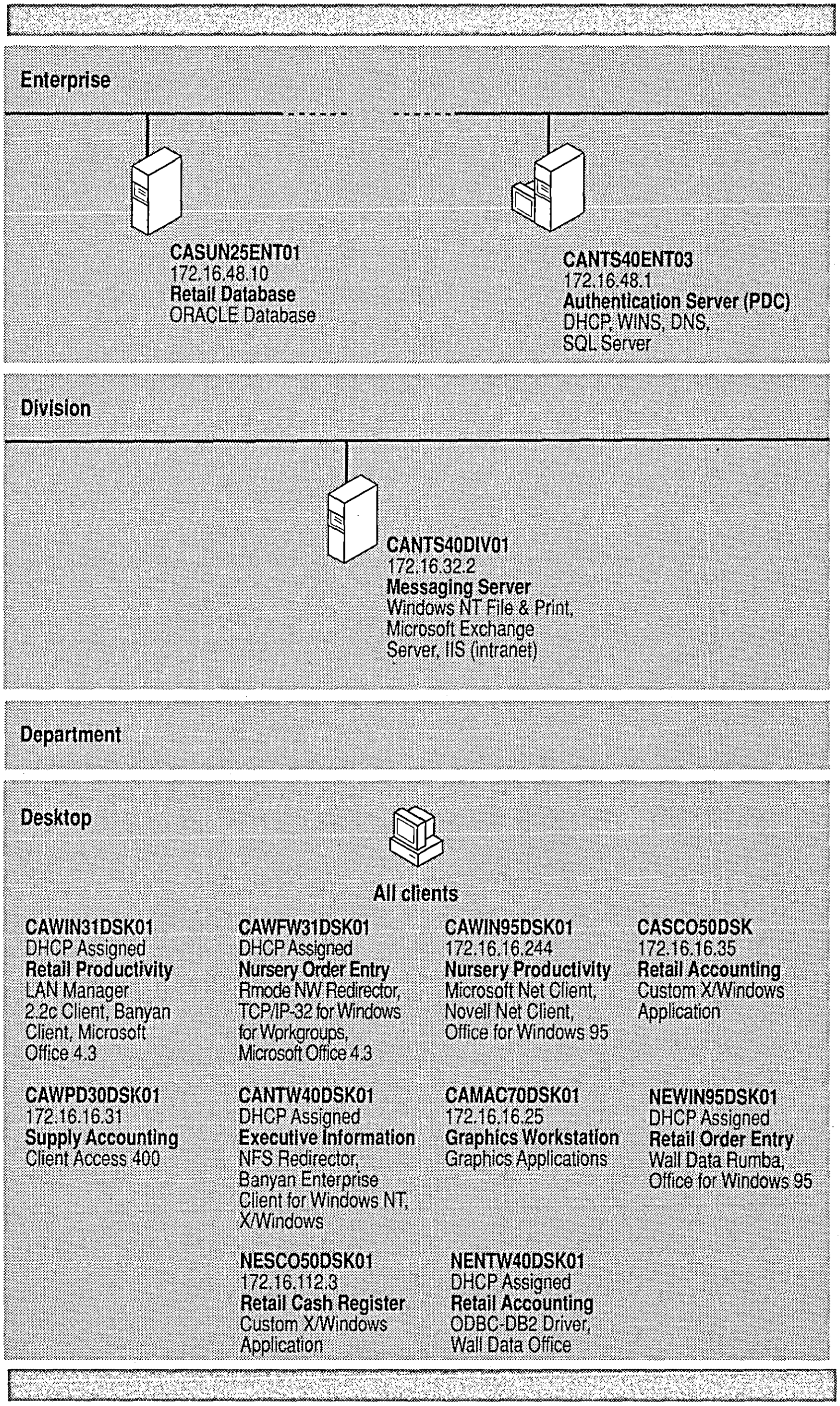


Figure 5.16 Database connector network overview

TCP/IP Properties of the Computer Running the Database Connector

The IP address and all TCP/IP properties for the computer named ORDERDESK are dynamically assigned by the network DHCP server CANTS40ENT03 during computer startup. The WINS server, also on CANTS40ENT03, is also notified of the IP address and the computer name of ORDERDESK.

Name Resolution of the Computer Running the Database Connector

The NetBIOS computer name of the computer hosting the IIS server is ORDERDESK. All Internet Information Server clients will use this NetBIOS computer name.

Internet Explorer clients automatically query the WINS server when a request uses the name of a computer, for example, **http://orderdesk**. The WINS server provides the IP address currently assigned by DHCP to that computer name. The DHCP assignment and WINS registration process is dynamic. Therefore, regardless of the IP address currently assigned to ORDERDESK, Internet Explorer users can always resolve **http://orderdesk** to the current IP address by using the WINS server.

Networks that do not use WINS can use an alternative name resolution system, usually DNS servers. DNS servers resolve a domain name—such as orderdesk.terraflora.com—to an IP address.

Typically, you add the IP address and domain name to your local DNS server. On Terra Flora's network, the DNS server is CANTS40ENT03. For information about configuring the DNS server, see the section "Virtual Server Name Resolution" earlier in this chapter.

After the DNS server is configured, users can then access the IIS server by using either the NetBIOS computer name (if WINS is supported on the client) or the domain name (if DNS is supported on the client), as shown in Table 5.3.

Table 5.3 ORDERDESK Computer Name Used in URLs

NetBIOS name	Computer name used in URL with WINS name resolution	Domain name URL used by DNS name resolution
ORDERDESK	**http://orderdesk**	**http://orderdesk.terraflora.com**

For more information on WINS and DNS interoperability, see the *Windows NT Server Networking Guide*.

Creating a System Data Source

You need no special configuration in Internet Service Manager to implement database connectivity by using Internet Database Connector. The Httpodbc.dll module supplies database connectivity. Httpodbc.dll is automatically loaded when Internet Information Server starts. To install Httpodbc.dll, you select the **ODBC** option during Internet Information Server setup.

Prior to using the database, you must create a system *Data Source Name(DSN).* The Data Source Name is a logical name used by Windows NT Open Database Connectivity (ODBC) to refer to the driver and any other information required to access the data, such as the actual server name or location of the database. You specify the Data Source Name in Internet Database Connector files to tell Internet Information Server where to access the data. For more information about using the DSN in .idc files, see "Accessing the Database," later in this section.

The simplest method to create a DSN is to use the sample pages provided with Internet Information Server. To access the sample pages, first make sure your World Wide Web (WWW) service is running. Then use Internet Explorer to access your own IIS server. For example, type **http://orderdesk** in the location box. The Database page contains a hyperlink to create the system data source. The manual method for creating a data source follows.

▷ **To create a system data source**

1. Double-click **ODBC** in **Control Panel.**

   The **Data Sources** dialog box appears. Other data sources appear in the list if you previously installed other ODBC drivers.

2. Click **System DSN**. In the **System Data Sources** dialog box, click **Add.**

   Important: Be sure to click **System DSN**. The Internet Database Connector works only with system DSNs.

3. In the **Add Data Source** dialog box, select an ODBC driver in the list box, then click **OK.**

   A dialog box specific to your driver appears. To install third-party ODBC drivers, see your third-party database documentation.

4. In the dialog box specific to your driver, enter the name of the data source and any other required information, then click **OK.**

   The **System Data Sources** dialog box appears again, but now it has the name of the data source displayed.

   If you do not know what to enter in the dialog box specific to your driver, accept the defaults. To find out the details, click **Help** and find the section that describes your network.

5. To close the **System Data Sources** dialog box, click **Close.** To close the **Data Sources** dialog box, click **Close** again.
6. To complete the ODBC and DSN setup, click **OK.**

Placing the .idc and .htx Files

After the Data Source Name is created, you can begin to create the Internet Database Connector (.idc) files that will be used to post and query data from the database, and the .htx files that will be used to format the results returned from it.

Place the .idc and .htx files in the /Scripts directory or another Internet Information Server directory configured with the Execute property. You mark a directory with the Execute property when you add or edit the directory on the **Directory** property sheet.

For details on creating the .idc and .htx files, see the section "Accessing the Database" later in this chapter, or the *Windows NT Server Microsoft Internet Information Server Installation and Administration Guide.*

Database Connectivity Security

Security for database connectivity consists of configuring access to:

- Internet Information Server files.
- The database.

You use Windows NT and Internet Information Server security when accessing the .idc and .htx files. Users must have permission to access these files in the same way as any other file made available through Internet Information Server. The Terra Flora intranet uses anonymous access. Therefore, the properties of the .idc and .htx files must permit access by the IUSR_*computername* account or by the account specified for anonymous access.

Also, the .idc file lists a user name and (optionally) a password, which must be valid on the ODBC data source. If the .idc file does not list a user name and password, the user name and password used by Internet Information Server are presented to the ODBC data source.

If you use anonymous access or Basic authentication, the password used by Internet Information Server works on any remote data source if the user name and password are valid for logon to that data source. Windows NT challenge/response authentication works only when a computer is running both Windows NT Internet Information Server and Microsoft SQL Server. For more information, see the next section, "Using Windows NT Challenge/Response for Microsoft SQL Server Access."

Using Windows NT Challenge/Response for Microsoft SQL Server Access

If you are running Microsoft SQL Server and Internet Information Server on the same computer, you can use integrated SQL Server security to pass encrypted user names and passwords for database access. SQL Server must be configured for integrated security. Integrated SQL Server security enables you to use the encrypted user name and password given by an Internet Information Server user for access to SQL Server.

If you use integrated SQL Server security, you do not provide a user name and password in the .idc file. For more information about configuring integrated security, see your SQL Server documentation.

Before you can set up Internet Information Server and SQL Server with integrated Windows NT security, you must install both on the same computer.

To set up integrated Windows NT security, select the **Windows NT Challenge/Response** check box on the **Service** property sheet. Clients must use Internet Explorer version 2.0 or later. Specify Local Server as the System Data Source in your .idc file.

Windows NT user names must adhere to SQL Server integrated security name rules. Underscores, dollar signs, and pound signs are not allowed. The default account IUSR_*computername* cannot be used.

Accessing the Database

Terra Flora has an existing table in its order database. This table is used to process retail orders. The ability to access existing stores of information is the primary benefit of using Internet Information Server at Terra Flora.

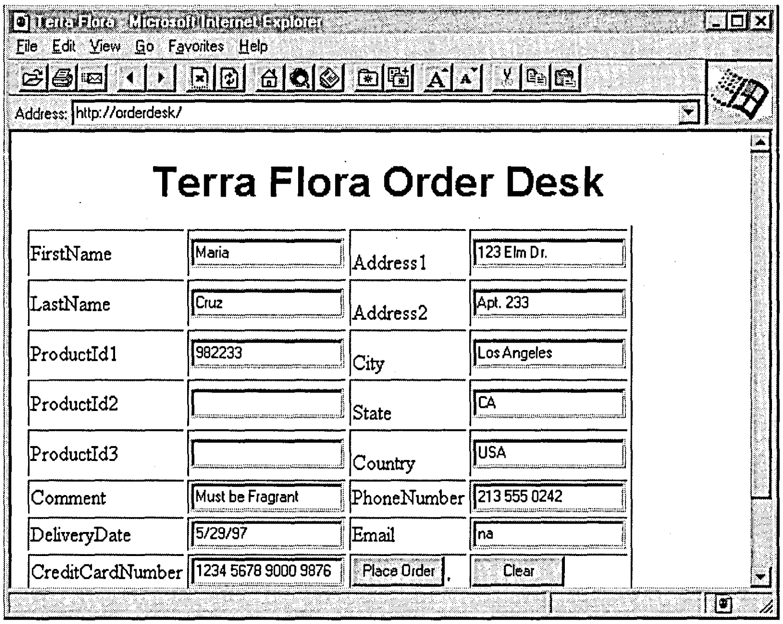
Users enter data into the database by using an HTML form, as shown in the .htm file in Figure 5.17.

```
<HTML>
<HEAD>
<TITLE>Terra Flora</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF">
<H1 Align = "Center"><CENTER><FONT SIZE=6 COLOR=#000000
FACE="Arial">Terra
Flora Order Desk</FONT><FONT SIZE=6> </FONT></CENTER></H1>
<FORM ACTION="/secure/Order.idc" METHOD = "POST">
<P>
<TABLE BORDER=2 BORDER BGCOLOR="#FFFFFF">
<TR><TD>FirstName</TD><TD><INPUT NAME="FirstName" VALUE="" &lt;/TD>
</TD><TD><BR>
```

```
Address1</TD><TD><A NAME="UQHTML0"></A><INPUT NAME="Address1" VALUE=""
&lt;/TD>
</TD></TR>
<TR><TD>LastName</TD><TD>
<INPUT NAME="LastName" VALUE="" &lt;/TD>
</TD><TD><BR>
Address2</TD><TD><INPUT NAME="Address2" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>ProductId1</TD><TD><INPUT NAME="ProductId1" VALUE="" &lt;/TD>
</TD><TD>
<BR>
City</TD><TD><INPUT NAME="City" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>ProductId2</TD><TD><INPUT NAME="ProductId2" VALUE="" &lt;/TD>
</TD><TD>
<BR>
State</TD><TD><INPUT NAME="State" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>ProductId3</TD><TD><INPUT NAME="ProductId3" VALUE="" &lt;/TD>
</TD><TD>
<BR>
Country</TD><TD><INPUT NAME="Country" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>Comment</TD><TD><INPUT NAME="Comment" VALUE="" &lt;/TD>
</TD><TD>PhoneNumber</TD><TD>
<INPUT NAME="PhoneNumber" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>DeliveryDate</TD><TD><INPUT NAME="DeliveryDate" VALUE=""
&lt;/TD>
</TD><TD>Email</TD><TD>
<INPUT NAME="Email" VALUE="" &lt;/TD>
</TD></TR>
<TR><TD>CreditCardNumber</TD><TD><INPUT NAME="CreditCardNumber" VALUE=""
&lt;/TD>
</TD><TD>
<INPUT TYPE="SUBMIT" VALUE="Place Order" ALIGN="MIDDLE"></P>
</TD><TD><INPUT TYPE="RESET" NAME="reset" VALUE="Clear" ALIGN="MIDDLE">
</TD></TR>
</TABLE>
<P>
</FORM>
<P>
<HR=2>
</BODY>
</HTML>
```

Figure 5.17 Sample .htm file for Terra Flora order desk

Figure 5.18 shows the results of this .htm file in Internet Explorer.


Terra Flora - Microsoft Internet Explorer
File Edit View Go Favorites Help
Place Order
Clear

Address: http://orderdesk/

Terra Flora Order Desk

FirstName	Maria	Address1	123 Elm Dr.
LastName	Cruz	Address2	Apt. 233
ProductId1	982233	City	Los Angeles
ProductId2		State	CA
ProductId3		Country	USA
Comment	Must be Fragrant	PhoneNumber	213 555 0242
DeliveryDate	5/29/97	Email	na
CreditCardNumber	1234 5678 9000 9876	Place Order	Clear

Figure 5.18 Terra Flora order desk file displayed by Internet Explorer

When a user clicks the **Place Order** button, the data is processed by using the .idc file shown in Figure 5.19.

```
Datasource: OrderDB
Template: Order.htx
SQLStatement:
+INSERT INTO "OrderDB" ("FirstName", "LastName", "Email", "PhoneNumber",
"CreditCardNumber", "Address1", "Address2", "City", "State", "Country",
"ProductId1", "ProductId2", "ProductId3", "Comment", "DeliveryDate")
+VALUES ('%FirstName%', '%LastName%', '%Email%', '%PhoneNumber%',
'%CreditCardNumber%', '%Address1%', '%Address2%', '%City%', '%State%',
'%Country%', '%ProductId1%', '%ProductId2%', '%ProductId3%',
'%Comment%', '%DeliveryDate%');
#IDC-Insert FrontHTM-default.htm ReportHTX-Order.htx
```

Figure 5.19 Sample .idc file for Terra Flora order desk

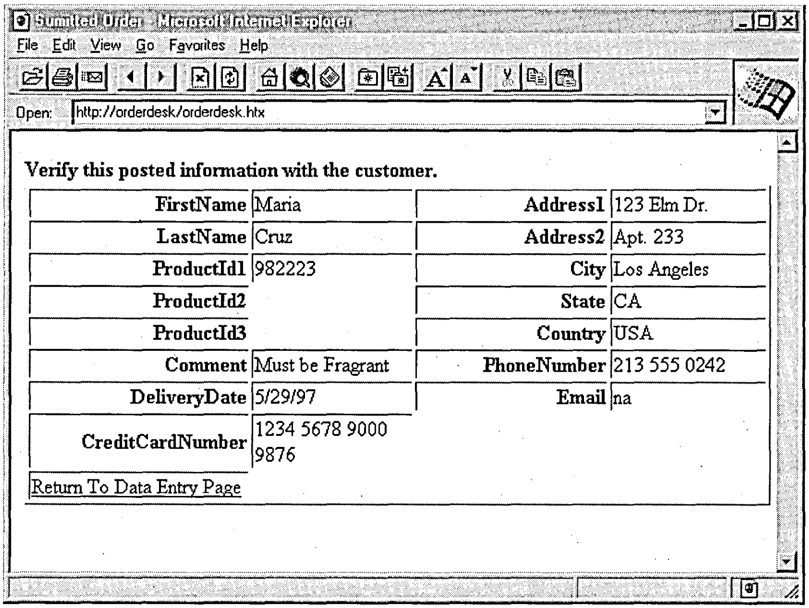
The .idc file then posts the information to the database and results are formatted by using the .htx file specified in the .idc file, Order.idc, as shown in Figure 5.20.

```
<HTML>
<HEAD>
<TITLE>Submitted Order</TITLE>
</HEAD>
```

```
<BODY BGCOLOR="#FFFFFF">
<P>
<B>Verify this posted information with the customer.<BR>
</B>
<P>
<TABLE BORDER=2 BORDER BGCOLOR="#FFFFFF">

<TR><TD ALIGN="RIGHT"><B>FirstName</B></TD><TD><%IDC.FIRSTNAME%>
</TD><TD ALIGN="RIGHT"><B>Address1</B></TD><TD><%IDC.ADDRESS1%>
</TD></TR>

<TR><TD ALIGN="RIGHT"><B>LastName</B></TD><TD><%IDC.LASTNAME%>
</TD><TD ALIGN="RIGHT"><B>Address2</B></TD><TD><%IDC.ADDRESS2%>
</TD></TR>

<TR><TD ALIGN="RIGHT"><B>ProductId1</B></TD><TD><%IDC.PRODUCTID1%>
</TD><TD ALIGN="RIGHT"><B>City</B></TD><TD><%IDC.CITY%></TD></TR>

<TR><TD ALIGN="RIGHT"><B>ProductId2</B></TD><TD><%IDC.PRODUCTID2%>
</TD><TD ALIGN="RIGHT"><B>State</B></TD><TD><%IDC.STATE%></TD>
</TR>

<TR><TD ALIGN="RIGHT"><B>ProductId3</B></TD><TD><%IDC.PRODUCTID3%>
</TD><TD ALIGN="RIGHT"><B>Country</B></TD><TD><%IDC.COUNTRY%>
</TD></TR>

<TR><TD ALIGN="RIGHT"><B>Comment</B></TD><TD><%IDC.COMMENT%></TD><TD
ALIGN="RIGHT"><B>PhoneNumber</B>
</TD><TD><%IDC.PHONENUMBER%></TD></TR>

<TR><TD ALIGN="RIGHT"><B>DeliveryDate</B></TD><TD><%IDC.DELIVERYDATE%>
</TD><TD ALIGN="RIGHT"><B>Email</B></TD><TD><%IDC.EMAIL%></TD>
</TR>

<TR><TD
ALIGN="RIGHT"><B>CreditCardNumber</B></TD><TD><%IDC.CREDITCARDNUMBER%>
</TD><TD></TD><TD></TD></TR>

</TABLE>

<P>

<P>
<A HREF="/default.htm">Return To Data Entry Page</A>
<P>
</BODY>
</HTML>
```

Figure 5.20 Sample .htx file for Terra Flora order desk

The process is complete when the database returns confirmation through the .htx file, as shown in Figure 5.21.


Sumitted Order - Microsoft Internet Explorer
File Edit View Go Favorites Help
Open: http://orderdesk/orderdesk.htx

Verify this posted information with the customer.

FirstName	Maria	**Address1**	123 Elm Dr.
LastName	Cruz	**Address2**	Apt. 233
ProductId1	982223	**City**	Los Angeles
ProductId2		**State**	CA
ProductId3		**Country**	USA
Comment	Must be Fragrant	**PhoneNumber**	213 555 0242
DeliveryDate	5/29/97	**Email**	na
CreditCardNumber	1234 5678 9000 9876		

Return To Data Entry Page

Figure 5.21 Terra Flora order desk confirmation .htx file in Internet Explorer

Internet Considerations for Database Connectivity

When you use database connectivity over the Internet, you must use the Secure Sockets Layer protocol to confidentially obtain credit card numbers, addresses, or any other information that should not be divulged to others.

The SSL protocol provides communication privacy over networks by using a combination of public key cryptography and bulk data encryption for data privacy. By using this protocol, clients and servers can communicate in a way that prevents eavesdropping, tampering, or message forgery.

For optimum efficiency, store the form requesting confidential information in a directory not enabled for SSL, but set the confidential information to return to an SSL-enabled directory. This directory is specified in the button used to submit the form, as illustrated in Figure 5.22.

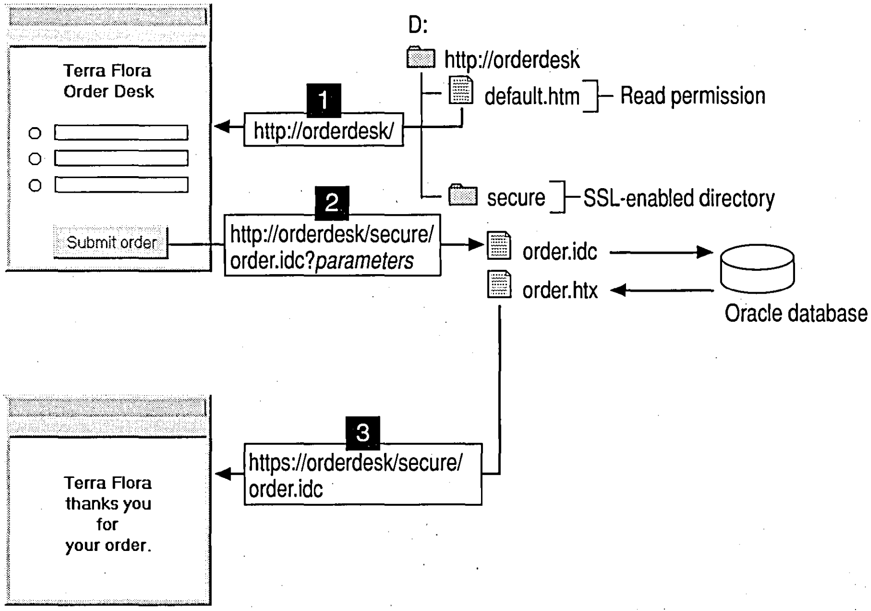


Figure 5.22 SSL process and directory configuration

Step 1 shows the order form sent to the client from a directory that is not enabled for SSL. Step 2 demonstrates that the completed form, with address and credit card information, is sent back to an SSL-enabled directory by clicking **Submit order**, which runs the request **https://orderdesk/secure/order.idc?***parameters*. Step 3 shows that the response is returned to the client through Order.htx.

For more information about SSL, see Chapter 3, "Server Security on the Internet."

Internet Information Server FTP and Gopher Services

In this scenario, the Terra Flora Human Resources department is setting up methods to ensure that all employees have access to Human Resources information currently provided through the WWW service. Some employees still use computers that run the MS-DOS or UNIX operating system; they cannot use Internet Explorer. And in addition to reading files, some Human Resources employees need to add and delete files by using the File Transfer Protocol (FTP) service.

Terra Flora adds the FTP and Gopher services to the same computer running the WWW service that was installed in the scenario described in "Internet Information Server as a Single Intranet Server" in Chapter 4. Human Resources employees will use the FTP service to maintain the files. All other employees can use the FTP or Gopher service to view the files.

Internet Information Server FTP and Gopher Services Hardware Configuration

The existing file and print server is two years old. The low system demands of Internet Information Server, including FTP and Gopher, will not significantly impact file and print server performance. Therefore, it is practical to run all three Internet Information Server services on this older hardware:

- Intel 486 processor with clock speed of 66 MHz
- 32 MB of RAM
- 1 GB disk space

Internet Information Server FTP and Gopher Services Network Configuration

The computer used for the intranet server is the same computer running the WWW service that was installed in the scenario described in "Internet Information Server as a Single Intranet Server" in Chapter 4. For a complete description of the network configuration for the FTP and Gopher services, see that section of Chapter 4.

The computer used is similar to the computer CANTS40DPT01 in the Terra Flora network diagram. See Figure 5.23 for a diagram of the network configuration.

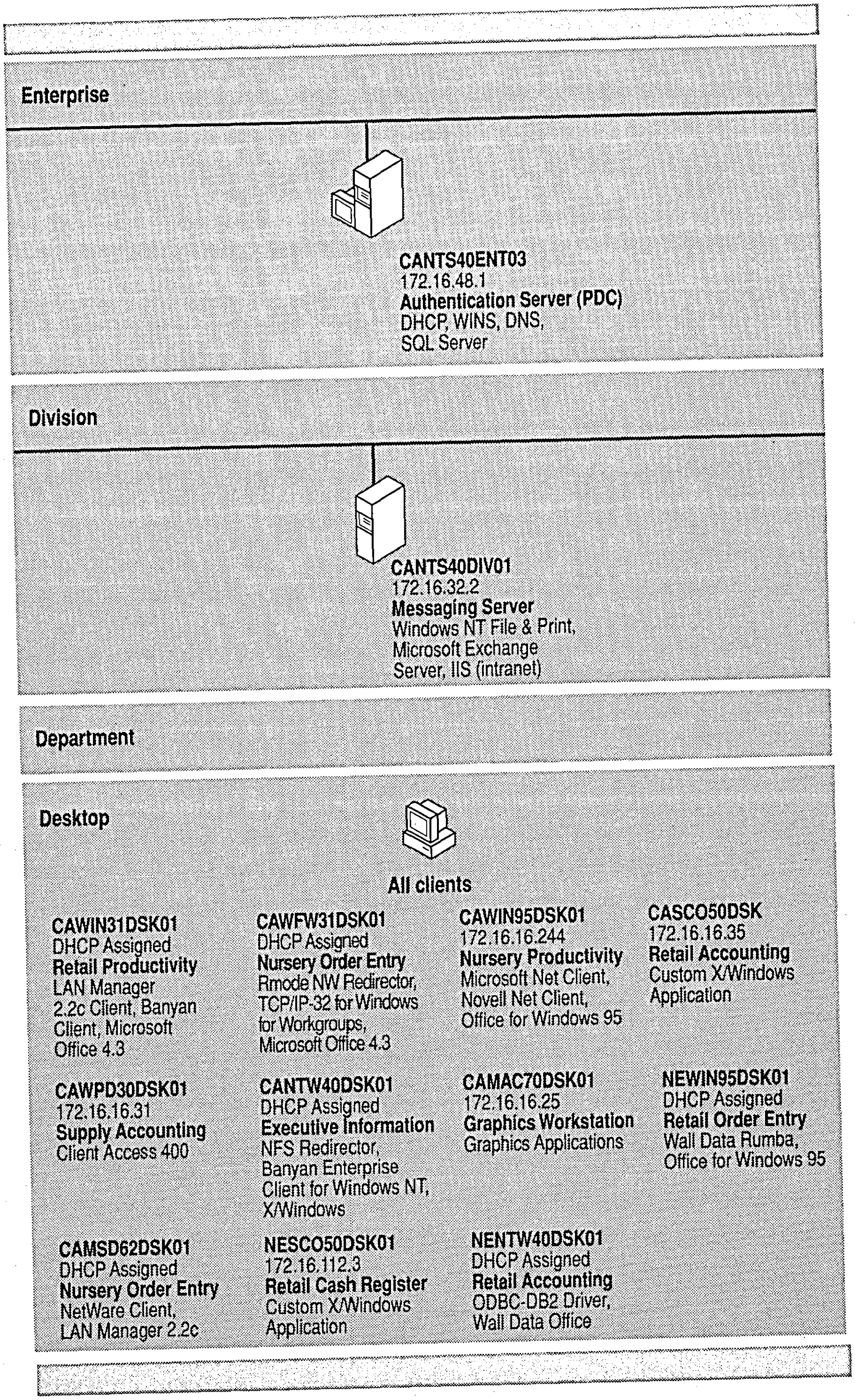


Figure 5.23 FTP and Gopher services network overview

Name Resolution for FTP and Gopher Services

After name resolution is configured as described in Chapter 4, users can then access the Internet Information Server FTP and Gopher services by using either the NetBIOS name if WINS is supported on the client) or the domain name (if DNS is supported on the client), as shown in Table 5.4.

Table 5.4 Computer Names in URLs for FTP and Gopher Services

NetBIOS name	Computer name used in URL with WINS name resolution	Domain name URL used by DNS name resolution
HR	**ftp://hr** **gopher://hr**	**ftp://hr.terraflora.com** **gopher://hr.terraflora.com**

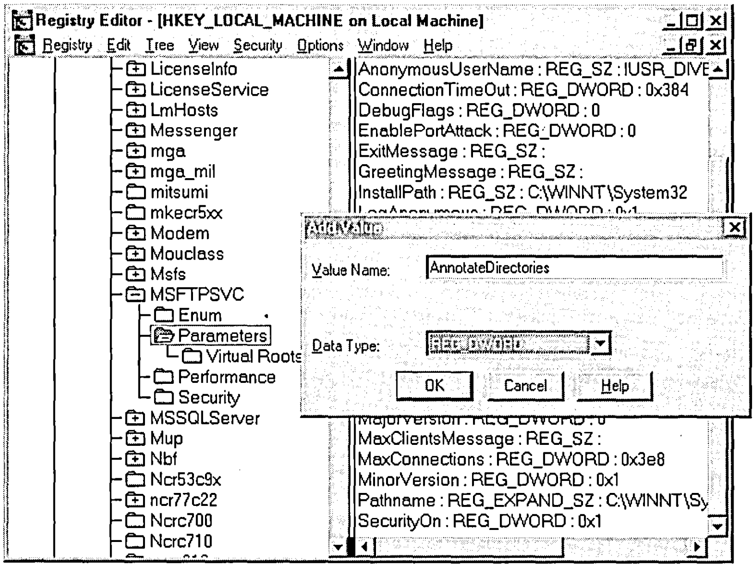
Control Files and Related Configuration

The FTP and Gopher services are configured to have the same home directory as the WWW service (wwwroot). Therefore, the same set of information is available through all services. Although no additional configuration is necessary, some additional configuration enhancements are described in the following two sections. They describe files and settings used to enhance the FTP and Gopher services that are not part of the default installation of Internet Information Server.

FTP Service Configuration

The FTP service allows you to use *directory annotations*, that is, comments about each directory. Because virtual directories do not appear in FTP listings, you use directory annotations to display additional virtual directories that can be traversed by the employees.

To annotate files, first use Registry Editor (run **Regedt32.exe** or **Regedit.exe**) to enable annotated directories by adding the **AnnotateDirectories** value to the HKEY_LOCAL_MACHINE/System key, as shown in Figure 5.24.



AnonymousUserName : REG_SZ : IUSR_DIVE
ConnectionTimeOut : REG_DWORD : 0x384
DebugFlags : REG_DWORD : 0
EnablePortAttack : REG_DWORD : 0
ExitMessage : REG_SZ :
GreetingMessage : REG_SZ :
InstallPath : REG_SZ : C:\WINNT\System32
MaxClientsMessage : REG_SZ :
MaxConnections : REG_DWORD : 0x3e8
MinorVersion : REG_DWORD : 0x1
Pathname : REG_EXPAND_SZ : C:\WINNT\Sy
SecurityOn : REG_DWORD : 0x1

Value Name: AnnotateDirectories

Data Type: REG_DWORD

Figure 5.24 Adding the FTP service's AnnotateDirectories value to the Registry

AnnotateDirectories is added to:

HKEY_LOCAL_MACHINE
\System
\CurrentControlSet
\Services
\MSFTPSVC
\Parameters

Entry syntax is:

AnnotateDirectories REG_DWORD 0x0 | 0x1

The default value for **AnnotateDirectories** is 0x0 (false—that is, directory annotation is off).

This Registry value defines the default behavior of directory annotation for newly connected users. When this value is 0x1 (true), directory annotation is enabled. This Registry entry does not appear by default, so you must add this entry to the Registry if you want to change its default value.

The directory annotations are stored in each directory in a text file named ~ftpsvc~.ckm. This is usually a hidden file, so directory listings do not display this file. Because some browsers display only the first line, you should keep the annonotation text to one line. For example,

```
See ftp://eunts40dpt05/seville for Seville's HR records.
```

Gopher Service Configuration

All information about a Gopher item that is sent to a client comes from tag files. This information includes the name of a file displayed for the client. Typical tag files contain:

- A display filename.
- A host name (that is, where the item is located).
- A port number.

The **Gdsset** program is a simple command-line tool that is used to create and set tags. In the following example, you see how to use it to add a link to Terra Flora's Gopher server in Seville.

First, create a tag file to make a link to the home directory on a Gopher server at the Seville site. Add an empty text file called link1 to the Gopher home directory. Issue the following command at the command prompt:

```
gdsset -l -g1 -f "Link to Seville HR Gopher Server" -s "" -h
eunts40div05.terraflora.com linkl
```

For more examples of using **Gdsset**, see the *Internet Information Server Installation and Administration Guide.*

Tag files are stored as hidden .gtg or .lnk files on File Allocation Table (FAT) partitions. On Window NT File System (NTFS) partitions, they are stored in a data fork of the tag file. When you move data files, you must remember to manually move the corresponding tag files if they exist on FAT partitions. When you move data files on NTFS partitions, use Windows NT Explorer and not the command-prompt **copy** command because **copy** does not copy the data forks.

If disk space is critical, do not forget to include the hidden tag files when you calculate the space the files will require. The size of the file depends on the size of the friendly name, host name, selector, and other information.

If you use Gopher+ clients, you can add more information to each tag file, such as the server administrator's name and e-mail address, and the file's date of creation and date of last modification.

Note The Internet Information Server Gopher service supports some Gopher+ additions: Info, Admin, and URL attribute blocks. But it does not support the Abstract or Ask Form attributes. For more information about Internet Information Server and Gopher, see the *Internet Information Server Installation and Administration Guide.*

Using Security with the FTP and Gopher Services

FTP and Gopher use anonymous access. In addition, FTP uses Basic authentication in conjunction with Windows NT groups for restricted administration of the files.

Anonymous FTP Access

MS-DOS clients and some UNIX clients do not have or cannot use an HTTP or Gopher browser such as Internet Explorer. These clients can use any FTP client to browse the files on HR. To accomplish this, the IUSR_CANTS40DIV01 user account was granted read-only access to the files.

Anonymous Gopher Access

The Human Resources department must provide information to the entire company, such as benefits summaries and company policies. All Gopher access is anonymous through the IUSR_HR user account. This local user account was added to the California domain database on CANTS40ENT03 and was granted the Log On Locally user right.

If Internet Information Server were installed on a primary domain controller (PDC) or a backup domain controller (BDC), the IUSR_*computername* account would automatically be added to the domain database it supports and the steps above would be unnecessary.

For more information about server roles and accounts used with Internet Information Server, see Chapter 3, "Server Security on the Internet."

FTP Site Administrative Access

You use Windows NT groups to provide selective access for remote division employees who must maintain (create and delete) files on the HR server.

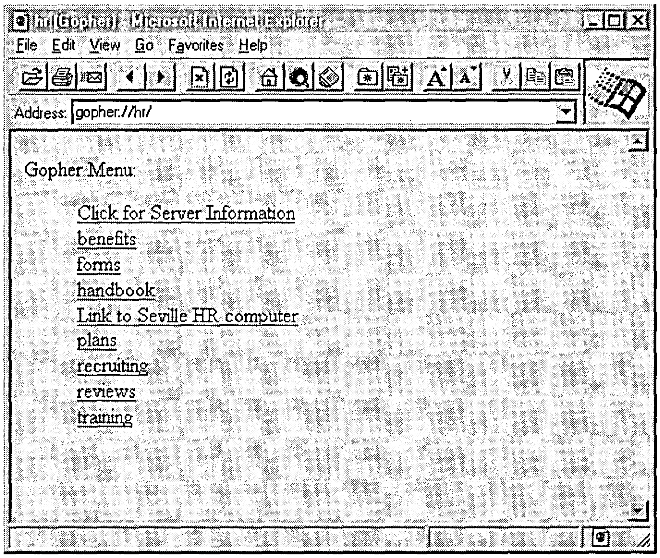
The Gopher and FTP site primarily uses a single directory structure for simplicity, although some directories reside on network drives.

Only clear-text authentication is supported with the FTP server. Because it has been determined that there is low risk of an employee sniffing Terra Flora's private intranet for user names and passwords, FTP administrators can log on to the FTP server by using their network user name and password. After they are authenticated, the FTP administrators can use FTP commands to create, move, and delete files or directories.

Using groups for selective access in FTP is similar to the process described earlier in this chapter in the section, "Using Groups for Selective Access." See that section for more discussion about using groups with Internet Information Server.

Content Provided

The Human Resources server provides information to the entire company, such as the employee handbook, training documents, personnel review documents, and company forms. Since directory names and filenames help provide the structure, the HR department kept this in mind when creating filenames, directory names, and directory structure, as shown in Figure 5.25.


hr (Gopher) - Microsoft Internet Explorer
File Edit View Go Favorites Help

Address: gopher://hr/

Gopher Menu:

- Click for Server Information
- benefits
- forms
- handbook
- Link to Seville HR computer
- plans
- recruiting
- reviews
- training

Figure 5.25 FTP and Gopher directory structure and filenames

In addition, Gopher tag files are used with the Gopher service to provide additional information about files and directories and to provide links to other computers. For more information about using Gopher tag files and an example of the tag files used on the Terra Flora Gopher server, see the section in this chapter, "Gopher Service Configuration."

FTP and Gopher on the Internet

The FTP logon is in clear text. Because of this, having an FTP site on the Internet that uses valid network user names and passwords could compromise your intranet's security. FTP sites on the Internet usually allow anonymous access only.

Gopher logon is anonymous only. Secure Gopher access is not possible.

Some client browsers do not display FTP directory listings that use the FTP service's default MS-DOS style. You can change the default listing style by using options on the **Service** property sheet for the FTP service.

Using and Upgrading the Windows NT 3.x FTP Server

If the FTP Server service from Windows NT version 3.51 or earlier is installed and running on your system, it will continue to run without modification under Windows NT 4.0.

However, if you install the Internet Information Server FTP service, the FTP Server service from Windows NT version 3.51 or earlier will be disabled. Both FTP services cannot run simultaneously.

You can upgrade your Windows NT 3.51 or earlier FTP service to Internet Information Server version 2.0. You must change the Internet Information Server FTP service home directory to the previous location. The FTP service continues to operate in the same way as the Windows NT 3.51 or earlier version of the FTP service.

Note The Windows NT 3.51 or earlier FTP service permitted users to traverse the directory structure above the specified FTP root. Internet Information Server removes this capability.

CHAPTER 6

Internet Connectivity Scenarios Using the Remote Access Service

This chapter gives an overview of Internet support that uses Dial-Up Networking and the Remote Access Service. It then details how Windows NT Server 4.0 can be deployed as an Internet gateway server.

For information about the Point-to-Point Tunneling Protocol (PPTP), see the *Windows NT Server Networking Supplement* and the *Microsoft Windows NT Server Resource Kit: Windows NT Server Networking Guide*.

Connecting to the Internet with Windows NT

Traditionally, connecting to the Internet has been a difficult process that is daunting for a beginner. Early tools, such as FTP (File Transfer Protocol) and Telnet, featured character-based commands suited for those who knew how to connect and maneuver through the intertwined network with 32-bit IP addresses. Today's tools, such as Internet Explorer, provide front-end viewers that enable users to scan and search for information without much knowledge of how information is stored and without having to log on to the source computer.

Windows NT provides and works with tools that make it easier to connect to the Internet.

- *Dial-Up Networking* is the software that enables clients to connect to remote computers, such as an Internet service provider.
- *Remote Access Service (RAS)* is the software that enables a computer running Windows NT to accept calls from remote computers. The remote computer can use Windows Dial-Up Networking or any other Point-to-Point Protocol (PPP) dial-up client.

Both Dial-Up Networking and RAS are included in Windows NT Workstation and Windows NT Server.

This section presents four scenarios for connecting to the Internet by using Windows NT Dial-Up Networking and Remote Access Service.

For more information about Remote Access Service and Dial-Up Networking, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

Dial-Up Client Connections

By using Windows NT and Dial-Up Networking, a user can make an Internet Protocol (IP) connection to a dial-up Internet host by using the Point-to-Point Protocol (PPP). Speeds from 2400 bits per second (bps) up to 128,000 bps are supported. After the Dial-Up Networking connection is established, the user can choose from a variety of tools—from the traditional and nongraphical to those that fully exploit the Windows interface.

For information about	See
Connecting to the Internet by using Dial-Up Networking	*Microsoft Windows NT Workstation Resource Kit: Windows NT Workstation Resource Guide*, Chapter 35, "Using Windows NT Workstation on the Internet"
Installing and using Dial-Up Networking	*Windows NT Workstation Start Here*

Simple Internet Router Using PPP

On small intranets (an intranet with less than 20 computers), a computer running Windows NT Server can use Dial-Up Networking, simple TCP/IP (Transmission Control Protocol/Internet Protocol) routing, and a PPP connection to an Internet service provider to create an Internet gateway for the computers on the small intranet. This configuration enables you to connect intranet clients to the Internet, as shown in Figure 6.1.

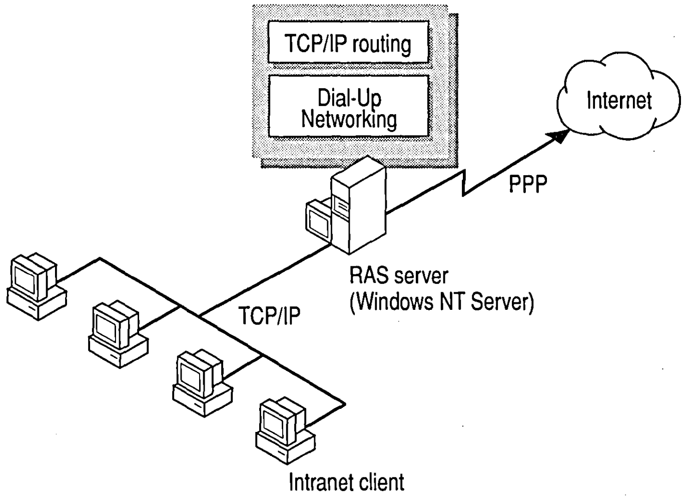


Figure 6.1 Windows NT Server as a static Internet router with PPP

In this scenario, the computer running Windows NT Server has a Dial-Up Networking connection to an Internet service provider (ISP). Static TCP/IP routing is enabled, and a static routing table is created for the computers on the private network. Routing information must also be provided to the Internet service provider because simple TCP/IP routing does not use the routing information protocol (RIP) to communicate with the ISP's router. The routing information enables the routers to route traffic to and from the Internet to computers on the private network.

This configuration can also support a very light-duty server running Internet Information Server.

For this scenario, you need to install and configure the following hardware or services:

- A computer running static TCP/IP routing with a static routing table
- TCP/IP networking protocol on all computers that will use the Internet
- Dial-Up Networking on the server that will dial in to the Internet service provider
- A modem
- Network interface cards on all computers
- Internet browsers, such as Internet Explorer, on all computers that will access the Internet
- Internetwide domain name resolution, as described in the section, "Establishing an Internet Connection," in Chapter 2, "Connecting Windows NT Server to the Internet."

For more information about simple TCP/IP routing and Dial-Up Networking, see the *Windows NT Server Networking Supplement* and the *Windows NT Server Resource Kit Networking Guide.*

Internet Service Provider

In this scenario, an Internet service provider uses Windows NT Server to set up an information service network. The network provides an Internet connection and other network services, including a mail server, fax server, database hosting, software distribution, and other custom applications.

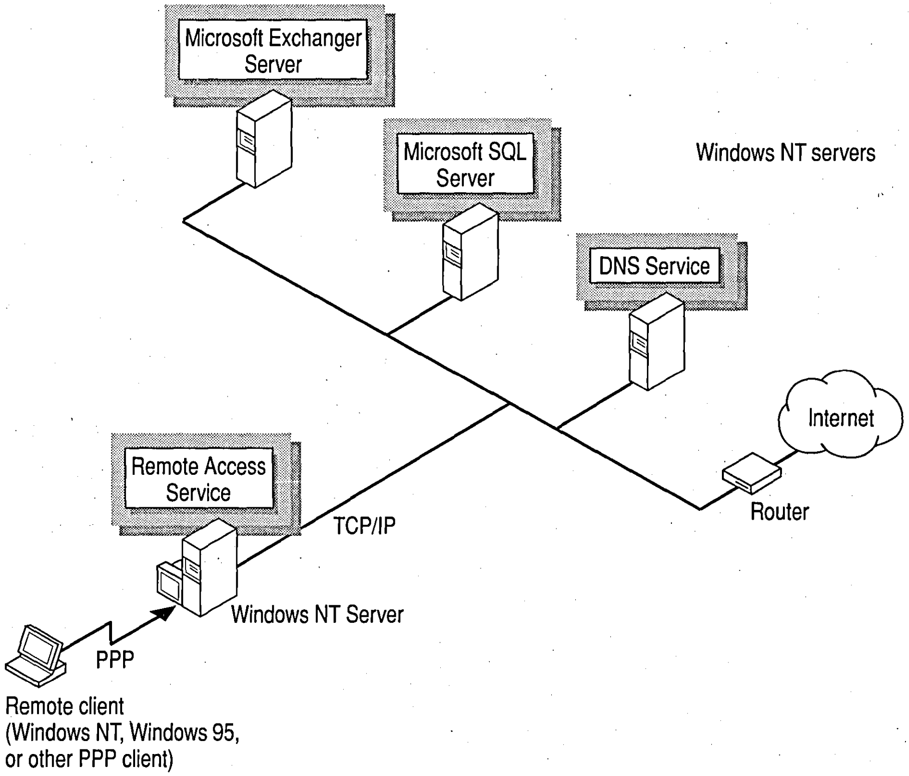


Figure 6.2 Internet service provider with Internet access and network services

The computer running Windows NT Server is on the Internet service provider's network, which also has a leased line to the Internet. The Remote Access Service accepts calls from customers who want Internet access or network services. RAS routes traffic to and from remote customers to servers on the private network and to and from the Internet.

For this scenario, you need to install and configure the following hardware or services:

- A computer running the Remote Access Service
- TCP/IP networking protocol on all computers that will use the Internet
- A multiport adapter, which allows multiple remote clients to dial in to the computer running RAS
- Network interface cards on all servers
- Internet browsers, such as Internet Explorer, on all remote clients that will access the Internet
- Dial-Up Networking on remote clients that will dial in to the RAS server
- Internetwide domain name resolution, as described in the section, "Establishing an Internet Connection," in Chapter 2, "Connecting Windows NT Server to the Internet."

For more information about multiprotocol routing and the Remote Access Service, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

Internet Gateway

An organization with a network can establish a RAS server with direct connections (through a router) to the Internet. To provide for security, the server can be isolated from the rest of the corporate network. (For more information about security, see Chapter 3, "Server Security on the Internet.")

Users can dial one number that gives them access to the Internet, and dial another number that gives them access to the corporate intranet. See the following section for more information about this scenario.

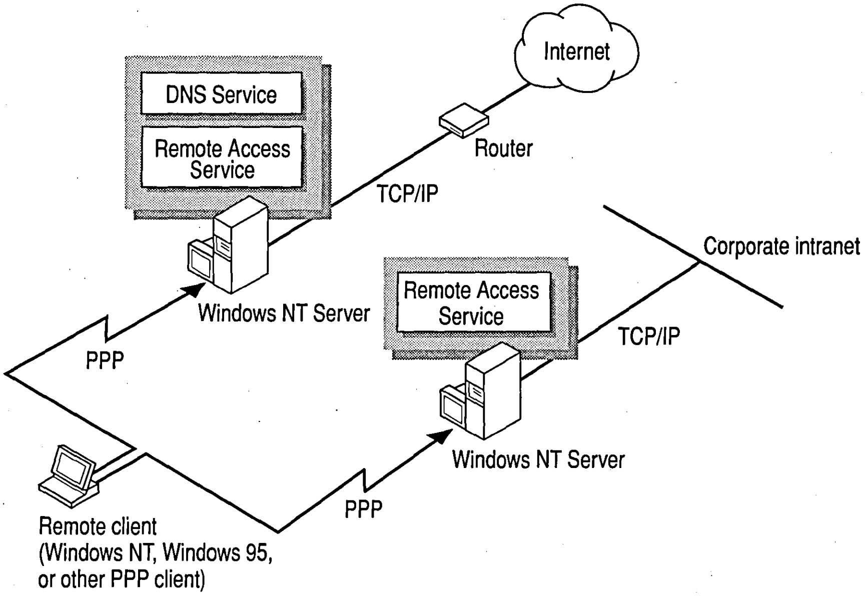


Figure 6.3 Microsoft RAS server as an Internet gateway server

Installing an Internet Gateway Server

Before you learn how to install Remote Access Service as an Internet gateway server, it is useful to understand a few TCP/IP networking terms, and how they relate to RAS. (For more information about TCP/IP and Remote Access Service, see the *Windows NT Server Networking Supplement*, the *Windows NT Server Resource Kit Networking Guide*, or online Help.)

IP Address

An IP address is used to identify a node (such as a workstation, a server, or a printer) on any network (such as your intranet or the Internet) and to specify routing information from one network or subnet to another network or subnet. Each node on a network or subnet must be assigned a unique IP address.

For Dial-Up Networking clients, the RAS server can automatically assign IP addresses to remote workstations when they connect. The IP address is obtained from a static pool that has been reserved for use by the RAS server, or through dynamic allocation from a Dynamic Host Configuration Protocol (DHCP) server. (For more information about DHCP, see the next section.)

Where needed, the RAS server can be configured to allow remote clients to specify their own IP addresses. This is useful for remote workstations that each need to be guaranteed a specific IP address when they are connected to the network.

Subnet masks are used in conjunction with the IP address to create subnets within an IP address space. Subnet masks are usually provided by the TCP/IP network administrator, such as an Internet service provider. If you need more information about subnet masks, see the *Windows NT Server Networking Supplement.*

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is an industry-standard protocol for automatic assignment of IP configuration to workstations. DHCP uses a client/server model for address allocation. The network administrator establishes one or more DHCP servers that maintain the network's TCP/IP configuration, including client configuration. Intranet workstations request leases on TCP/IP configuration from the DHCP server, thus eliminating the need for administrators to manually configure each workstation. For more information about configuring DHCP servers, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

A RAS server can act as a DHCP client, thereby obtaining TCP/IP configuration information on behalf of remote workstations. The RAS server leases a pool of IP configuration information from the DHCP server or servers. When remote workstations dial in to the network, the RAS server allocates IP configuration information to each workstation out of this pool.

Domain Name System

The Domain Name System (DNS) resolves friendly computer names to IP addresses. DNS is sometimes referred to as the BIND service in BSD UNIX.

To specify the DNS server that a workstation uses, you double-click **Network** in Control Panel to reach the configuration options for TCP/IP properties. A workstation's TCP/IP configuration typically includes one or two DNS servers that are on the local network. If a DNS server is unable to identify the IP address of a name requested by the workstation, it sends back information about other DNS servers that might be able to resolve the address. The workstation then queries the new set of DNS servers.

The Domain Name System makes it easy for users to access information from servers on the Internet. For example, it is easier to remember the name www.microsoft.com than to remember the IP address for that server.

To use the Domain Name System, workstations must be configured to recognize at least one DNS server's IP address. DNS server addresses can be assigned to a computer in one of two ways:

- Static TCP/IP configuration on the workstation
- Dynamic assignment by a DHCP server

In the Remote Access Service, DNS server addresses are assigned to remote workstations in one of three ways:

- Static assignment on the workstation
- Static assignment on the RAS server, which in turn assigns that address to remote workstations
- Dynamic assignment to the RAS server by using DHCP; the RAS server in turn assigns that DNS server's address to remote workstations

The RAS server always assigns the DNS address to workstations dialing in that run Windows NT Workstation or Windows 95. The address is either statically assigned by the RAS server or dynamically assigned for the RAS server by DHCP. For remote access solutions from vendors other than Microsoft, remote users might need to statically assign their DNS server.

For more information about setting up a RAS server to use DNS, see the *Windows NT Server Networking Supplement.*

Default Gateway

The *default gateway* is the intermediate network node on the network or subnet that has addresses for the network IDs of other subnets in the network. When a workstation sends data, the default gateway can forward the packets to other gateways until the data is eventually delivered to its final destination. Gateways are usually computers that are called *routers* because they are dedicated to directing network traffic.

TCP/IP workstations can each be configured for one default gateway only. This poses an interesting situation for remote workstations that are also connected to an intranet. For example, a computer at a branch office dials in to the corporate network while it is still connected to the branch office network. This type of a workstation is referred to as a *multihomed* workstation.

When a multihomed computer running Windows NT Workstation or Windows NT Server attempts to access a particular IP address, the destination server is located by using the following process:

- If the destination IP address indicates that it is on the same IP subnet as the workstation's network interface card, then data is sent through the network interface card.
- If the destination IP address indicates that it is not on the same subnet as the workstation's network interface card, then data is sent to the default gateway assigned by the RAS server. The default gateway then locates the destination route on behalf of the remote workstation.

  If a default gateway IP address was previously configured for the network interface card, it is ignored by default. If required, the remote workstation can be configured so that the default gateway on the network interface card is used instead of the default gateway on the remote link.

Configuration Overview

Complete the following tasks to make a computer running Windows NT Server an Internet gateway.

▷ **To configure an Internet gateway**

1. Select an Internet service provider.

   For a complete list of Internet service providers, refer to the book, *Connecting to the Internet* by Susan Estrada (published by O'Reilly and Associates). Or refer to your phone book or, if possible, the Internet.

2. Assign a dedicated pool of IP addresses for remote clients.

   –or–

   Use DHCP servers on your network.

   For details, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

3. Configure a DNS server locally on your intranet.

   –or–

   Contact your Internet service provider for the IP address of a DNS computer on the ISP's network.

4. Install any optional communication hardware you will need to provide Internet service.

   For example, your server can be configured with a multiport adapter, Integrated Services Digital Network (ISDN) interface cards, and X.25 interface cards.

5. Install Windows NT Server 4.0 on your computer.

   For details, see the *Windows NT Server Start Here* manual.

Internet Gateway Configuration

The scenario described in this section was an actual pilot test of Windows NT as an Internet gateway server at Microsoft Corporation. For security reasons, the Internet gateway server was installed on an isolated network, which was in turn connected to the Internet by third-party routers. The RAS server and the third-party routers were not connected to the corporate network.

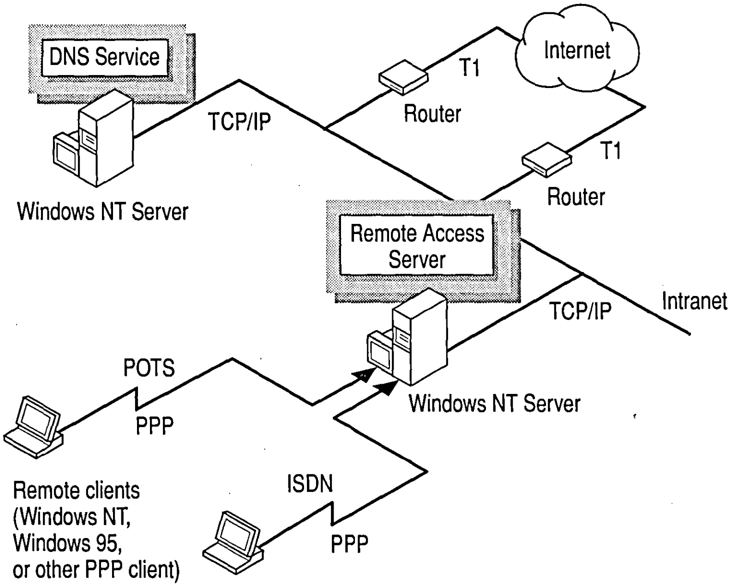


Figure 6.4 Windows NT as an Internet gateway server

In this scenario, the computer running Windows NT Server has a leased line to an Internet service provider through third-party routers. The Remote Access Service is installed. This enables traffic from the Internet to be routed to and from computers on the private network. The Remote Access Service enables Windows Dial-Up Networking clients or other dial-up clients to connect to the RAS server by using ISDN or a POTS line (plain old telephone service, also known as PSTN or public switched telephone network), giving them Internet access.

The Internet gateway server for the pilot test had the following configuration:

- A MIPS Rx4000 RISC-based computer (with 32 MB of RAM) running the Remote Access Service
- TCP/IP networking protocol on all computers that will use the Internet
- Network interface cards on all computers
- Third-party (Cisco) routers
- A Digi International PC/2e serial adapter, which enables multiple remote clients to dial in on telephone lines to the computer running the Remote Access Service
- A Digi International PCIMAC4 ISDN adapter, which enables multiple remote clients to dial in on ISDN lines to the computer running the Remote Access Service
- Dial-Up Networking on remote clients that will dial in to the RAS server
- Modems or ISDN cards on remote clients that will dial in to the RAS server
- ISDN lines and standard analog telephone lines
- A DNS server
- Internet browsers, such as Internet Explorer, on all computers that will access the Internet

For more information about the Remote Access Service, see the *Windows NT Server Networking Supplement* and *Windows NT Server Resource Kit Networking Guide.*

CHAPTER 7

Internet Tools

The Microsoft Windows NT Server Resource Kit version 4.0 compact disc includes several tools for Internet users, including the following:

- Mail Server, a mail server for Windows NT Server that uses Simple Mail Transfer Protocol (SMTP) and Post Office Protocol version 3 (POP3).
- Telnet Server, a tool that enables remote clients to use Telnet to log on to the Windows NT Server as if the remote client is using a local terminal.
- Microsoft dbWeb, a gateway between Microsoft Open Database Connectivity (ODBC) data sources and the Microsoft Internet Information Server (IIS).

This chapter provides information about these tools and how to use them. For specific information about installation or command syntax, see Resource Kit Tools Help. At the end of this chapter is a list of other Microsoft products and development tools for Internet users.

Mail Server (MailSrv)

Mail Server (**MailSrv**) is a tool you use to configure a computer running Windows NT Server to provide electronic mail service for intranet or Internet users. With **MailSrv** installed, you can send and receive mail by using a TCP/IP-based intranet or the Internet. TCP/IP (Transmission Control Protocol/Internet Protocol is the networking protocol supported by most computers on the Internet.)

MailSrv is based on the TCP/IP protocols described in Table 7.1.

Table 7.1 TCP/IP Mail Protocols in MailSrv

Protocol	RFC	Description
Simple Mail Transfer Protocol (SMTP)	RFC 821 and RFC 822	TCP/IP-based networks use SMTP to transfer mail reliably and efficiently. SMTP transports a mail message across TCP/IP-based networks to a destination SMTP server.
Post Office Protocol version 2 and version 3 (POP2, POP3)	RFC 1460	POP defines the standard for user mailboxes and the protocol for downloading mail messages to a user's local computer. This protocol is generally referred to with its version number (POP3, POP2) to avoid confusion with the telephony POP (Point of Presence) terminology.
MIME and UUENCODE	RFC 1521 and RFC 1154	**MailSrv** does not contain support for Multipurpose Internet Mail Extension (MIME) and UNIX-to-UNIX Encode (UUENCODE). However, **MailSrv** can send and receive messages containing MIME and UUENCODE attachments.

MailSrv is based on a combination of the SMTP and POP3 protocols. It provides only the SMTP send-and-receive services and the POP3 user post office services that are required by the RFC specifications.

MailSrv is completely separate from the electronic messaging and groupware services of Microsoft Exchange and Microsoft Mail. Because **MailSrv** provides only the basic required SMTP and POP3 services, it can be used in small TCP/IP-based networks that cannot provide the resources required for advanced messaging and groupware services. A computer that runs the **MailSrv** tool under Windows NT Server can also be used with Microsoft Exchange and Microsoft Mail systems as a dedicated SMTP/POP3 server.

Using MailSrv with the Windows NT Inbox

New to Windows NT Server version 4.0 and Windows NT Workstation version 4.0 is a universal inbox client (also referred to as Windows Messaging client) that can send and receive electronic mail. The inbox client organizes, accesses, and stores all types of information. For example, you can open the Inbox on the Windows NT desktop to read, compose, forward, and delete messages, or to create automatic replies and other notification policies based on individual preferences.

The Windows NT Inbox is optimized for use with Microsoft Exchange Server and Microsoft Exchange clients. However, because it is a universal inbox client, you can use it with different mail systems and mail client software, including **MailSrv**.

Mail client software—for example, the Windows Messaging client—must be installed on each computer supported by the computer running the **MailSrv** tool under Windows NT Server. After the mail client software is installed, you must enable Internet mail service. For example, to enable Internet mail service by using the Windows Messaging client, follow the procedure in the Help topic "Installing an Information Service."

Using MailSrv with Microsoft Exchange

Microsoft Exchange Server integrates mail, group scheduling, electronic forms, and groupware applications on a single platform. It can also extend those capabilities to encompass Internet and X.400 systems, to provide access to the most widely used messaging standards.

Microsoft Exchange Server version 4.0 supports messaging between intranet and Internet locations and between different electronic mail systems, including SMTP/POP3 services such as **MailSrv**. **MailSrv** running with Windows NT Server can function as a dedicated SMTP host for Microsoft Exchange Server by using the Microsoft Exchange-based Internet Mail Connector (IMC). The IMC service converts messages from Microsoft Exchange format to the format required by the SMTP messaging system and vice versa.

Microsoft Exchange Server is not included with the Windows NT product. For information about installing and configuring Microsoft Exchange Server and client software with the Internet Mail Connector option, see the Microsoft Exchange Server product documentation.

Using MailSrv with Microsoft Mail

Microsoft Mail for PC Networks, version 3.5 or later, is an electronic messaging system for large and small organizations. Microsoft Mail supports networks that include computers using Windows NT Server, Windows NT Workstation, Windows for Workgroups, Windows 95, 16-bit Windows, MS-DOS, Macintosh, and OS/2® operating systems.

Microsoft Mail for PC Networks, version 3.5, provides an SMTP gateway that enables Microsoft Mail users to exchange Internet mail with SMTP host computers—for example, **MailSrv** running with Windows NT Server. The Microsoft Mail Gateway to SMTP can also be used to transparently link multiple Microsoft Mail networks by using **MailSrv** running with Windows NT Server as an SMTP backbone.

For information about installing and configuring Microsoft Mail for PC Networks, see the Microsoft Mail for PC Networks product documentation.

Security Considerations When Using SMTP/POP3

Windows NT provides built-in security that controls:

- User account access based on user names and passwords.
- File and directory access, permissions, and operations.
- User operations based on user and group policies.

Windows NT security provides a high level of security both for stand-alone computers and for Windows NT–based networks. However, the **MailSrv** tool uses only the clear-text password authentication of POP3. Passwords are sent over the network in readable (clear) format and are not encrypted. Administrators must plan for security on networks that use the **MailSrv** tool. They must consider the potential for unauthorized users acquiring passwords and subsequent malicious tampering with Internet communications.

You can use the classification of Internet communications in Table 7.2 to identify your enterprise security requirements when using SMTP/POP3. For additional information on security, see Chapter 3, "Server Security on the Internet."

Table 7.2 Enterprise Security Guidelines

Type of communication	Description
General communications	Include private mail or limited access to public-domain data published on a Web server. Communication authentication and integrity are based on password systems.
Business communications	Include intra-organization business mail, correspondence, data, and public correspondence (such as product advertising) and information (such as customer support service). Authentication and message integrity, as well as privacy, can be critically important and require more sophisticated control than for general communications.
Financial transactions	Are not suitable for mail communication because of the need for high security control. Additionally, financial data is often partitioned. Each party to the communication needs some of the data, but not all of the parties need (or should have) all the data.

Installing and Running MailSrv

To install **MailSrv,** you need the following components installed on your computer:

- Windows NT Server version 4.0
- TCP/IP

Before you install **MailSrv** ,configure TCP/IP to use the Domain Name System (DNS). To do this, on the **WINS Address** tab of the **Microsoft TCP/IP Properties** dialog box, select the **Enable DNS for Windows Resolution** check box. You must do this on the computer running **MailSrv** under Windows NT Server and on any other Windows NT–based computer in the network that uses **MailSrv** services. SMTP uses DNS for name–to–IP address mapping.

Note The **MailSrv** server must be added to the DNS name server for the domain. If the DNS name server is a computer running DNS Server under Windows NT Server, you can do this by using DNS Manager to create the following DNS resource records:

- *A record.* The A (address) resource record maps a host (computer or other network device) name to an IP address in a DNS zone.
- *MX record.* The MX (mail exchanger) resource record specifies a mail exchange server for the specified DNS domain name.

MailSrv can be installed only on a drive formatted by using the Windows NT File System (NTFS) because **MailSrv** checks the local user account database when storing messages in a local user mail spool directory. Installation fails if you attempt to use a network or non-NTFS drive for the mail spool directories.

The installation program installs and automatically starts the services described in Table 7.3.

Table 7.3 Services Installed with MailSrv

Service	Description
SMTP Server	Receives and sends SMTP mail.
POP3 Server	Provides the POP3/POP2 mailboxes and processes user requests to retrieve mail from their mailboxes.
Local Mail Delivery Agent	Delivers (downloads) mail to the user's local computer.
Eudora Password Change Server	Processes Eudora user requests to change their Eudora passwords. (Eudora is a popular mailbox client program.) The Eudora Password Change Server does not start automatically. To manually start the service, click **Start**, point to **Settings**, and click **Control Panel.** In Control Panel, double-click the **Services** icon. You can also configure this service to start automatically by using the **Services** icon.
Mail Server Admin	Will be a graphical manager tool. The tool is installed but is not implemented as of this writing. For now, you must manually configure **MailSrv** by using the Registry.

See Resource Kit Tools Help for detailed information about installing and configuring **MailSrv**.

Administering Microsoft MailSrv

The administrative tasks of running **MailSrv** on Windows NT Server include:

- Creating user mail accounts.
- Deleting user mail accounts.
- Deleting user spool directories.
- Adding address rules (transforms).
- Using the Event Viewer to monitor **MailSrv**.

The following sections discuss each of these tasks.

Creating User Mail Accounts

MailSrv creates a mail account for each user account on the computer. You do not need to create separate mail accounts for users. The mail accounts are created by using the Windows NT Server local user account database on the computer running **MailSrv**. Because the local user account database is used, domain (or alias) mail accounts are not supported by **MailSrv**.

For information about creating local user accounts, see the Windows NT Server product documentation and the *Windows NT Server Resource Guide.*

No additional administrator action is required to create a user mailbox. The user mailbox is established the first time a user opens the Inbox on the desktop and then opens **Mailbox** - *user name.*

Important The local computer name must be the same as the DNS host name, which is the default configuration of TCP/IP. If you need to return to the default configuration, display the DNS host name and change it by using the options on the **DNS** tab in the **Microsoft TCP/IP Properties** dialog box. For more information, see Help.

Deleting User Mail Accounts

A user's mail account is deleted when you delete the local user account by using either **User Manager** from Windows NT Workstation or **Server User Manager** from Windows NT Server. You do not need to perform any additional operation. Note that you must have administrator permissions to delete a local user account.

Deleting User Spool Directories

When a user's local account (and concurrently the user's mail account) is deleted, the user's mail directory remains. You can delete the spooled user directory on the local computer if you have administrator permissions on that computer.

Adding Address Rules (Transforms)

Transforms are rules that the administrator creates to add, remove, and modify domain names appended to inbound and outbound messages. Transforms also enable the administrator to mask host names and domain names.

When an administrator modifies the names and addresses that are attached to inbound and outbound mail messages, mail addressing becomes easier for users and secures the use of domain names. The transform is transparent to the user, who does not need to worry about the information that is appended to, or deleted from, the mail address.

For example, if **MailSrv** is used for a small intranet, the administrator can create a transform to automatically add the domain name to the address. Using this transform, a message addressed only as "Lydia" in the terraflora.com domain is actually transmitted with the address of Lydia@terraflora.com.

For detailed information about creating transforms, see Resource Kit Tools Help.

Using Event Viewer to Monitor MailSrv

MailSrv is designed to post any **MailSrv** event messages to the Windows NT Server Event Viewer. Service stops, starts, and other events are written to the system and application logs. To manually start and stop **MailSrv** services, double-click **Services** in Control Panel.

Note To ask questions about the **MailSrv** tool, contact rkinput@microsoft.com.

Microsoft Telnet Server (Beta)

The Telnet Server tool in the Microsoft Windows NT Server Resource Kit version 4.0 provides basic TCP/IP Telnet Server functionality. A computer running the Telnet Server tool under Windows NT Server can support connections from various TCP/IP Telnet clients, including UNIX-based and Windows NT–based computers.

The Telnet Server tool supports command-line execution of commands that normally can be run in the command window—for example, TCP/IP tool or MS-DOS commands. A command you enter at the remote Telnet client console (computer) runs on the Windows NT–based Telnet Server computer. The Telnet Server then sends the results of the command back to the remote Telnet client computer.

When you install Windows NT Server or Windows NT Workstation, a Telnet client is automatically installed in the **Accessories** folder. You use the Telnet client to connect to another computer running a TCP/IP–based Telnet server—for example, the Windows NT–based Telnet server, or a UNIX-based Telnet server.

Each Telnet client session started on the Windows NT–based Telnet server is allocated a console session that runs in the remote user's desktop context and that does not interfere with any local user sessions on the computer running Telnet Server under Windows NT. At the start of a Telnet session, the remote Telnet client must provide a user name and password to log on to the Windows NT–based Telnet Server. This information is used to create a console session with the security attributes of the user. For example, an administrator can log on to a computer running Windows NT Workstation, start the Windows NT–based Telnet client, connect to the computer running Windows NT Server with the Telnet Server tool, and run command-line scripts to add users, services, and so on.

Note The Telnet Server tool provided with the Microsoft Windows NT Server Resource Kit version 4.0 is beta software. It does not support terminal types and provides only basic TTY functionality. To ask questions about the Telnet Server tool, contact rkinput@microsoft.com.

Microsoft dbWeb

Microsoft dbWeb is a gateway between Microsoft Open Database Connectivity (ODBC) data sources and the Internet Information Server. You can use Microsoft dbWeb to selectively publish data from an ODBC data source by using Hypertext Markup Language (HTML) pages. A user of a Web browser can easily create data queries and navigate by using hyperlinks through the data. But you control which data is accessible to users by creating parameters under Microsoft dbWeb that limit the data that can be retrieved by the user data queries. In other words, you can use Microsoft dbWeb to control access to the data you publish on the Internet and to provide easy-to-use tools such as query-by-example (QBE) and HTML.

Microsoft dbWeb supports 32-bit ODBC databases including:

- Microsoft SQL Server
- Microsoft Access
- Microsoft Visual FoxPro™

The architecture of Microsoft dbWeb includes these services, which are discussed in the sections that follow:

- The dbWeb Administrator, a graphical user interface
- The dbWeb Internet Server Application Program Interface (ISAPI) client (dbWebc.dll)
- The schema repository, a Microsoft Access database (dbWeb.mdb)

The dbWeb Service, a Windows NT Server service

dbWeb Administrator

The dbWeb Administrator is the component that an administrator uses to create *schemas*. Schemas control how the information in a database is published on the Internet and define the query and the resulting HTML pages that display to Internet clients.

The dbWeb Administrator provides an interactive Schema Wizard that leads you through the schema creation process by asking a series of questions. You can use the wizard to:

- Specify search fields for a query-by-example (QBE) HTML page.
- Choose the data fields that will appear on a displayed HTML page.
- Specify the links within a displayed HTML page for interactive data navigation.

For information about using the dbWeb Wizard, see Resource Kit Tools Help.

dbWeb ISAPI Client

The dbWeb ISAPI client (dbWebc.dll) is the component that acts as the interface between the Internet client and the dbWeb service.

dbWeb Schema Repository

The dbWeb schema repository is a Microsoft Access database that stores query and formatting information. This information is entered by a site administrator by using the dbWeb Administrator service. After the query and formatting information is entered in the dbWeb schema, it is used by the dbWeb service, in turn, to retrieve user data selections or queries from the Microsoft SQL Server, Microsoft Access, or other 32-bit ODBC data source.

dbWeb Service

The dbWeb service component communicates with a user of Internet Explorer or another Web browser. The dbWeb service is a gateway that sends the user data queries to the ODBC data source.

When a user selects a schema, the dbWeb service retrieves the schema from the schema repository and uses it to dynamically build HTML pages in the form of query-by-example (QBE) forms, query results, or other method requests.

For instructions on how to configure and start the dbWeb service, see Resource Kit Tools Help.

The interaction between the dbWeb service and Internet clients is illustrated in Figure 7.1.

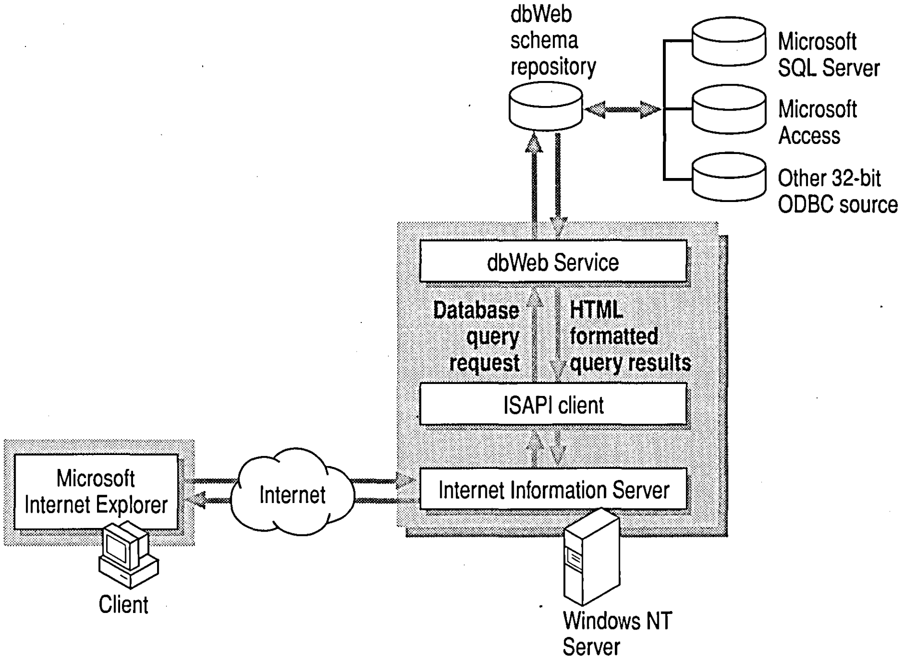


Figure 7.1 Microsoft dbWeb architecture

Installing and Running Microsoft dbWeb

To start Microsoft dbWeb, you need the following components installed on your computer:

- Windows NT Server version 4.0, or version 3.51 with Service Pack 4
- Internet Information Server
- Microsoft Open Database Connectivity (ODBC) driver
- Microsoft dbWeb
- Internet Explorer or another Web browser

Before installing Microsoft dbWeb, you must install Microsoft Internet Information Server and the ODBC driver. For detailed information about installing Microsoft dbWeb and about using the dbWeb Administrator and the dbWeb service, see Resource Kit Tools Help.

Note To ask questions about Microsoft dbWeb, contact rkinput@microsoft.com.

Additional Internet Products from Microsoft

Microsoft has developed browser, server, viewer, authoring, and development products specifically for the Internet. These products help you publish and view information on the Internet, and can be used to develop new Internet-based applications. You can get information about Microsoft products for the Internet at the Microsoft Internet Resource Center at **http://www.microsoft.com/internet**.

CHAPTER 8

Troubleshooting an Internet Information Server Installation

This chapter presents approaches to solving common problems encountered when installing or configuring a computer running Internet Information Server (IIS) or Peer Web Services. This chapter provides information about:

- Troubleshooting Internet Information Server—specific troubleshooting techniques or problems.
- Sources of troubleshooting information—places to go for more troubleshooting information or general information about Windows NT.
- Using troubleshooting tools—Windows NT Server tools that can be useful when determining a problem with Internet Information Server.

Troubleshooting Internet Information Server

This section provides four types of troubleshooting information:

- A procedure to test Internet Information Server operation.
- Where to go for more information when you receive Windows NT error messages.
- The meaning of Hypertext Markup Language (HTML) 1.0 status codes and messages presented to users.
- Tips for troubleshooting specific problems, listed by category of problem.

Testing an Installation

The default installation of Internet Information Server contains sample files that you can use to test the functionality of your Internet Information Server World Wide Web (WWW) service.

▷ **To test the WWW service on your server**

1. Ensure your computer has an active connection to your intranet and that name resolution is working properly.
2. Start Microsoft Internet Service Manager and use it to verify that the WWW service is running.
3. In Internet Explorer, click **Open** on the **File** menu and type the Uniform Resource Locator (URL) for the home directory of your new server.

   The URL is **http://** followed by the NetBIOS name of your server. For example, if your server is called Myserver you type

   http://myserver

   A sample HTML page appears. If it does not, try the full path to access the samples page, for example

   http://myserver/samples

Windows NT Messages

The Messages database, included in this Resource Kit, is another source of general troubleshooting information. Thousands of Windows NT messages are documented, along with the probable cause of errors that generate them and recommended solution to each. This database includes documentation of the STOP messages that appear with a blue screen when the system fails. For more general information on blue-screen messages, see Chapter 38, "Windows NT Executive STOP Messages," in the *Windows NT Workstation Resource Guide.*

HTTP 1.0 Status Codes and Reason Phrases

Clients can receive an HTTP status code and matching reason phrase after making a request to the IIS server.

The Hypertext Transport Protocol (HTTP) defines status codes and reason phrases that HTTP servers such as Internet Information Server can return to clients.

Status codes are returned by the server in response to a request. The three-digit code acknowledges an attempt to understand and satisfy the request. The reason phrase gives a short description of the status code.

Note This section describes the status codes and reason phrases from the HTTP 1.0 Internet-draft. Note that Internet-drafts are valid for a maximum of six months. You should check the full text of the latest draft for the most current information. To learn the current status of any Internet draft, use FTP to check the 1id-abstracts.txt file in the Internet-Drafts directory on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

The first digit of the status code defines the class of response. There are five possible values for the first digit of the status code. Table 8.1 lists the five classes of codes and the reasons they are returned by the server.

Table 8.1 HTTP 1.0 Status Code Classification

Code	Class	Use
1*xx*	Informational	Not used, but reserved for future use.
2*xx*	Success	The action was successfully received, understood, and accepted.
3*xx*	Redirection	Further action must be taken in order to complete the request.
4*xx*	Client Error	The request contains incorrect syntax or cannot be fulfilled.
5*xx*	Server Error	The server failed to fulfill an apparently valid request.

Table 8.2 presents the individual values of the numeric status codes defined for HTTP 1.0. The reason phrases listed here are those that are recommended by the HTTP 1.0 protocol and are used by Internet Information Server.

Table 8.2 HTTP 1.0 Status Codes, Reason Phrases, and Meanings

Status code	Reason phrase	Meaning
200	OK	The request has succeeded. The information returned with the response is dependent on the method used in the request, as follows: GET An entity[1] corresponding to the requested resource is being sent in the response. HEAD The response must contain only the header information and no Entity-Body. POST An entity describing or containing the result of the action is being sent in the response.
301	Moved permanently	The requested resource has been assigned a new permanent URL and any future references to this resource should use that URL.

Table 8.2 HTTP 1.0 Status Codes, Reason Phrases, and Meanings *(Continued)*

Status code	Reason phrase	Meaning
302	Moved temporarily	The requested resource resides temporarily under a different URL. Because the redirection is sometimes altered, the client should continue to use the Request-URI[2] for future requests.
304	Not modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified since the date and time specified in the If-Modified-Since field, the server responds with this status code and does not send an Entity-Body to the client. Header fields contained in the response should include only information that is relevant to cache managers and that may have changed independently of the date specified in the entity's Last-Modified field. Examples of relevant header fields include Date, Server, and Expires.
400	Bad request	The request could not be understood by the server because of incorrect syntax.
401	Unauthorized	The request requires user authentication.
403	Forbidden	The server understood the request, but refuses to perform the request for an unspecified reason. Authentication will not help and the request should not be repeated.
404	Not found	The server has not found anything matching the Request-URI. The server does not indicate whether the condition is temporary or permanent.
500	Internal server error	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	Not implemented	The server does not support the functionality required to fulfill the request.
502	Bad gateway	The server received an invalid response from the gateway or upstream server it accessed in attempting to fulfill the request.

[1] An entity is a particular representation or rendition of a resource that may be enclosed within a request or response message. An entity consists of metainformation in the form of entity headers, and content in the form of an entity body.

[2] Uniform Resource Identifier; see the HTTP 1.0 specification for an explanation of URI.

HTTP status codes are extensible, but the codes in Table 8.2 are the only codes that are recognized in current practice and are used by Internet Information Server.

Installation Problems

Cannot Install File During Setup

During Internet Information Server Setup, you can install Open Database Connectivity (ODBC) drivers. If you select ODBC drivers to be installed, the following message can appear when Setup tries to copy ODBC files:

```
Cannot install file c:\winnt\system32\odbc32.dll. It might be in use.
Close all applications and click Retry.

Click Ignore if you want to skip this file.
```

This problem occurs when applications that use ODBC drivers are running. However, it also happens when services, such as SQL Executive, are running.

▷ **To correct this problem**

1. Close all open applications except the Internet Information Server Setup program. (The **Error** dialog box is displayed.)
2. In Control Panel, double-click **Services**.
3. Click **SQL Executive** and then click **Stop**.
4. Switch back to Internet Information Server Setup (**Error** dialog box) and click **Retry**.

Server Configuration Problems

Access Is Denied for Virtual Directories

The **Directories** property sheet for an Internet Information Server service displays the message "Access is Denied" in the Error column of a virtual directory listing. This message appears after you create a virtual directory in Internet Service Manager by specifying a network share in universal naming convention (UNC) format.

This problem occurs if the user account information is missing or incorrect when the virtual directory is created.

To correct this problem, you must enter the correct user account information by using Internet Service Manager.

▷ **To specify a user name for a virtual directory on a network drive**

1. In Internet Service Manager, double-click the computer name of the service that uses the virtual directory.
2. Click the **Directories** property sheet and then select the virtual directory reporting the error.
3. Click **Edit Properties**. Enter the account information in the following format and then click **OK**:

   User name: domainname\username
   Password: password

FTP Server Users Experience Delayed Responses

Microsoft Internet Information Server File Transfer Protocol (FTP) clients experience delayed responses to commands when a large number of users are logged on through FTP. This problem occurs sporadically. File transfer speeds are not affected.

The default number of threads per processor (**MaxPoolThreads** value in Registry) installed on your system is 10. This might be insufficient for a heavily used FTP server because some of the FTP commands use synchronous I/O, causing threads to block while they complete.

▷ **To correct this problem**

1. Click the **Start** button, then point to **Run**. In the **Open** box, type **regedt32.exe** and then click **OK**.
2. Click the HKEY_LOCAL_MACHINE window and locate the following key:

```
\System
  \CurrentControlSet
    \Services
      \InetInfo
        \Parameters.
```

3. From the **Edit** menu, click **Add Value**.
4. In the **Add Value** dialog box, enter the value **MaxPoolThreads** with the data type **REG_DWORD**.

5. In the **DWORD Editor** dialog box, enter a value in the range 0 to 0xFFFFFFFF.

   For example, a twin processor with 500 to 1,000 concurrent users might require 50 or more threads per processor to provide quick response for all FTP client users.
6. Click **OK** and quit the Registry Editor.
7. Shut down and restart Windows NT.

Warning If you use Registry Editor incorrectly it can cause serious, system-wide problems that may require you to reinstall Windows NT to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk.

Anonymous Users Have Same Access as Domain Users

You allow anonymous users access to specific public Web pages and allow domain users access to additional Web pages. Your server is a primary domain controller that uses the Windows NT File System (NTFS) security permissions. However, after configuration, anonymous users have the same access as domain users.

The problem is that any user account that you create on a primary domain controller automatically becomes a member of the Domain Users group.

In Internet Information Server, you can allow both anonymous and domain users access to the selected Web pages. To do this, select **Allow Anonymous** and **Windows NT Challenge/Response** boxes on the **WWW** property sheet, then use NTFS security permissions to specify access. However, the Internet Information Server anonymous access account, IUSR_*computername*, becomes a member of Domain Users when Internet Information Server is installed on a primary domain controller. As a result, anonymous users have the same access as the domain users.

To correct this problem, remove IUSR_*computername* from the global group Domain Users. You must then add the Log On Locally user right to the IUSR_*computername* account. As an alternative, you can replace the IUSR_*computername* account on the domain controller with an account that has appropriate permissions.

Cannot Start Internet Information Server Services

When the WWW service cannot automatically start during Windows NT startup, the Event Viewer records the message, "HTTP could not initialize socket library." The options to change properties of Internet Information Server services are unavailable in Internet Service Manager. When you attempt to start the WWW service and FTP service manually, a message states "Data area passed to system call is too small."

To solve this problem, you change the order of protocols listed in the Registry key and move **Tcpip** to the first entry in the list of values.

```
HKEY_LOCAL_MACHINE\System
  \CurrentControlSet
    \Services
      \Winsock
        \Parameters
          \Transports
```

Clients Cannot See Virtual Directories in Directory Listings

FTP, Gopher, and WWW directory browsing clients (such as Internet Explorer) are not able to see virtual directories.

Internet Information Server does not display virtual directories in directory listings returned to clients.

If you know the name (alias) of the virtual directory, you can work around this limitation by explicitly specifying the name of the virtual directory in the client. In a WWW browser, you include the virtual directory name in the URL, for example:

ftp://myftpserver/*virtual_directory***/**

In a dedicated FTP client, you explicitly change directories by using the virtual directory name, for example:

cd /*virtual_directory*

You must type the forward slash (/). Otherwise, **cd** tries to change the directory from within the client's current directory.

HTTP/1.0 Error 500

The following HTTP server message can be returned for an anonymous user logon request:

```
HTTP/1.0 500 Server Error (Logon failure: the user has not been granted
the requested logon type at this computer.)
```

Frequently, this message means that your anonymous user does not have local logon rights.

▷ **To make sure an anonymous user can log on locally**

1. In the Microsoft Internet Service Manager, open the **WWW Service** properties sheet. Verify that the anonymous logon user name and password specified here are identical to the user name and password in User Manager.
2. Run User Manager to verify that the Log On Locally user right includes your designated anonymous user name.

   –or–

   Change the anonymous user account to an account that has the Log On Locally user right specified in User Manager.

Client Problems

Netscape Navigator 2.0 Does Not Support Authentication

If you use Netscape Navigator 2.0 to access an IIS server that uses Windows NT challenge/response password authentication, a dialog box appears that requests your user name and password. After you enter the correct user name and password, you see the message "Error: Access is Denied."

Even though Netscape Navigator 2.0 prompts you for a user name and password, it does not support Windows NT challenge/response password authentication.

To correct this problem, use Anonymous access or Basic user authentication in Internet Information Server, or upgrade clients to Internet Explorer version 2.0 or later.

Internet Explorer 2.0 Ignores Size Attribute

Internet Explorer 2.0 does not use the Size attribute of the Select tag on HTML pages properly.

RFC 1866 specifies that the Size attribute indicates the number of selections that are displayed when a user clicks a list box. A user should be able to see the selections by scrolling through the selection list box.

Internet Explorer 2.0 displays more than one list item even when Size is set to 1. If you increase the value of the Size attribute, the list box size grows. However, the size of the list box might not correspond to the setting. For example, with Size set to 1, the list box shows three selections, but with Size set to 5, the selection list box shows only four selections.

To overcome this problem, upgrade to Internet Explorer version 3.0.

Internet Explorer 1.5 Does Not Use Default Selection

Internet Explorer version 1.5 for Windows NT does not automatically select (highlight) the preselected item of an option list in an HTML form. The user must click the **Reset** button or manually select the item.

Internet Explorer 1.5 Is Unable to Save Files

If you run Internet Explorer version 1.5, you might see the message:

```
Unable to save C:\Temp\filename. Disk may be full.
The attempt to load ftp:filename failed.
```

This might be caused by a full disk, as stated in the message. The problem can also be caused by a client browser that does not have a \Temp directory.

To solve this problem, create a directory named "Temp" off the root of the boot drive, for example, C:\Temp.

Browsers Fail to Connect When Using SSL

Netscape Atlas and other browsers that support version 3 of the Secure Sockets Layer (SSL) might fail to connect to Microsoft Internet Information Server when the IIS server is using SSL.

Internet Information Server version 2.0 supports SSL version 2. Newer Web browsers, such as Netscape Atlas, support SSL version 3. When the Web browser connects to Internet Information Server, the browser tries to connect by using SSL version 3. Internet Information Server does not recognize SSL version 3 clients, so the connection is immediately dropped. Clients do not attempt to use version 2 after version 3 is rejected by the server.

To solve this problem, use a browser that supports SSL version 2.

Internet Explorer 2.0 Fails to Connect to SSL-Enabled Internet Information Server

When connecting to SSL-enabled IIS servers, you might get one or more of the following messages:

```
HTTP/1.0 403 Access Forbidden (Secure Channel Required - This Virtual
Directory requires a browser that supports the configured encryption
options.)
```

–or–

```
Unable to connect to servername
```

To fix this problem, upgrade to Internet Explorer version 2.01 or later.

Logging Problems

Logging to SQL Server on the Network Fails

Although a valid SQL Server user name and password are entered on the **Logging** property sheet in Internet Service Manager, they might seem to disappear when you start Internet Service Manager.

This is a problem with SQL Server Login Security Mode set to Integrated. In Integrated mode, the user name and password specified in Internet Service Manager are ignored because SQL Server attempts to use the logon account specified when the computer running the IIS server was started. Because this account probably does not have permission to use SQL Server, Internet Information Server logging to SQL Server fails and the SQL Server log records this message:

```
failure condition - logon failed because there is no valid user account.
```

And the IIS server reports the following:

```
Error: odbc reported an error. The Datasource name "DSN_name" may be
incorrect. Check the server's event log for details.
```

To resolve this issue, set the SQL Server Login Security Mode to Mixed. This setting enables the IIS server to access SQL Server for logging. Access to SQL Server by using other access methods is unaffected.

For more information about SQL Server Login Security Mode, see Part 4, "Security," of the *Administrator's Companion* in the *Microsoft SQL Server Books Online*.

Time Field Appears Wrong in Log

The Microsoft Internet Information Server log file contains a Time field. This field displays the elapsed time from the start of a request (connect) until the request is finished and the item is about to be logged. The value represents only a checkpoint in terms of millisecond difference.

Application and Script Problems

Testing CGI Scripts

You can use a Perl script to test for the proper installation and execution of Common Gateway Interface (CGI) scripts with Internet Information Server.

Use a text editor to create a file with the following lines of code. Save the file in the /Scripts directory as Hello.pl.

```
print "Content-Type: text/html\n\n";
print "<HTML>\n";
print "<HEAD>\n";
print "<TITLE>Hello World</TITLE>\n";
print "</HEAD>\n";
print "<BODY>\n";
print "<H4>Hello World</H4>\n";
print "<P>\n";
print "Your IP Address is $ENV{REMOTE_ADDR}.\n";
print "<P>";
print "<H5>Have a nice day</H5>\n";
print "</BODY>\n";
print "</HTML>\n";
```

After you create the file, configure Perl to run securely with Internet Information Server. Do not locate Perl.exe in any directory accessible by a user. Create a script mapping in the Registry for Perl.exe to enable the script to run by using Perl.

▷ **To configure script mapping for Perl**

1. Click the **Start** button, then point to **Run**. In the **Open** box, type **regedt32.exe** and then click **OK**.
2. Click the HKEY_LOCAL_MACHINE window and locate the following key:

   \System
     \CurrentControlSet
       \Services
         \W3SVC
           \Parameters
             \ScriptMap

3. From the **Edit** menu, click **Add Value**.

4. In the **Add Value** dialog box, enter the value name **.pl** with the data type **REG_SZ**.
5. In the **String Editor** dialog box type the string value

   *full path***perl.exe** %s

   and click **OK**.
   This instructs Internet Information Server to interpret all files with the extension .pl by using Perl.exe.
6. To implement these changes, quit the Registry Editor, then stop and restart the WWW service.
7. Test the Perl script with your browser. For example, in Internet Explorer, type

   http://*Servername*/scripts/helloworld.pl?

Programs Attempt to Download to Client Computers

When you attempt to run a script on a client Web browser, an **Unhandled File Type** dialog box might appear. It requests that you save the file as a different filename or in a different location (**Save As**).

The problem is that the /Scripts directory has both Read and Execute access permissions set in Internet Service Manager. To work around this problem, do one of the following:

- Change the access permissions in Internet Service Manager to Execute only.
- Add a question mark (?) to the end of the URL. For example,

  http://myserver/scripts/test.exe?

Programs from 16-bit Compilers Fail to Run

A CGI script compiled with a 16-bit C compiler might fail to run on Internet Information Server.

For example, say you use a 16-bit compiler to compile and build an executable file out of this C language source code:

```
#include <stdio.h>
void main()|
{
   printf( "Content-type: text/html\n\n" );
   printf( "<BODY BGCOLOR=\"#FFFFF0\" TEXT=\"#0000FF\">" );
   printf( "<TITLE>This is a Test page</TITLE>" );
   printf( "<h2>Hello World.</h2><br>" );
   printf( "<h1><center>End of the test page.</center></h1>" );
   printf( "</BODY>\n" );
}
```

If you then run the .exe file from the command prompt of Windows NT, the correct HTML output is generated. However, the results will be different if you place the same executable file in the /Scripts directory of the computer running Internet Information Server. If you try to run it from a Web browser by using the syntax.

http://*Server***/***Path***/***File.exe***?**

it fails to generate the correct page.

To correct this problem, use a 32-bit C compiler to compile and build the C language source code. Microsoft C/C++ 4.0 and C/C++ 2.0 are 32-bit C compilers.

REMOTE_USER Variable Is Blank

Microsoft Internet Information Server does not return a user name for the variable REMOTE_USER unless both of the following are true:

- Basic (clear-text) password authentication is used.
- Anonymous access is not allowed. (That is, you clear the **Allow Anonymous** box on the **WWW Service** property sheet.)

If you use anonymous authentication, all users are authenticated with the IUSR_*computername* account, and the variable is not assigned a value by default.

One method of obtaining the REMOTE_USER variable is to create a batch file with the following lines and save it in the /Scripts directory, or a directory enabled in Internet Information Server for execute permissions:

```
@echo off
echo Content-Type: text/plain
echo.
Set
```

This batch file lists the environment variables used by Internet Information Server, including the REMOTE_USER variable. The list is returned as an HTML page to the Web browser that started the batch file.

Make sure you have configured script mapping for .bat or .cmd files, as described in the *Internet Information Server Installation and Administration Guide.*

You run the script from a browser by typing a URL with the syntax

http://*Server_Name /Script*

For example, you might type

http://www.company.com/scripts/environment.cmd?

The question mark at the end of the URL is required. The question mark signals the server that this is a GET request, which makes the server return script results rather than downloading the file to the user.

CGI Scripts Return Error

When submitting an HTML form or clicking a link to a script from a Web browser, the following message might be returned:

```
CGI Error
The specified CGI application misbehaved by not returning a complete
set of HTTP headers. The headers it did return are:
Can't open perl script "c:\inetsrv\wwwroot\scripts\test.pl":
No such file or directory
```

This error is caused by missing or incorrect CGI header information. In this case, the headers are missing because the script file cannot be run. Therefore, the message was displayed instead of the output from the script.

The CGI specification calls for the script file to return at least one header. This header indicates how to fill out the remainder of the HTTP headers as required by that protocol. HTTP also requires a blank line between the end of the headers and the start of the document. Some servers return an error if the blank line is not present. The only headers currently supported by the CGI specification are:

- Content-type
- Location
- Status

For more information about these headers, see the HTTP and CGI protocol draft specifications at **http://www.w3.org**.

IDC Problems

Troubleshooting Microsoft SQL Server

If an Internet Information Server application cannot connect to SQL Server, it might indicate a problem with the network or SQL Server. You can test Microsoft Internet Information Server connectivity with SQL Server by using tools provided with Microsoft SQL Server. Table 8.3 describes tools included with the Microsoft SQL Server product that can help isolate network problems.

Table 8.3 SQL Server Troubleshooting Tools

SQL Server tool	Purpose	Location
Makepipe.exe	Tests the integrity of the network named pipe services.	SQL Server
Readpipe.exe	Tests the integrity of the network named pipe services.	SQL Server clients
Odbcping.exe	Troubleshoots connectivity to SQL Server through Microsoft ODBC SQL Server drivers.	SQL Server
Isqlw.exe	Queries SQL Server, analyzes the execution plan of a query, and views statistics about the executed query.	SQL Server and clients

For more information about Microsoft SQL Server and these tools, see the *Microsoft SQL Server Books Online.*

SYBASE SQL Server Does Not Work with Internet Information Server

If you try to connect to a SYBASE® database through an .idc file by using the ODBC drivers included in Internet Information Server, you might see this message:

```
Error performing query state=01000, error 1225 Microsoft ODBC SQL Server
Driver DBNMPNTW Connection open Create file
State = 08001 error = 1225 Microsoft ODBC SQL Server Driver unable to
connect to data source.
```

The current Microsoft SQL Server ODBC driver is not certified for use with SYBASE SQL Server.

To correct this problem, use SYBASE SQL Server ODBC drivers. Contact SYBASE Corporation for ODBC drivers certified for use with SYBASE SQL Server. Many third-party ODBC vendors also provide ODBC drivers certified for use with SYBASE SQL Server.

SQL Server Returns 'Not Defined as a Valid User'

You might see the following message when accessing an Internet Database Connector (IDC) script:

```
Error Performing Query
*[State=3700][Error=18450][Microsoft][ODBC SQL Driver][SQL Server]
Login failed- User: _ Reason: Not defined as a valid user of a trusted
SQL Server Connection.
```

This message can appear under the following conditions:

- You are not running SQL Server and Internet Information Server on the same computer.
- You are using Windows NT challenge/response authentication on Internet Information Server.
- You are using integrated or mixed security with Microsoft SQL Server.
- You are not providing the user name or password values in your .idc file.

When the client runs the IDC script, Internet Information Server must determine whether the data source is local or remote. If the data source is defined as Local System, the query is passed to SQL Server on the same computer. If the data source is remote, the computer running Internet Information Server must make a network connection to SQL Server. When Internet Information Server makes the network connection, it does not pass the credentials of the remote user. It passes a blank user name and password instead.

SQL Server does not validate a user without a user name, and returns the message to Internet Information Server. Internet Information Server then passes the results of the query to the client Web browser.

There are two possible workarounds:

- Install SQL Server and Internet Information Server on the same computer. Then set up your ODBC system Data Source Name (DSN) to be Local Server instead of a remote computer name.
- Use Basic authentication instead of Windows NT challenge/response authentication.

Pipe/Connection Busy or Time-out Expired Errors Appear when Using SQL Server

If Internet Information Server connects to Microsoft SQL Server through the Internet Database Connector, multiple error messages can appear as databases are added to SQL Server.

The following messages might be displayed when using the Internet Database Connector to make SQL requests to Microsoft SQL Server, if it has a growing number of databases:

```
*[State=01000][Error=231][Microsoft][ODBC SQL Server Driver]Pipe busy.
*[State=08001][Error=3][Microsoft][ODBC SQL Server Driver]Connection is
busy.
*[State=S1T00][Error=0][Microsoft][ODBC SQL Server Driver]Time-out
expired.
```

These problems can result if the SQL Server configuration parameter Open Databases is set too low. SQL Server 6.0 sets this value to 20 by default. If you add databases to SQL Server until you exceed the configured value, it does not generate an “out of open databases” message in the SQL Server log. Instead, the messages listed above appear when you query the database from Internet Information Server.

To solve this problem, increase the value of the SQL Server configuration parameter Open Databases. For more information on setting this parameter, consult the *Microsoft SQL Server Administrator's Companion.*

Sources of Troubleshooting Information

In addition to the troubleshooting tools that are described later in this chapter, there are several other sources of troubleshooting information in the *Windows NT Server Resource Kit* and elsewhere. Table 8.4 describes resources that can help you in troubleshooting your Internet Information Server installation.

Table 8.4 Sources of Troubleshooting Information

Resource	Information
Windows NT Workstation Resource Guide, Chapter 23, "Overview of the Windows NT Registry"	Describes how to use information in the Registry for troubleshooting and configuration maintenance.
Windows NT Workstation Resource Guide, Chapter 25, "Configuration Management and the Registry"	Provides problem-solving techniques that use the Registry.
Windows NT Workstation Resource Guide, Chapter 36, "General Troubleshooting"	Provides troubleshooting information for Windows NT.
Windows NT Workstation Resource Guide, Chapter 21, "Troubleshooting Startup and Disk Problems"	Discusses what you can do to find the cause of problems when your computer fails to complete startup.
Windows NT Workstation Resource Guide, Chapter 38, "Windows NT Executive STOP Messages"	Describes the different kinds of STOP, STATUS, and hardware malfunction messages.
Windows NT Workstation Resource Guide, Chapter 39, "Windows NT Debugger"	Describes how to set up for debugging and use Windows NT debugging tools.
Windows NT Server Resource Kit Messages database	Documents thousands of messages with the probable cause of errors and recommended solution. This includes the STOP messages that appear when the system fails with a blue screen.
Windows NT Help	Contains troubleshooting information for the Windows NT operating system.
Microsoft Knowledge Base	Contains support information developed by the Microsoft Support Network. The Windows NT Knowledge Base is included on the *Windows NT Workstation Resource Kit* CD and *Windows NT Server Resource Kit* CD. It is also included on the Microsoft Developer Network (MSDN) CD and the TechNet CD, and is accessible through the Microsoft home page, www.microsoft.com. You can search for all Windows NT Internet Information Server articles by specifying Internet Information Server in the query.
Windows NT Workstation Start Here, Appendix A, "Windows NT Setup Troubleshooting"	Describes how to overcome problems installing Windows NT 4.0 on Intel-based computers.

Using Troubleshooting Tools

This section provides a brief overview of the troubleshooting tools that are available on the Windows NT Workstation and Windows NT Server product CDs and the *Windows NT Workstation Resource Kit* CD and *Windows NT Server Resource Kit* CD.

Windows NT Tools

The tools described in Table 8.5 are installed when you install Windows NT Workstation or Windows NT Server.

Table 8.5 Windows NT Troubleshooting Tools

Tool	Purpose	For more information
Event Viewer	Displays the system, security, and application logs.	Chapter 37, "Monitoring Events," in the *Windows NT Workstation Resource Guide*
Performance Monitor	Measures your computer's efficiency, identifies and troubleshoots possible problems, and plans for additional hardware needs.	Part III, "Optimizing Windows NT Workstation," in the *Windows NT Workstation Resource Guide*, and Chapter 8, "Monitoring Performance," in *Windows NT Server Concepts and Planning*
Task Manager	Monitors active applications and processes on your computer, and starts and stops them.	Chapter 11, "Performance Monitoring Tools," in the *Windows NT Workstation Resource Guide*
Windows NT Diagnostics	Enables you to view hardware information in the Registry, such as currently loaded device driver and IRQ values.	Chapter 36, "General Troubleshooting," in the *Windows NT Workstation Resource Guide*
Network Monitor	Determines problems during session initialization and problems related to broadcast storms, and troubleshoots packets for transmission problems between computers.	Chapter 10, "Monitoring Your Network," in *Windows NT Server Concepts and Planning*
TCP/IP Utilities	Verifies and debugs TCP/IP networking problems.	Appendix A, "TCP/IP Utilities," in the *Windows NT Server Networking Guide*

Windows NT Resource Kit Tools

The *Windows NT Workstation Resource Kit* and *Windows NT Server Resource Kit* CDs contain many tools that can be used for troubleshooting. This list shows the tools available:

- Crystal Reports Event Log Viewer
- Device Driver Information
- Dump Event Log
- Find Group
- Obtain Ethernet layer address and binding order
- Task Killing Utility
- Event Logging Utility
- Performance Data Logging Service and Configuration Tool
- Performance Meter
- Performance Tools
- Page Fault Monitor
- Process Resource Monitor
- Process and Thread Status
- Process Viewer
- CPU Usage by Processes
- TimeThis
- Task List Viewer

For information about these tools, refer to the Resource Kit Tools Help and double-click the *Computer Diagnostic Tools* topic on the **Contents** page.

Glossary

A

A-type resource record A line (record) in a computer's Domain Name System database that maps a computer's domain name (host name) to an IP address in a DNS zone.

ActiveX™ An umbrella term for Microsoft technologies that enable developers to create interactive content for the World Wide Web.

application programming interface (API) A set of routines that an application program uses to request and carry out lower-level services performed by another component, such as the computer's operating system or a service running on a network computer.

auditing Tracking activities of users by recording selected types of events in the security log of a server or a workstation.

authentication Validation of a user's logon information. Authentication is used to enforce selective permission to access resources or to perform an operation.

B

backup domain controller (BDC) In a Windows NT Server domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). BDCs also authenticate user logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist on a domain. See also domain controller; primary domain controller.

bandwidth In communications, the difference between the highest and lowest frequencies in a given range. For example, a telephone line accommodates a bandwidth of 3000 Hertz (Hz), the difference between the lowest (300 Hz) and highest (3300 Hz) frequencies it can carry. In computer networks, greater bandwidth indicates faster data-transfer capability and is expressed in bits per second (bps).

Basic (clear-text) authentication A method of authentication that encodes user name and password data transmissions. Basic authentication is called "clear text" because the base-64 encoding can be decoded by anyone with a freely available decoding utility. Note that encoding is not the same as encryption. See also challenge/response authentication; encryption.

BDC See *backup domain controller.*

bits per second (bps) The measure of speed at which data is transferred over a network.

blue screen The screen displayed when Windows NT encounters a serious error.

bootstrap protocol (BOOTP) A TCP/IP network protocol used to configure network computers. Defined by RFC 951 and RFC 1542. DHCP provides a superset of the functions provided by BOOTP. DHCP and BOOTP interoperation is defined by RFC 1534. See also *Dynamic Host Configuration Protocol.*

bps See *bits per second.*

browser See *Web browser.*

BSD UNIX A version of UNIX developed by Berkeley Software Design Incorporated.

bulk data encryption
The encryption of all data sent over a network.

C

CGI See *Common Gateway Interface.*

challenge/response authentication
A method of authentication in which a server uses challenge/response algorithms and Windows NT security to control access to resources. See also *Basic (clear-text) authentication; encryption.*

clear-text authentication See *Basic (clear-text) authentication.*

Common Gateway Interface (CGI)
A standard interface for HTTP server application development. The standard was developed by the National Center for Supercomputing Applications.

connection-oriented protocol A network protocol with four important characteristics: the path for data packets is established in advance; the resources required for a connection are reserved in advance; a connection's resource reservation is enforced throughout the life of that connection; and when a connection's data transfer is completed, the connection is terminated and the allocated resources are freed.

D

Data Source Name (DSN) The logical name used by ODBC to refer to the drive and other information required to access data. The name is use by Internet Information Server for a connection to an ODBC data source, such as a SQL Server database. To set this name, you double-click ODBC in the Control Panel.

dbWeb Administrator The graphical user tool for Microsoft dbWeb that allows an administrator to create definition templates referred to as schemas. Schemas control how and what information from a private database is available to visitors who use the Internet to access the public Microsoft dbWeb gateway to the private database. See also *schemas.*

default gateway In TCP/IP, the intermediate network device on the local network that has knowledge of the network IDs of the other networks in the Internet, so it can forward the packets to other gateways until the packet is eventually delivered to a gateway connected to the specified destination.

DHCP See *Dynamic Host Configuration Protocol.*

DHCP Relay Agent The component responsible for relaying DHCP and BOOTP (bootstrap protocol) broadcast messages between a DHCP server and a client across an IP router. See also *bootstrap protocol; Dynamic Host Configuration Protocol.*

DHCP server Dynamic Host Configuration Protocol server. A server that automatically administers client TCP/IP addresses and related settings for a network.

Dial-Up Networking A component of Windows NT and Windows 95. Enables users to connect to remote networks, such as the Internet or a private network.

directory replication The copying of a master set of directories from a server (called an export server) to specified servers or workstations (called import computers) in the same or other domains. Replication simplifies the task of maintaining identical sets of directories and files on multiple computers, because only a single master copy of the data must be maintained. Files are replicated when they are added to an exported directory, and every time a change is saved to the file. See also *Directory Replicator service.*

Directory Replicator service Replicates directories, and the files in those directories, between computers. See also *directory replication.*

Directory Service Manager for NetWare (DSMN) A component of Windows NT Server. Enables network administrators 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.

DLL See *dynamic-link library.*

DNS name See *domain name.*

DNS name servers In the DNS client/server model, the servers containing information about a portion of the DNS database, which makes computer names available to clients querying for name resolution across the Internet. See also *Domain Name System.*

DNS server See *DNS name servers.*

DNS service The service that provides domain name resolution. See also *DNS name servers.*

domain controller In a Windows NT Server domain, refers to the computer running Windows NT Server that manages all aspects of user-domain interactions, and uses information in the directory database to authenticate users logging on to domain accounts. One shared directory database is used to store security and user account information for the entire domain. A domain has one primary domain controller (PDC) and one or more backup domain controllers (BDCs). See also *backup domain controller; primary domain controller.*

domain name Part of the Domain Name System (DNS) naming structure, a domain name is the name by which a domain is known to the network. Domain names consist of a sequence of labels separated by periods. DNS domains are not Windows NT networking domains. See also *Domain Name System.*

Domain Name System (DNS) Sometimes referred to as the BIND service in BSD UNIX, DNS offers a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses, allowing users of workstations configured to query the DNS to specify remote systems by host names rather than by IP addresses. For example, a workstation configured to use DNS name resolution can use the command **ping remotehost** rather than **ping 172.16.16.235** if the mapping for the system named "remotehost" was contained in the DNS database. DNS domains are not the same as Windows NT networking domains.

DSMN See *Directory Service Manager for NetWare.*

dynamic assignment The automatic assignment of TCP/IP properties in a changing network.

Dynamic Host Configuration Protocol (DHCP) A protocol that offers dynamic configuration of IP addresses and related information. 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. Defined in RFC 1541.

dynamic-link library (DLL) An operating system feature that enables executable routines (generally serving a specific function or set of functions) to be stored separately as files with .dll extensions and to be loaded only when needed by the program that calls them.

E

encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during network transmission or when it is stored on a transportable magnetic medium.

enterprise network A network for a large organization that has several thousand employees (for example, more than 40,000 users) and sometimes has multiple sites.

F

file allocation table (FAT) A table or list maintained by some operating systems to keep track of the status of various segments of disk space used for file storage. Also referred to as the FAT file system. See also *Windows NT File System.*

File and Print Services for NetWare (FPNW) A Windows NT Server component that enables a computer running Windows NT Server to provide file and print services directly to NetWare-compatible client computers.

File Transfer Protocol (FTP) An older TCP/IP protocol used for transferring files between different computers. FTP is characterized by a required logon to the remote computer and the ability to browse directories and two-way file transfer. Most of the functions of this protocol have been subsumed by Hypertext Transport Protocol (HTTP).

firewall A system or combination of systems that enforces a boundary between two or more networks and keeps intruders out of private networks. Firewalls serve as virtual barriers to passing packets from one network to another.

FPNW See *File and Print Services for NetWare.*

Frame Relay A synchronous High-level Data Link Control (HDLC) protocol–based network that sends data in HDLC packets.

FTP See *File Transfer Protocol.*

G

Gateway Service for NetWare (GSNW) A Windows NT Server component that enables a computer running Windows NT Server to connect to NetWare servers. Creating a gateway enables computers running only Microsoft client software to access NetWare resources through the gateway.

Gopher A hierarchical system for finding and retrieving information from the Internet or an intranet. Similar to FTP, Gopher uses a menuing system and enables links to other servers.

GSNW See *Gateway Service for NetWare.*

H

home directory The root directory for an Internet Information Server service. The directory is accessible to the user and contains files and programs. Typically the home directory for a site contains the home page. See also *home page.*

home page The initial page of information for a collection of pages. The starting point for a Web site or section of a Web site is often referred to as the home page. Individuals also post pages that are called home pages.

HOSTS file A local text file in the same format as the 4.3 Berkeley Software Distribution (BSD) UNIX \etc\hosts file. This file maps host names to IP addresses. In Windows NT, this file is stored in the \Systemroot\System32\Drivers\Etc directory.

HTML See *Hypertext Markup Language.*

hyperlink A way of jumping to another place on the Internet. Hyperlinks usually appear in a different format from regular text. You initiate the jump by clicking the link.

Hypertext Markup Language (HTML)
A simple markup language used to create hypertext documents that are portable from one platform to another. HTML files are simple ASCII text files with codes embedded (indicated by markup tags) to indicate formatting and hypertext links. The formatting language used for documents on the World Wide Web.

Hypertext Transport Protocol (HTTP)
The underlying protocol by which WWW clients and servers communicate. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

I

IANA
See *Internet Assigned Numbers Authority.*

IDC
See *Internet Database Connector.*

IETF See *Internet Engineering Task Force.*

IIS See *Internet Information Server.*

IMIII See *Intelligent Messaging III.*

IMC See *Internet Mail Connector.*

Inetinfo A process containing the FTP, Gopher, and HTTP services. This process is about 400K in size. In addition to the FTP, Gopher, and HTTP services, this process contains the shared thread pool, cache, logging, and SNMP services of Internet Information Server.

Integrated Services Digital Network (ISDN)
A type of phone line used to enhance WAN speeds, an ISDN line can transmit at speeds of 64 or 128 kilobits per second, as opposed to standard phone lines, which typically transmit at only 9600 bits per second (bps). An ISDN line must be installed by the phone company at both the server site and the remote site. See also *bits per second.*

Intelligent Messaging III (IMIII) Electronic mail server software for Banyan® VINES® networks.

internet A collection of two or more private networks.

Internet The global network of networks.

Internet Assigned Numbers Authority (IANA)
The central coordinator for the assignment of unique parameter values for Internet protocols. IANA is chartered by the Internet Society (ISOC) and the Federal Network Council (FNC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters. Contact IANA at **http://www.iana.org/iana/.**

Internet Assistant Several Internet Assistant add-on software components are available for Microsoft Office products. Each Internet Assistant adds functionality that is relevant to creating content for the Internet. For example, Internet Assistant for Microsoft Word enables Word to create HTML documents from within Microsoft Word.

Internet Database Connector (IDC)
Provides access to databases for Internet Information Server by using ODBC. The Internet Database Connector is contained in Httpodbc.dll, which is an Internet Server API DLL.

Internet Engineering Task Force (IETF)
A consortium that introduces procedures for new technology on the Internet. IETF specifications are released in documents called requests for comments (RFCs). See also *request for comments.*

Internet Information Server (IIS) A network file and application server that supports multiple protocols. Primarily, Internet Information Server transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

Internet Mail Connector (IMC) The Internet Mail Connector is a component of Microsoft Exchange Server that runs as a Windows NT Server service. You can use the Internet Mail Connector to exchange information with other systems that use the Simple Mail Transfer Protocol (SMTP).

Internet Network Information Center (InterNIC)
The coordinator for DNS registration. To register domain names and obtain IP addresses, contact InterNIC at **http://internic.net.**

Internet Protocol (IP) The part of TCP/IP that routes messages from one Internet location to another. IP is responsible for addressing and sending TCP packets over the network. IP provides a best-effort, connectionless delivery system that does not guarantee that packets arrive at their destination or that they are received in the sequence in which they were sent. See also *packet.*

Internet Relay Chat (IRC) A protocol that enables two or more people, each in remote locations, who are connected to an IRC server to hold real-time conversations. IRC is defined in RFC 1459.

Internet Server Application Programming Interface (ISAPI)
An API for developing extensions to the Microsoft Internet Information Server and other HTTP servers that support the ISAPI interface. See also *application programming interface.*

Internet service provider (ISP) A company or educational institution that enables remote users to access the Internet by providing dial-up connections or installing leased lines.

InterNIC See *Internet Network Information Center.*

intranet A TCP/IP network that uses Internet technology. May be connected to the Internet; if connected to the Internet, intranets are usually protected by a firewall or other security device.

IP See *Internet Protocol.*

IP address Used to identify a node on a network and to specify routing information. Each node on the network must be assigned a unique IP address, which is made up of the network ID, plus a unique host ID assigned by the network administrator. This address is typically represented in dotted-decimal notation, of four period-delimited octets (eight bits, or one byte) consisting of up to 12 numerals (for example, 138.57.7.27). See also *Dynamic Host Configuration Protocol; node.*

IPX Transport protocol used in Novell NetWare networks. Also referred to as IPX/SPX. Windows NT implements IPX through NWLink.

ISDN interface card Similar in function to a modem, an ISDN card is hardware that enables a computer to connect to other computers and networks on an Integrated Services Digital Network.

ISP See *Internet service provider.*

K

kiosk A computer, connected to the Internet, made available to users in a commonly accessible location.

L

LAN See *local area network.*

leased line A high-capacity line (most often a telephone line) dedicated to network connections.

line printer daemon (LPD) A line printer daemon service on the print server receives documents (print jobs) from line printer remote (LPR) utilities running on client systems.

LMHOSTS file A local text file that maps IP addresses to the computer names of Windows NT networking computers outside the local subnet. In Windows NT, this file is stored in the *Systemroot* \System32\Drivers\Etc directory.

local area network (LAN) A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

Local Mail Delivery Agent The component of the SMTP server that processes messages that have been received by the SMTP server and downloads the messages to the user's local computer.

loopback address The IP address 127.0.0.1, which has been specified by the Internet Engineering Task Force as the IP address to use in conjunction with a loopback driver to route outgoing packets back to the source computer. See also *loopback driver.*

loopback driver A network driver that allow the packets to bypass the network adapter card completely and be returned directly to the computer that is performing the test. See also *loopback address.*

LPD See *line printer daemon.*

M

Mail Server (MailSrv) A Windows NT service that sends and receives electronic mail on a TCP/IP network by using the SMTP and POP3 protocols. Also simply referred to as an SMTP server, this tool is provided in the *Windows NT Server Resource Kit.*

Management Information Databases (MIBs) Software that describes manageable aspects of your network that use the Simple Network Management Protocol (SNMP). The MIB files included with Windows NT can be used by third-party SNMP monitors to enable SNMP monitoring.

Microsoft dbWeb A database publishing gateway provided in the *Windows NT Server Resource Kit.* dbWeb can run under Internet Information Server to provide public access to private enterprise ODBC sources as specified by an administrator of the private enterprise.

The Microsoft Network (MSN) Online service that offers a free Internet site to all Internet users. Subscribers can also use proprietary information and obtain Internet access.

MIME See *Multipurpose Internet Mail Extensions.*

modem Modulator/demodulator. A communications device that enables a computer to transmit information over a standard telephone line.

MPR See *multiprotocol routing.*

multihomed system A system with multiple network adapters attached to separate physical networks.

multiport serial adapter A communications device that enables a computer to simultaneously transmit information over standard telephone lines to multiple computers. Similar to multiple modems contained in one device. See also *modem.*

multiprotocol routing (MPR) Enables routing over IP and IPX networks by connecting LANs or by connecting LANs to WANs. MPR refers to both the **RIP for Internet Protocol** service and the **RIP for NWLink IPX/SPX Compatible Transport** service.

Multipurpose Internet Mail Extensions (MIME) A standard mechanism for specifying and describing the format of Internet message bodies. MIME enables the exchanging of objects, different character sets, and multimedia in e-mail on different computer systems. Defined in RFC 1521.

MX record The MX (mail exchanger) resource record specifies a mail exchange server for a DNS domain name. A mail exchange server is a host (computer or other network device) that will either process or forward mail for the DNS domain name.

N

NCSA National Center for Supercomputing Applications is a scientific research center that is developing and implementing a national strategy to create, use, and transfer advanced computing and communication tools and information technologies. Developed one of the first Web browsers.

NDS See *NetWare Directory Services.*

NetBEUI A network protocol usually used in small, department-size local area networks of 1 to 200 clients. It can use Token Ring source routing as its only method of routing. See also *router.*

NetBIOS See *network basic input/output system.*

NetWare Directory Services (NDS) A NetWare service that runs on NetWare servers. The service enables the location of resources on the network.

network basic input/output system (NetBIOS) An application programming interface (API) that can be used by applications on a local area network. NetBIOS provides applications with a uniform set of commands for requesting the lower-level services required to conduct sessions between nodes on a network and to transmit information back and forth. See also *application programming interface.*

network card An expansion card or other device used to connect a computer to a local area network (LAN). Also called a network adapter; network adapter card; adapter card; network interface card (NIC).

network drive See *shared directory.*

Network File System (NFS) A service for distributed computing systems that provides a distributed file system, eliminating the need to keep multiple copies of files on separate computers.

network interface card (NIC) See *network card.*

Network News Transfer Protocol (NNTP) The protocol used to distribute network news messages to NNTP servers and to NNTP clients (news readers) on the Internet. NNTP provides for the distribution, inquiry, retrieval, and posting of news articles by using a reliable stream-based transmission of news on the Internet. NNTP is designed so that news articles are stored on a server in a central database, thus enabling a user to select specific items to read. Indexing, cross-referencing, and expiration of aged messages are also provided. Defined in RFC 977.

network protocols Software that enables computers to communicate over a network. The Internet protocol is TCP/IP.

NFS See *Network File System.*

NIC See network card.

node Any workstation, server, printer, or other device on a network that uses TCP/IP. Also called host.

NTFS See *Windows NT File System.*

NWLink IPX/SPX Compatible Transport A standard network protocol that supports routing, and can support NetWare client/server applications, where NetWare-aware sockets-based applications communicate with IPX\SPX sockets-based applications.

O

Open Database Connectivity (ODBC) ODBC is an application programming interface that enables applications to access data from a variety of existing data sources.

P

packet A transmission unit of fixed maximum size that consists of binary information representing both data and a header containing an ID number, source and destination addresses, and error-control data.

PDC See *primary domain controller.*

Peer Web Services A collection of services that enable the user of a computer running Windows NT Workstation to publish a personal Web site from the desktop. The services include the WWW service, the FTP service, and the Gopher service.

Perl Practical Extraction and Report Language. A scripting (programming) language that is frequently used for CGI scripts.

Point-to-Point Protocol (PPP) A set of industry-standard framing and authentication protocols included with Windows NT Remote Access Service to ensure interoperability with third-party remote access software. PPP negotiates configuration parameters for multiple layers of the OSI (Open Systems Interconnection) model.

Point-to-Point Tunneling Protocol (PPTP) A new networking technology that supports multiprotocol virtual private networks (VPNs). PPTP enables secure access to private networks across the Internet. With PPTP enabled, remote users can dial into an Internet service provider (ISP), or connect directly to the Internet, and all communication between the user and private network is secure.

Post Office Protocol (POP) The Post Office Protocol version 3 (POP3) is a protocol that permits a workstation to dynamically access a mail drop on a server in a useful fashion. Usually, this means that a POP3 server is used to allow a workstation to retrieve mail that an SMTP server is holding for it. POP3 is specified in RFC 1725.

POTS Acronym for Plain-Old Telephone Service. Same as public switched telephone network (PSTN). POTS is also an acronym for point of termination station, which refers to where a telephone call terminates.

primary domain controller (PDC) In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC. See also *backup domain controller; domain controller.*

PTR record The pointer (PTR) resource record maps an IP address to a host name in a DNS reverse zone (those in the In-addr.arpa DNS domain).

public key cryptography A method of encrypting data transmissions to and from a server.

Q

query-by-example (QBE) A simple-to-use query language implemented on relational database management systems.

R

Remote Access Service (RAS) A service that can be used by remote clients running Microsoft Dial-Up Networking, all Microsoft RAS clients, or any third-party PPP client to dial in to a network. Remote users with RAS on a Windows NT–based computer can dial in to their networks for services such as Internet access, file and printer sharing, electronic mail, scheduling, and SQL database access.

remote procedure call (RPC) A message-passing facility that allows a distributed application to call services available on various machines in a network. Used during remote administration of computers.

replicate See *directory replication.*

request for comments (RFC) An official document of the IETF (Internet Engineering Task Force) that specifies the details for protocols included in the TCP/IP family. See also Internet Engineering Task Force.

RIP See *Routing Information Protocol.*

router A network device that manages traffic between networks or subnets. Routers match packet headers to a location on a LAN and choose the best path for the packet, optimizing network performance.

Routing Information Protocol (RIP)
Enables a router to exchange routing information with a neighboring router. See also *router.*

RPC See *remote procedure call.*

S

Schema Wizard Interactive tool in dbWeb Administrator that leads a user through creation of HTML pages or through implementing an ISAPI application.

schemas
Schemas control how and what information from a private database is available to visitors who use the Internet to access the public Microsoft dbWeb gateway to the private database. See also *dbWeb administrator.*

Secure Sockets Layer (SSL) A protocol that supplies secure data communication through data encryption and decryption. SSL enables communications privacy over networks by using a combination of public key cryptography and bulk data encryption.

Serial Line Internet Protocol (SLIP)
An older industry standard that is part of Windows NT Remote Access Service to ensure interoperability with third-party remote access software.

service pack An update to the Windows NT operating system.

shared directory A directory that network users can connect to.

Simple Mail Transfer Protocol (SMTP)
A protocol used on TCP/IP networks to exchange mail on the Internet between SMTP servers.

Simple Network Management Protocol (SNMP)
A protocol for monitoring your network. The protocol is used by SNMP consoles and agents to communicate. In Windows NT, the SNMP service is used to get and set status information about a host on a TCP/IP network. See also *Management Information Databases.*

SLIP See *Serial Line Internet Protocol.*

SMTP See *Simple Mail Transfer Protocol.*

sniffer A network device that monitors packets sent over a network.

SNMP See *Simple Network Management Protocol.*

socket A bidirectional pipe for incoming and outgoing data between networked computers. Defined in the University of California at Berkeley Sockets API. See also *Windows Sockets.*

SQL See *structured query language.*

SQL Server A server typically running on a personal computer that uses the structured query language to query, update, and manage a relational database.

SSL See *Secure Sockets Layer.*

static mapping A method provided on a WINS server to assign a static (unchanging) IP address to a client.

static routing Static routing limits you to fixed routing tables, as opposed to dynamically updating the routing tables.

structured query language (SQL)
A database query and programming language originally developed by IBM for mainframe computers. It is widely used for accessing data in, querying, updating, and managing relational database systems. See also *SQL Server.*

subnet mask A TCP/IP configuration parameter that extracts network and host configuration from an IP address. This 32-bit value enables the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID.

Systems Management Server A Windows NT Server network server application that remotely manages the personal computers on a network. Systems Management Server detects computers on the network, inventories software and hardware configurations, and installs desktop applications from a central location.

T

T1 or T3 connection Standard measurements of network bandwidth.

tag file A configuration file that contains information about a corresponding file on a Gopher server or links to other servers. This information is sent to clients in response to a Gopher request.

TCP/IP See *Transmission Control Protocol/Internet Protocol.*

Telnet (VTP) A terminal emulation protocol for logging on to remote computers. Once referred to as Virtual Terminal Protocol (VTP). Defined in RFC 854, among others. See also Telnet Server.

Telnet Server A server that runs a Telnet service, enabling remote users to log on and run programs. See also *Telnet.*

TFTP See *Trivial File Transfer Protocol.*

token ring network A local area network formed in a ring (closed loop) topology that uses token passing as a means of regulating traffic on the line.

transforms Rules the administrator creates to add, remove, and modify domain names appended to inbound and outbound messages.

Transmission Control Protocol/Internet Protocol (TCP/IP)
A set of networking protocols that provide communications across interconnected networks made up of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trivial File Transfer Protocol (TFTP)
A file transfer protocol that transfers files to and from a remote computer running the TFTP service. TFTP was designed with less functions than FTP. Defined in RFC 1350, among others. See also *File Transfer Protocol.*

U

UDP See *User Datagram Protocol.*

Uniform Resource Locator (URL)
A naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the appropriate Internet protocol, such as HTTP, FTP, IRC, or Gopher.

Uninterruptible Power Supply (UPS)
A battery-operated power supply connected to a computer to keep the system running during a power failure.

URL See *Uniform Resource Locator.*

User Datagram Protocol (UDP) A TCP complement that offers a connectionless datagram service that guarantees neither delivery nor correct sequencing of delivered packets (much like IP). See also *packet.*

UUENCODE (UNIX-to-UNIX Encode) A utility that converts a binary file (such as a word-processing file or a program) to text so that it can be transmitted over a network. UUDECODE (UNIX-to-UNIX Decode)is the utility used to convert the file back to its original state.

V

virtual directory An Internet Information Server directory outside the home directory. A virtual directory appears to browsers as a subdirectory of the home directory.

virtual server A computer with several IP addresses assigned to the network adapter card. This configuration makes the computer look like several servers to a browser.

Virtual Terminal Protocol (VTP) See *Telnet.*

W

WAIS See *wide area information server.*

WAN See *wide area network.*

Web browser A software program, such as Internet Explorer, that retrieves a document from a Web server, interprets the HTML codes, and displays the document to the user with as much graphical content as the software can supply.

Web page A World Wide Web document. Pages can contain almost anything, such as news, images, movies, and sounds.

Web server A computer equipped with the server software to respond to HTTP requests, such as requests from a Web browser. A Web server uses the HTTP protocol to communicate with clients on a TCP/IP network.

Well Known Port Number The standard port numbers used by the Internet community for well known (commonly used) services. Ports are used in TCP to name the ends of logical connections that carry long-term conversations. Well known services are defined by RFC 1060. The relationship between the well known services and the well known ports is described in RFC 1340.

wide area information server (WAIS) A network publishing system designed to help users find information over a computer network. WAIS software has four main components: the client, the server, the database, and the protocol. Discussed in RFC 1625.

wide area network (WAN) A communications network that connects geographically separated areas.

Windows Internet Name Service (WINS) A name resolution service that runs on Windows NT Server. WINS resolves NetBIOS computer names to IP addresses for WINS clients on a routed network. A WINS server handles name registrations, queries, and releases. See also *Domain Name System; IP address; WINS server.*

Windows NT File System (NTFS) A file system used on computers running Windows NT that enables users to set access control permissions on files and directories. NTFS supports file system recovery, extremely large storage media, long filenames, and various features for the POSIX subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes. See also *file allocation table.*

Windows NT Server Event Viewer
A program provided with Windows NT that enables users to monitor system, security, and application events by viewing logs generated by Event Viewer.

Windows Sockets Windows Sockets is a Windows implementation of the widely used UC Berkeley Sockets API. The Windows Sockets API is a networking API used by programmers to create TCP/IP–based sockets applications. Microsoft TCP/IP, NWLink, and AppleTalk® protocols use this interface. Windows Sockets provides interfaces between programs and the transport protocol and works as a bidirectional pipe for incoming and outgoing data. Also called WinSock API. See also *application programming interface.*

WINS See *Windows Internet Name Service.*

WINS server A computer running Windows NT Server and the WINS service.

World Wide Web (WWW) The World Wide Web has become synonymous with the Internet. However, the World Wide Web began as a networked information project developed by Tim Berners-Lee at the European Laboratory for Particle Physics (CERN). The World Wide Web is, specifically, the software, protocols, conventions, and information that enable hypertext and multimedia publishing of resources on different computers around the world.

X

X.25 (interface card) A recommendation published by the Comite Consultatif International de Telegraphique et Telephonique (CCITT) international communications standards organization, X.25 defines the connection between a terminal and a packet-switching network. An X.25 network is a type of packet-switching network that routes units of information (packets) as specified by X.25 and is used in public data communications networks. See also *packet.*

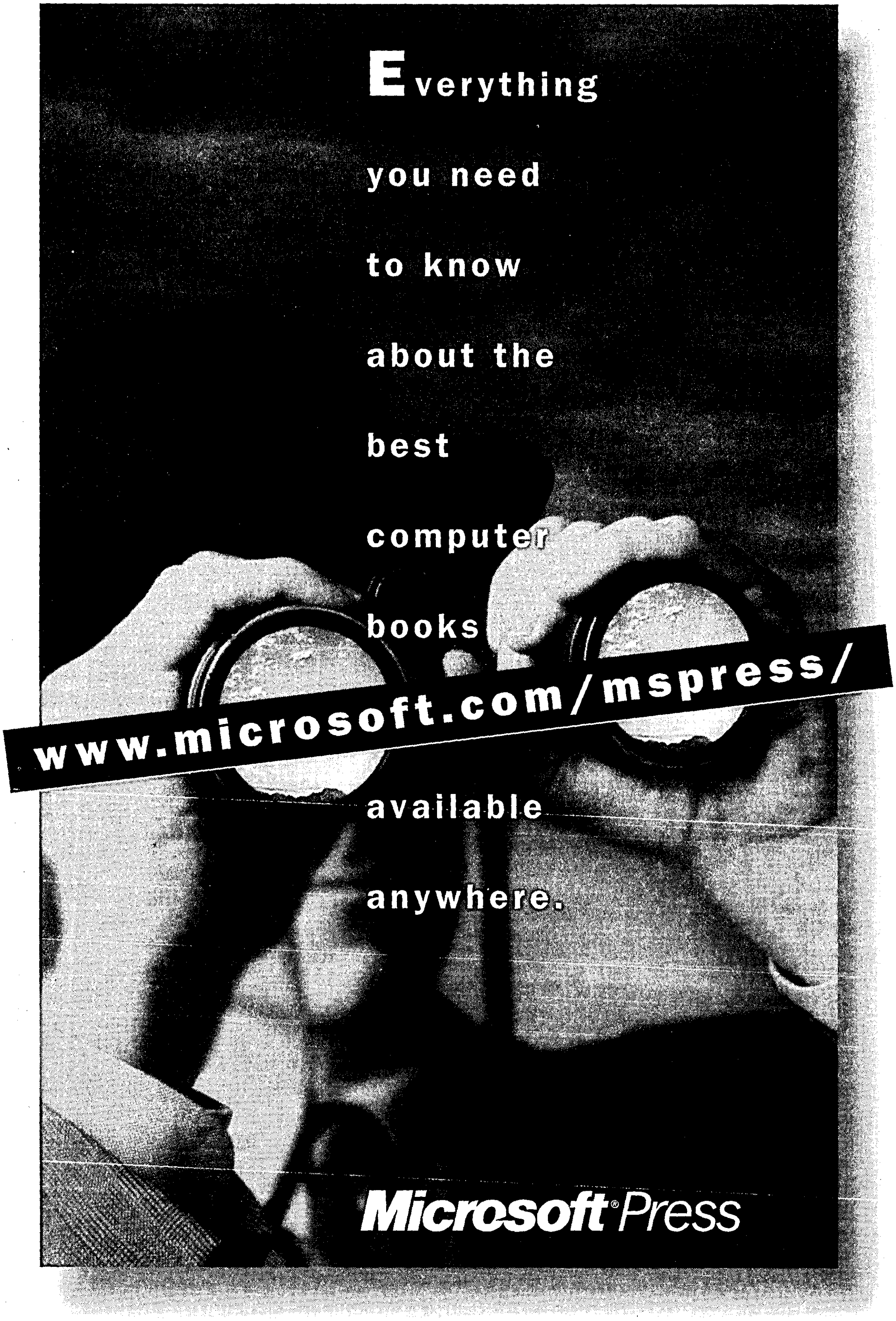
X.400 system A messaging system that is compliant with the X.400 standards developed under the Comite Consultatif International de Telegraphique et Telephonique (CCITT) and the International Standards Organization (ISO).

X Windows A graphical windowing system for UNIX computers.

Z

zone data file A Domain Name System database for a zone in the DNS name space.

Index


Everything
you need
to know
about the
best
computer
books
www.microsoft.com/mspress/
available
anywhere.
Microsoft® Press

Microsoft® Windows NT® Server

Internet Guide

For Windows NT Server Version 4.0

This companion volume to the *Microsoft Windows NT Server Resource Guide* and the *Microsoft Windows NT Server Networking Guide* provides the tools and information needed by network administrators who are responsible for maintaining and integrating Microsoft Windows NT Server version 4.0 in an Internet environment.

The MICROSOFT WINDOWS NT SERVER INTERNET GUIDE covers:

- Microsoft Internet Information Server architecture
- Connecting Windows NT Server to the Internet
- Server security on the Internet
- Desktop and enterprise scenarios
- Internet connectivity scenarios using the Remote Access Service
- Internet tools
- Troubleshooting an Internet Information Server installation

Use this valuable resource to learn what you need to know about the Internet features of Microsoft Windows NT Server version 4.0.

Part No. 097-0001649

Microsoft® Press