Microsoft

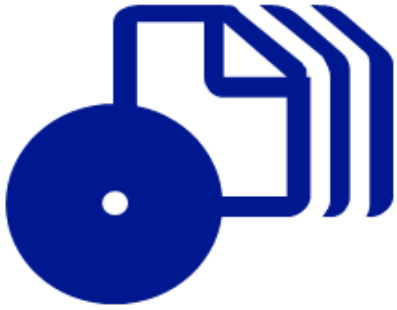
William R. Stanek
Award-winning author and Windows administration expert

Windows Server® 2008

INSIDE OUT

- The ultimate, in-depth reference
- Hundreds of timesaving solutions
- Supremely organized book and CD

How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/624382/files, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

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

Library of Congress Control Number: 2007942102

ISBN: 978-0-7356-2438-2

Printed and bound in the United States of America.

5 6 7 8 9 10 11 12 13 QGT 7 6 5 4 3 2

Distributed in Canada by H.B. Fenn and Company Ltd.

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 infor-mation about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Acquisitions Editor: Martin DelRe
Developmental Editor: Karen Szall
Project Editor: Victoria Thulman
Editorial Production: Publishing.Com
Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X14-40131 [2012-03-23]

Contents at a Glance

Table of Contents

Part 3: Managing Windows Server 2008 Storage and File Systems

Part 4: Managing Windows Server 2008 Networking and Print Services

Part 5: Managing Active Directory and Security

Acknowledgments

Few projects have ever been as challenging or as fun as writing *Windows Server 2008 Inside Out*. Why? When I set out to write *Windows Server 2008 Inside Out*, I decided I would try to detail every quirk, every insider secret, and every sticky detail that I've learned about Windows Server 2008 since I started working with it in 2002—back when Windows Server 2008 was known as Windows Longhorn. As nearly six years have passed since I began working with Windows Server 2008, it is my sincere hope that the book you hold in yours hands is the best of its class when it comes to managing a Windows Server 2008 implementation and handling everyday administration. I also hope the result of all the hard work is that *Windows Server 2008 Inside Out* is something unique. It takes into account all the experiences I've had while consulting, conducting training courses, and writing books about Windows Vista and Windows Server 2008. As this is my 35th Windows-related book and I've helped millions of people learn Windows over my 20+-year career, I hope that counts for an awful lot. But no man is an island and this book couldn't have been written without help from some very special people.

Without the support of my wife and children, this book would not have been possible. As I literally was writing every day since I signed on to this project—holidays included—my wife had to manage everything else and the little ones had a lot more responsibilities around the house. Thank you for your support and your extraordinary ability to put up with the clackety-clackety of my keyboard.

As I've stated in *Windows Server 2008 Administrator's Pocket Consultant* and in *Windows Vista Administrator's Pocket Consultant*, the team at Microsoft Press is top-notch. Karen Szall was instrumental throughout the writing process. Martin DelRe was the acquisitions editor for the project. He believed in the book and my unique approach and was really great to work with. Completing and publishing the book wouldn't have been possible without their help! Thanks also to Lucinda Rowley!

Curt Philips headed up the editorial process for Publishing.com. As the project manager for this and other Pocket Consultants I've written, he wore many hats and helped out in many ways. Thank you! I'd also like to add that everyone was very understanding—writing a book of this length is very fun but also very exhausting.

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I've seen anywhere—and I've written a lot of books for many different publishers. Randall Galloway was the technical editor for the book. Rozanne Whalen served as the copyeditor and was particularly thorough in her edits, which was much appreciated. I also want to thank Andrea Fox for her careful proofreading of the pages.

I want to thank a number of other people at Microsoft who provided technical reviews and insights, including Jose Luis Auricchio, Craig Threadgill, Jackson Robinson, Sasa Vidanovic, Anders Brabæk, Chris Gregory, Pat Telford, Monica Ene-Pietrosanu, Jose Renato Roda, Robert Hoover, Deepak Shenoy, Akshat Kesarwani, Shawn Travers, Heath Aubin, David Kennedy, Greg Cottingham, Sanjay Pandit, Lesley Kipling, Bernardo Castaneda Leon, Mark Kradel, and Robert Mitchell. Robert Mitchell in particular went above and beyond. Thank you!

I'd also like to thank Valerie DeGiulo and the Microsoft Press Creative Team for their contributions.

Hopefully, I haven't forgotten anyone but if I have, it was an oversight. *Honest*. ;-)

About the CD

The companion CD that ships with this book contains many tools and resources to help you get the most out of your *Inside Out* book.

What's on the CD

The companion CD is loaded with useful tools and links to help you with your Windows Server 2008 installation. The CD includes:

- **Complete e-book** An electronic version of *Windows Server 2008 Inside Out* in PDF format.
- **Product information** Links to information about the features and capabilities of Windows Server 2008 as well as product guides to help you optimize Windows Server 2008 in your enterprise.
- **Resources** Links to white papers, guides, webcasts, test labs and more to help you use and troubleshoot the features of Windows Server 2008.
- **Scripts** More than 700 sample scripts to help you automate management and maintenance tasks.
- **Tools** Many links to tools for IIS, PowerShell, System Center Data Operations, and more that you can put to use right away.
- **Sample chapters** Chapters from 15 other Windows Server 2008 books contain a wealth of information and provide a preview look at books that were recently published or will be published in the near future.

System Requirements

The following are the minimum system requirements necessary to run the CD:

- Microsoft Windows Vista, Windows XP with Service Pack (SP) 2, Windows Server 2003 with SP1, or newer operating system
- 500 megahertz (MHz) processor or higher
- 2 gigabyte (GB) storage space (a portion of this disk space will be freed after installation if the original download package is removed from the hard drive)
- 256 megabytes (MB) RAM
- CD-ROM or DVD-ROM drive
- 1024×768 or higher resolution monitor

- Microsoft Windows or Windows Vista–compatible sound card and speakers
- Microsoft Internet Explorer 6 or newer
- Microsoft Mouse or compatible pointing device

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD.
Visit http://www.microsoftpressstore.com/title/9780735624382 to get your downloadable content. This content is always up-to-date and available to all readers.

Viewing the E-Book

The electronic version of the book and some of the other documentation included on this CD is provided in Portable Document Format (PDF). To view these files, you will need Adobe Acrobat or Acrobat Reader. For more information about these products or to download the Acrobat Reader, visit the Adobe Web site at *http://www.adobe.com*.

Support Information

Every effort has been made to ensure the accuracy of the contents of the book and of this CD. As corrections or changes are collected, they will be added to a Microsoft Knowledge Base article. Microsoft Press provides support for books and companion CDs at the following Web site:

http://www.microsoft.com/learning/support/books/

If you have comments, questions, or ideas regarding the book or this CD, or questions that are not answered by visiting the site above, please send them via e-mail to:

mspinput@microsoft.com

You can also click the Feedback or CD Support links on the Welcome page. Please note that Microsoft software product support is not offered through the above addresses. If your question is about the software, and not about the content of this book, please visit the Microsoft Help and Support page or the Microsoft Knowledge Base at:

http://support.microsoft.com

In the United States, Microsoft software product support issues not covered by the Microsoft Knowledge Base are addressed by Microsoft Product Support Services. Location-specific software support options are available from:

http://support.microsoft.com/gp/selfoverview/

Microsoft Press provides corrections for books through the World Wide Web at *http://www.microsoft.com/mspress/support/*. To connect directly to the Microsoft Press Knowledge Base and enter a query regarding a question or issue that you may have, go to *http://www.microsoft.com/mspress/support/search.htm*.

Find Additional Content Online

As new or updated material becomes available that complements your book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. Based on the final build of Windows Server 2008, the type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site will be available soon at *www.microsoft.com/learning/books/online/serverclient*, and will be updated periodically.

How to Reach the Author

E-mail: williamstanek@aol.com

Web: *http://www.williamstanek.com/*

Conventions and Features Used in This Book

This book uses special text and design conventions to make it easier for you to find the information you need.

Text Conventions

Convention	Meaning
Abbreviated menu commands	For your convenience, this book uses abbreviated menu commands. For example, "Click Tools, Track Changes, Highlight Changes" means that you should click the Tools menu, point to Track Changes, and click the Highlight Changes command.
Boldface type	**Boldface** type is used to indicate text that you enter or type.
Initial Capital Letters	The first letters of the names of menus, dialog boxes, dialog box elements, and commands are capitalized. Example: the Save As dialog box.
Italicized type	*Italicized* type is used to indicate new terms.
Plus sign (+) in text	Keyboard shortcuts are indicated by a plus sign (+) separating two key names. For example, Ctrl+Alt+Delete means that you press the Ctrl, Alt, and Delete keys at the same time.

Design Conventions

INSIDE OUT

This statement illustrates an example of an "Inside Out" heading

These are the book's signature tips. In these tips, you'll get the straight scoop on what's going on with the software—inside information about why a feature works the way it does. You'll also find helpful hints, timesaving tricks, and handy workarounds to deal with software problems or alternative procedures related to the task being discussed.

TROUBLESHOOTING

This statement illustrates an example of a "Troubleshooting" problem statement

Look for these sidebars to find solutions to common problems you might encounter. Troubleshooting sidebars appear next to related information in the chapters. You can also use the Troubleshooting Topics index at the back of the book to look up problems by topic.

CAUTION!

Cautions identify potential problems that you should look out for when you're completing a task or problems that you must address before you can complete a task.

Note

Notes offer additional information related to the task being discussed.

Sidebars

The sidebars sprinkled throughout these chapters provide ancillary information on the topic being discussed. Go to the sidebars to learn more about the technology or a feature.

Cross-references point you to other locations in the book that offer additional information about the topic being discussed.

CHAPTER 7

Configuring Roles, Role Services, and Features

Windows Server 2008 has different configuration architecture than its predecessors. You prepare servers for use by installing and configuring the following components:

- **Server roles** Server roles are related sets of software components that allow servers to perform a specific function for users and other computers on networks. A computer can be dedicated to a single role, such as Active Directory Domain Services, or a computer can provide multiple roles.
- **Role services** Role services are software components that provide the functionality of server roles. Each server role has one or more related role services. Some server roles, such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP), have a single function and installing the role installs this function. Other roles, such as Network Policy And Access Services and Active Directory Certificate Services, have multiple role services that you can install. With these server roles, you can choose which role services to install.
- **Features** Features are software components that provide additional functionality. Features, such as WINS and Windows Server Backup, are installed and removed separately from roles and role services. A computer can have multiple features installed or none, depending on its configuration.

You configure roles, role services, and features using the Server Manager console. Server Manager has a command-line counterpart, called ServerManagerCmd.exe, which you can install as a feature.

Using Roles, Role Services, and Features

Before modifying a server's configuration, you should carefully plan how adding or removing a role, role service, or feature will affect a server's overall performance. Although you typically want to combine complementary roles, doing so increases the workload on the server, so you'll need to optimize the server hardware accordingly. Also, keep in mind that roles, role services, and features can be dependent on other roles, role services, and features. When you install roles, role services, and features, Server Manager prompts you to install any additional roles, role services, or features that are required. If you try to remove a required component of an installed role, role service, or feature, Server Manager warns that you cannot remove the component unless you also remove the other role, role service, or feature.

Table 7-1 provides an overview of the primary roles and the related role services that you can deploy on a server running Windows Server 2008. In addition to roles and features that are included with Windows Server 2008 by default, Server Manager enables integration of additional roles and features that are available on the Microsoft Download Center as optional updates to Windows Server 2008.

Table 7-1 Primary Roles and Related Role Services for Windows Server 2008

Role	Description
Active Directory Certificate Services (AD CS)	AD CS provides functions necessary for issuing and revoking digital certificates for users, client computers, and servers. Includes these role services: Certification Authority, Certification Authority Web Enrollment, Online Certificate Status Protocol, and Microsoft Simple Certificate Enrollment Protocol (MSCEP).
Active Directory Domain Services (AD DS)	AD DS provides functions necessary for storing information about users, groups, computers, and other objects on the network and makes this information available to users and computers. Domain controllers give network users and computers access to permitted resources on the network.
Active Directory Federation Services (AD FS)	AD FS complements the authentication and access management features of AD DS by extending them to the World Wide Web. Includes these role services and subservices: Federation Service, Federation Service Proxy, AD FS Web Agents, Claims-Aware Agent, and Windows Token-Based Agent.
Active Directory Lightweight Directory Services (AD LDS)	AD LDS provides a data store for directory-enabled applications that do not require AD DS and do not need to be deployed on domain controllers. Does not include additional role services.
Active Directory Rights Management Services (AD RMS)	AD RMS provides controlled access to protected e-mail messages, documents, intranet Web pages, and other types of files. Includes these role services: Active Directory Rights Management Server and Identity Federation Support.
Application Server	Application Server allows a server to host distributed applications built using ASP.NET, Enterprise Services, and .NET Framework 3.0. Includes more than a dozen role services, which are discussed in detail in *Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant* (Microsoft Press, 2007).
DHCP Server	DHCP provides centralized control over Internet Protocol (IP) addressing. DHCP servers can assign dynamic IP addresses and essential TCP/IP settings to other computers on a network. Does not include additional role services.
DNS Server	DNS is a name resolution system that resolves computer names to IP addresses. DNS servers are essential for name resolution in Active Directory domains. Does not include additional role services.
Fax Server	Fax Server provides centralized control over sending and receiving faxes in the enterprise. A fax server can act as a gateway for faxing and allows you to manage fax resources, such as jobs and reports, and fax devices on the server or on the network. Does not include additional role services.

Role	Description
File Services	File Services provide essential services for managing files and the way they are made available and replicated on the network. A number of server roles require some type of file service. Includes these role services and subservices: File Server, Distributed File System, DFS Namespace, DFS Replication, File Server Resource Manager, Services for Network File System (NFS), Windows Search Service, Windows Server 2003 File Services, File Replication Service (FRS), and Indexing Service.
Network Policy And Access Services (NPAS)	NPAS provides essential services for managing routing and remote access to networks. Includes these role services: Network Policy Server (NPS), Routing And Remote Access Services (RRAS), Remote Access Service, Routing, Health Registration Authority, and Host Credential Authorization Protocol (HCAP).
Print Services	Print Services provide essential services for managing network printers and print drivers. Includes these role services: Print Server, LPD Service, and Internet Printing.
Terminal Services	Terminal Services provide services that allow users to run Windows-based applications that are installed on a remote server. When users run an application on a terminal server, the execution and processing occur on the server, and only the data from the application is transmitted over the network. Includes these role services: Terminal Server, TS Licensing, TS Session Broker, TS Gateway, and TS Web Access.
Universal Description Discovery Integration (UDDI) Services	UDDI provides capabilities for sharing information about Web services both within an organization and between organizations. Includes these role services: UDDI Services Database and UDDI Services Web Application.
Web Server (IIS)	Web Server (IIS) is used to host Web sites and Web-based applications. Web sites hosted on a Web server can have both static content and dynamic content. You can build Web applications hosted on a Web server using ASP.NET and .NET Framework 3.0. When you deploy a Web server, you can manage the server configuration using IIS 7.0 modules and administration tools. Includes several dozen role services, which are discussed in detail in *Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant*.
Windows Deployment Services (WDS)	WDS provides services for deploying Windows computers in the enterprise. Includes these role services: Deployment Server and Transport Server.
Windows SharePoint Services	Windows SharePoint Services enable team collaboration by connecting people and information. A SharePoint server is essentially a Web server running a full installation of IIS and using managed applications that provide the necessary collaboration functionality.
Windows Server Update Services	Microsoft Windows Server Update Services (WSUS) allows you to distribute updates that are released through Microsoft Update to computers in your organization using centralized servers rather than individual updates.

Table 7-2 provides an overview of the primary features that you can deploy on a server running Windows Server 2008. Unlike earlier releases of Windows, some important server features are not installed automatically. For example, you must add Windows Server Backup to use the built-in backup and restore features of the operating system.

Table 7-2 Primary Features for Windows Server 2008

Feature	Description
.NET Framework 3.0	Provides .NET Framework 3.0 APIs for application development. Additional subfeatures include .NET Framework 3.0 Features, XPS Viewer, and Windows Communication Foundation (WCF) Activation Components.
BitLocker Drive Encryption	Provides hardware-based security to protect data through full-volume encryption that prevents disk tampering while the operating system is offline. Computers that have Trusted Platform Module (TPM) can use BitLocker Drive Encryption in Startup Key or TPM-only mode. Both modes provide early integrity validation.
Background Intelligent Transfer Service (BITS) Server Extensions	Provides intelligent background transfers. When this feature is installed, the server can act as a BITS server that can receive file uploads by clients. This feature isn't necessary for downloads to clients using BITS.
Connection Manager Administration Kit (CMAK)	Provides functionality for generating Connection Manager profiles.
Desktop Experience	Provides additional Windows Vista desktop functionality on the server. Windows Vista features added include Windows Media Player, desktop themes, and Windows Photo Gallery. Although these features allow a server to be used like a desktop computer, they can reduce the server's overall performance.
Failover Clustering	Provides clustering functionality that allows multiple servers to work together to provide high availability for services and applications. Many types of services can be clustered, including file and print services. Messaging and database servers are ideal candidates for clustering.
Group Policy Management	Installs the Group Policy Management Console (GPMC), which provides centralized administration of Group Policy.
Internet Printing Client	Provides functionality that allows clients to use HTTP to connect to printers on Web print servers.
Internet Storage Name Server (iSNS)	Provides management and server functions for Internet SCSI (iSCSI) devices, allowing the server to process registration requests, de-registration requests, and queries from iSCSI devices.
Line Printer Remote (LPR) Port Monitor	Installs the LPR Port Monitor, which allows printing to devices attached to UNIX-based computers.

Feature	Description
Message Queuing	Provides management and server functions for distributed message queuing. A group of related subfeatures is available as well.
Multipath I/O (MPIO)	Provides functionality necessary for using multiple data paths to a storage device.
Network Load Balancing (NLB)	NLB provides failover support and load balancing for IP-based applications and services by distributing incoming application requests among a group of participating servers. Web servers are ideal candidates for load balancing.
Peer Name Resolution Protocol (PNRP)	Provides Link-Local Multicast Name Resolution (LLMNR) functionality that allows peer-to-peer name-resolution services. When you install this feature, applications running on the server can register and resolve names using LLMNR.
Remote Assistance	Allows a remote user to connect to the server to provide or receive Remote Assistance.
Remote Server Administration Tools (RSAT)	Installs role- and feature-management tools that can be used for remote administration of other Windows Server 2008 systems. Options for individual tools are provided or you can install tools by top-level category or subcategory.
Removable Storage Manager (RSM)	Installs the Removable Storage Manager tool, which you can use to manage removable media and removable media devices.
Remote Procedure Call (RPC) over HTTP Proxy	Installs a proxy for relaying RPC messages from client applications over HTTP to the server. RPC over HTTP is an alternative to having clients access the server over a VPN connection.
Simple TCP/IP Services	Installs additional TCP/IP services, including Character Generator, Daytime, Discard, Echo, and Quote of the Day.
Simple Mail Transfer Protocol (SMTP) Server	SMTP is a network protocol for controlling the transfer and routing of e-mail messages. When this feature is installed, the server can act as a basic SMTP server. For a full-featured solution, you'll need to install a messaging server such as Microsoft Exchange Server 2007.
Simple Network Management Protocol (SNMP) Services	SNMP is a protocol used to simplify management of TCP/IP networks. You can use SNMP for centralized network management if your network has SNMP-compliant devices. You can also use SNMP for network monitoring via network management software.
Storage Manager For SANs	Installs the Storage Manager For SANs console. This console provides a central management interface for storage area network (SAN) devices. You can view storage subsystems, create and manage logical unit numbers (LUNs), and manage iSCSI target devices. The SAN device must support Visual Disk Services (VDS).

Feature	Description
Subsystem for UNIX-based Applications (SUA)	Provides functionality for running UNIX-based programs. You can download additional management utilities from the Microsoft Web site.
Windows Internal Database	Installs SQL Server 2005 Embedded Edition. This allows the server to use relational databases with Windows roles and features that require an internal database, such as AD RMS, UDDI Services, Windows Server Update Services (WSUS), Windows SharePoint Services, and Windows System Resource Manager.
Windows PowerShell	Installs Windows PowerShell, which provides an enhanced command-line environment for managing Windows systems.
Windows Process Activation Service	Provides support for distributed Web-based applications that use HTTP and non-HTTP protocols.
Windows Recovery Environment	You can use the recovery environment to restore a server using recovery options if you cannot access recovery options provided by the server manufacturer.
Windows Server Backup	Allows you to back up and restore the operating system, system state, and any data stored on a server.
Windows System Resource Manager (WSRM)	Allows you to manage resource usage on a per-processor basis.
WINS Server	WINS is a name-resolution service that resolves computer names to IP addresses. Installing this feature allows the computer to act as a WINS server.
Wireless Networking	Allows the server to use wireless networking connections and profiles.

Making Supplemental Components Available

Microsoft designed Server Manager and the underlying framework for managing components to be extensible. This makes it easier to provide supplemental roles, role services, and features for the operating system. Some additional components are available as downloads from the Microsoft Web site, including Windows Media Server 2008 and Windows SharePoint Server 2008.

You can make these components available for installation and configuration by completing the following steps:

1. Download the installer package or packages from the Microsoft Web site. Typically, these are provided as a set of Microsoft Update Standalone Packages (.msu) files.
2. Double-click each installer package to register it for use.

3. If Server Manager is running on the server, restart or refresh Server Manager to make the new components available.
4. In Server Manager, use the appropriate wizard to install and configure the supplemental role, role service, or feature.

Installing Components with Server Manager

Server Manager is the primary tool you'll use to manage roles, role services, and features. Not only can you use Server Manager to add or remove roles, role services, and features, but you can also use Server Manager to view the configuration details and status for these software components.

Viewing Configured Roles and Role Services

When you select Roles in the left pane, Server Manager lists roles you've installed. The main view of the Roles node displays a Roles Summary entry that lists the number and names of roles installed. In the case of error-related events for a particular server role, Server Manager displays a warning icon to the left of the role name.

In the Roles window, the name of a role is a clickable link that accesses the related role details, as shown in Figure 7-1. The role details provide the following information:

- Summary information about the status of related system services. If applicable, Server Manager lists the number of related services that are running or stopped, such as "System Services: 9 Running, 1 Stopped." You can manage a service by selecting it and then clicking Stop, Start, or Restart. In many cases, if a service isn't running as you think it should, you can click Restart to resolve the issue by stopping and then starting the service.
- Summary information about events the related services and components have generated in the last 24 hours, including details on whether any errors have occurred, such as "Events: 31 warning(s), 191 informational in the last 24 hours." If you select an event and then click View Properties, you can get detailed information about the event.
- Summary information about the role services installed, including the number of role services installed and the status (Installed or Not Installed) of each individual role service that you can use with the role.

You can refresh the details manually by selecting Refresh on the Action menu. If you want to set a different default refresh interval, click Configure Refresh at the bottom of the main pane, use the options provided to set a new refresh interval, and then click OK. Otherwise, Server Manager refreshes the details periodically for you.

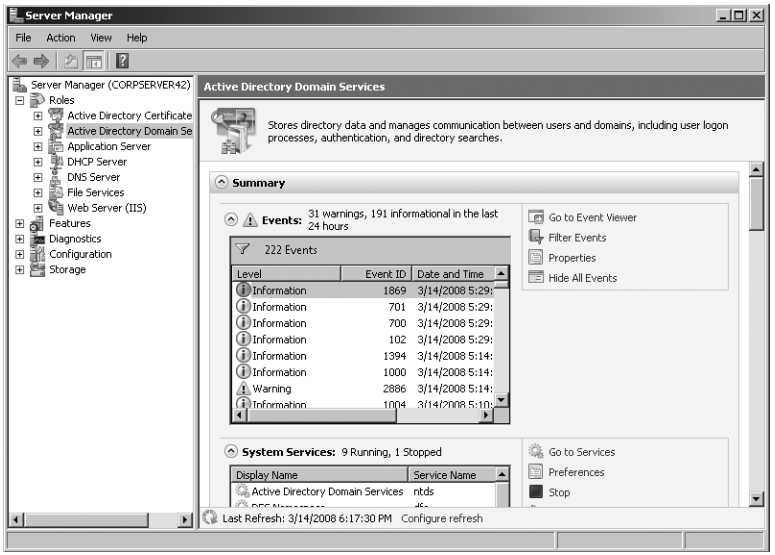


Figure 7-1 View the status details for installed roles.

Managing Server Roles

When you select Roles in Server Manager, the Roles Summary pane provides details on the current roles that you've installed. In the Roles Summary section, you'll find options for adding and removing roles. Keep in mind that some roles cannot be added at the same time as other roles, and you'll have to install each role separately. Other roles cannot be combined with existing roles, and you'll see warning prompts about this.

Adding a Server Role

You can add a server role by following these steps:

1. In Server Manager, select Roles in the left pane and then click Add Roles. This starts the Add Roles Wizard. If the wizard displays the Before You Begin page, read the introductory text and then click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before clicking Next.

2. On the Select Server Roles page, select the check box for the role or roles to install (see Figure 7-2).

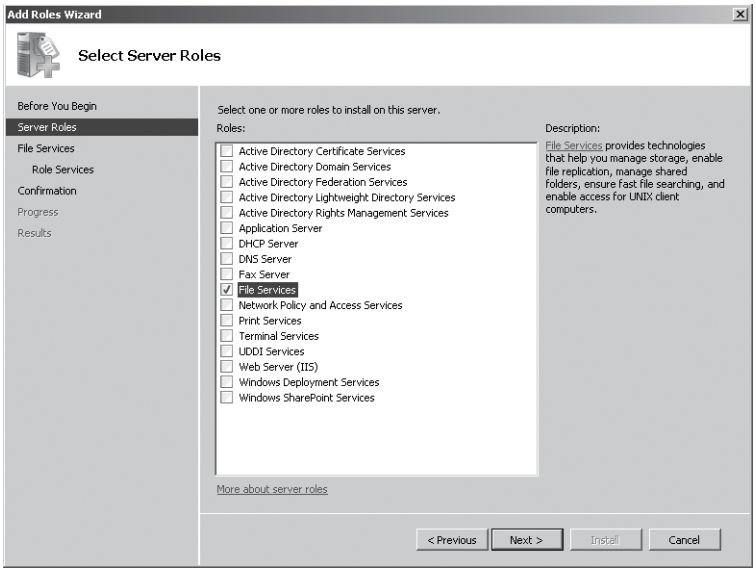


Figure 7-2 Select the roles to install.

> **Note**
>
> Adding the Active Directory Domain Services role does not configure the server as a domain controller. To configure the server as a domain controller, you must run Dcpromo.exe as discussed in Chapter 33, "Implementing Active Directory." Additionally, if you plan to have a domain controller also act as a DNS server, Microsoft recommends that you install the Active Directory Domain Services role and then use Dcpromo to configure the server as a DNS server and domain controller. A server running a core server installation can act as a domain controller and can also hold any of the Flexible Single Master Operations (FSMO) roles for Active Directory.

3. If additional features are required to install a role, as shown in Figure 7-3, you'll then see the Add Features Required For dialog box. Click Add Required Features to close the dialog box and add the required components to the server installation. Click Next twice to continue.

> **Note**
>
> Occasionally, you'll need to install additional role services to install a role or role service. The procedure is similar to installing additional features. If so, you'll see an Add Role Services Required For dialog box. Click Add Required Role Services to close the dialog box and add the required components to the server installation.

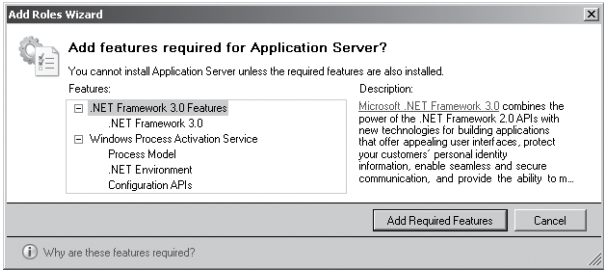


Figure 7-3 Confirm that required features can also be installed.

4. For each of the roles you are adding, you'll see a series of related pages that let you configure the associated role services as well as any other required configuration details. When selecting or clearing role services, keep the following in mind before you click Next to continue:
   - If you select a role service with additional required features or role services, you'll see a dialog box listing the additional required features or roles. After you review the required feature or roles, accept the additions and close the dialog box. If you click Cancel instead, the Add Roles Wizard will clear the role service you previously selected.
   - If you try to remove a role service that is required based on a previous role service, you'll see a warning prompt about dependent services that the Add Roles Wizard must also remove. In most cases, you'll want to click Cancel to preserve the previous selection. If you click the Remove Dependent Role Services button, the Add Roles Wizard will also remove the previously selected dependent services, which could cause the server to not function as expected.
5. On the Confirm Installation Selections page, click the Print, E-Mail, Or Save This Information link to generate an installation report and display it in Internet Explorer. You can then use standard Internet Explorer features to print or save the report. After you've reviewed the installation options and saved them as necessary, click Install to begin the installation process.

6. When the Add Roles Wizard finishes installing the server with the features you've selected, you'll see the Installation Results page. Review the installation details to ensure that all phases of the installation completed successfully. If any portion of the installation failed, note the reason for the failure and then use these troubleshooting techniques:
   a. Click the Print, E-Mail, Or Save The Installation Report link to create or update the installation report and display it in Internet Explorer.
   b. Scroll down to the bottom of the installation report in Internet Explorer and then click Full Log (Troubleshooting Only) to display the Server Manager log in Notepad.
   c. In Notepad, press Ctrl+F, enter the current date in the appropriate format for your language settings (such as 2009-08-30), and then click Find Next. Notepad will then move through the log to the first entry for the current date.
   d. Review the Server Manager entries for installation problems and take corrective actions as appropriate.

> **Note**
>
> In some cases, you might need to restart the server before installation or removal of a role, role service, or feature can be completed. In this case, you'll be prompted to restart the server when the Add Roles Wizard finishes. When you restart the server and log on, Server Manager will complete the installation or removal process.

Removing a Server Role

You can remove a server role by following these steps:

1. In Server Manager, select Roles in the left pane and then click Remove Roles. This starts the Remove Roles Wizard. If the wizard displays the Before You Begin page, read the introductory text and then click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before clicking Next.
2. On the Remove Server Roles page, the wizard selects the currently installed roles as shown in Figure 7-4. Clear the check box for the role you want to remove and then click Next.

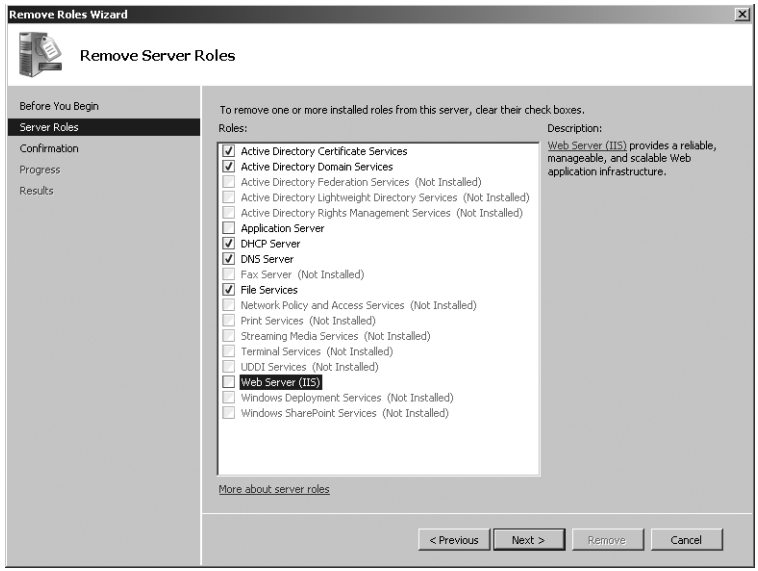


Figure 7-4 Clear selected roles to remove them.

3. If you try to remove a role that another role depends on, as shown in Figure 7-5, you'll see a warning prompt stating that you cannot remove the role unless you also remove the other role as well. If you click the Remove Dependent Role Services button, the Remove Roles Wizard will remove both roles.

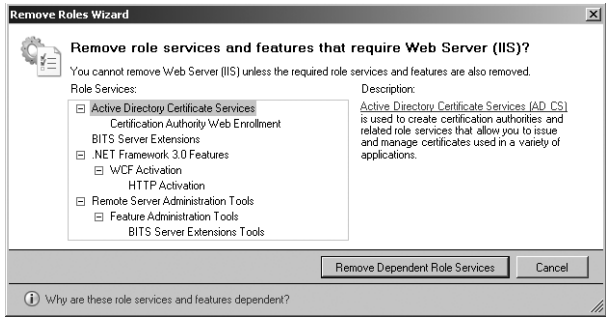


Figure 7-5 Confirm that dependent roles can also be removed.

4. On the Confirm Removal Selections page, review the related role services that the Remove Roles Wizard will remove based on your previous selections and then click Remove.

5. When the Remove Roles Wizard finishes modifying the server configuration, you'll see the Removal Results page. Review the modification details to ensure that all phases of the removal process completed successfully. If any portion of the removal process failed, note the reason for the failure and then use the previously discussed troubleshooting techniques to help resolve the problem.

Managing Role Services

In Server Manager, you can view the role services configured for a role by selecting Roles in the left pane and then scrolling down to the details section for the role that you want to work with. In the details section, you'll find a list of role services that you can install as well as their current Installed or Not Installed status. You can manage role services for servers by clicking Add Role Services or Remove Role Services for the related role details entry. Some roles, however, do not have individual role services that you can manage in this way. With these roles, you can modify the server role or remove the role only.

Adding a Role Service

You can add role services by following these steps:

1. In Server Manager, select Roles in the left pane and then scroll down until you see the details section for the role you want to manage. In the details section for the role, click Add Role Services. This starts the Add Role Services wizard.

2. On the Select Role Services page, the wizard dims the currently installed role services so that you cannot select the associated check box (see Figure 7-6). To add a role service, select its check box in the Role Services list. When you are finished selecting role services to add, click Next and then click Install.

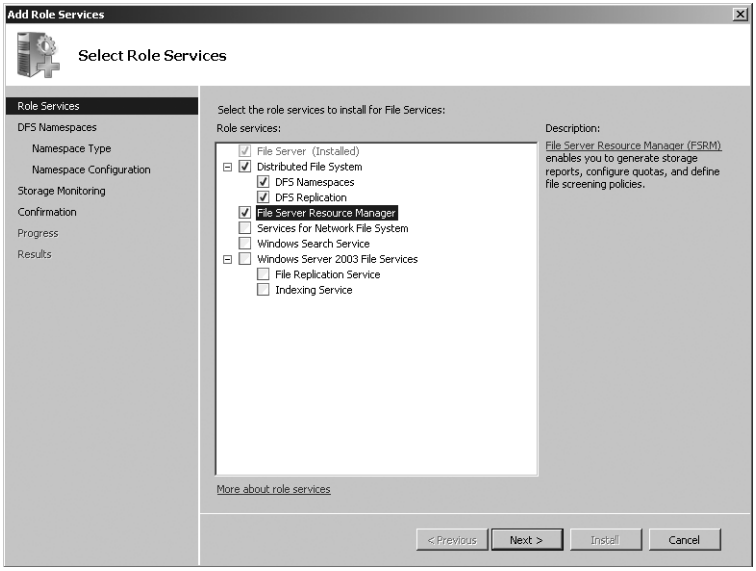


Figure 7-6 Select the role services to add.

Removing a Role Service

You can remove role services by following these steps:

1. In Server Manager, select Roles in the left pane and then scroll down until you see the details section for the role you want to manage. In the details section for the role, click Remove Role Services. This starts the Remove Role Services wizard.
2. On the Select Role Services page, the wizard selects the currently installed role services as shown in Figure 7-7. To remove a role service, clear the related check box. If you try to remove a role service that another role service depends on, you'll see a warning prompt stating that you cannot remove the role service unless you also remove the other role service as well. If you click the Remove Dependent Role Service button, the Remove Role Services wizard will remove both role services.
3. When you are finished selecting role services to remove, click Next and then click Remove.

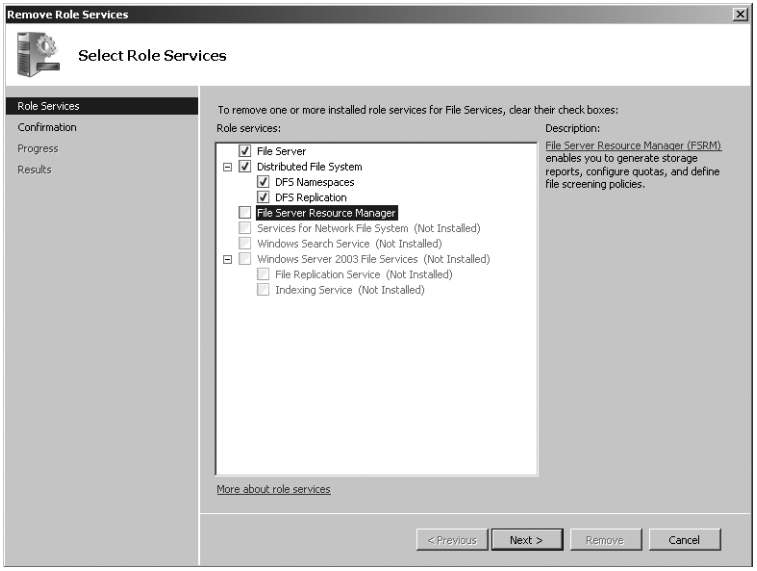


Figure 7-7 Clear selected role services to remove them.

Managing Windows Features

In earlier versions of Windows, you used the Add/Remove Windows Components option of the Add Or Remove Programs utility to add or remove operating system components. In Windows Server 2008, you configure operating system components as Windows features that you can turn on or off rather than add or remove.

Adding a Feature

You can add server features by following these steps:

1. In Server Manager, select Features in the left pane and then click Add Features. This starts the Add Features Wizard. If the wizard displays the Before You Begin page, read the introductory text and then click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before clicking Next.

2. On the Select Features page, select the check boxes for the feature or features to install as shown in Figure 7-8. If additional features are required to install a feature, you'll then see the Add Features Required For dialog box. Click Add Required Features to close the dialog box and add the required components to the server installation.

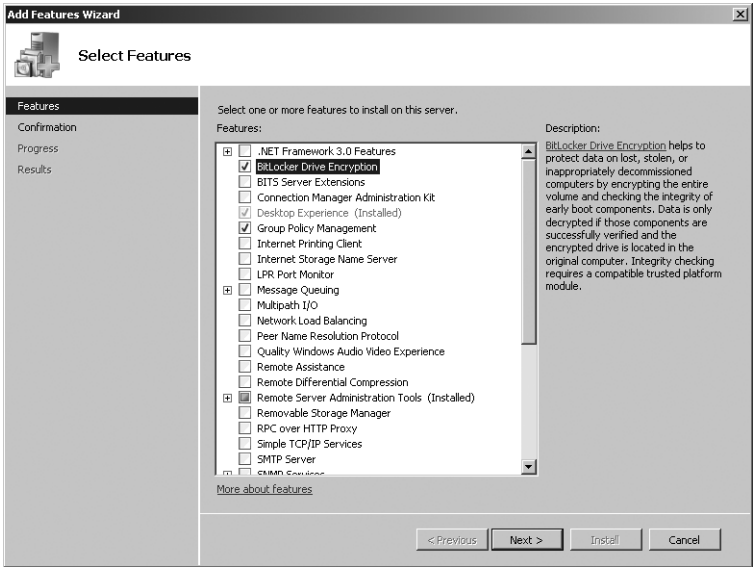


Figure 7-8 Select the features to add.

3. When you are finished selecting features to add, click Next and then click Install.

Removing a Feature

You can remove server features by following these steps:

1. In Server Manager, select Features in the left pane and then click Remove Features. This starts the Remove Features Wizard. If the wizard displays the Before You Begin page, read the introductory text and then click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before clicking Next.

2. On the Select Features page, the Remove Features Wizard selects the currently installed features as shown in Figure 7-9. To remove a feature, clear the related check box. If you try to remove a feature that another feature depends on, you'll see a warning prompt stating that you cannot remove the feature unless you also remove the other feature as well. If you click the Remove Dependent Feature button, the Remove Features Wizard will remove both features.

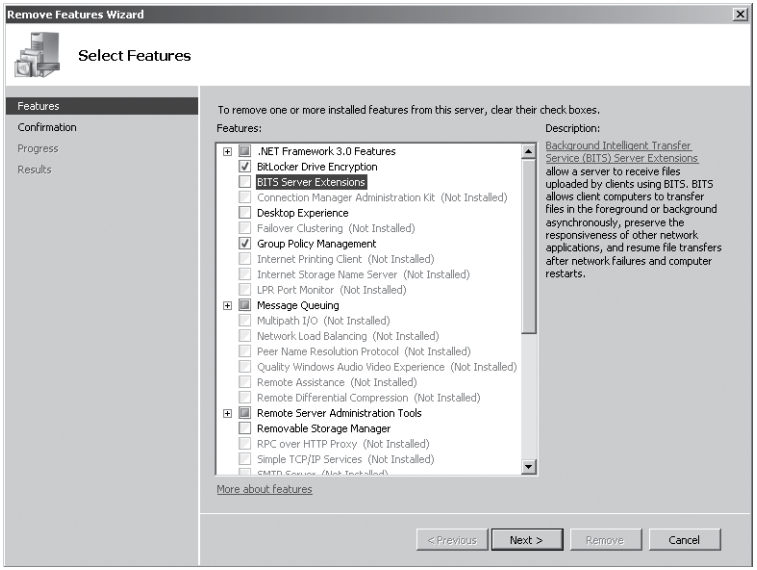


Figure 7-9 Clear the check boxes for selected features to remove them.

3. When you are finished selecting features to remove, click Next and then click Remove.

Installing Components at the Command Line

Server Manager's command-line counterpart is ServerManagerCmd.exe. When you work with ServerManagerCmd, you can:

- View the current configuration
- Add roles, role services, and features
- Remove roles, role services, and features

> **Note**
>
> You can't use ServerManagerCmd at the same time you are using one of Server Manager's add or remove wizards. Only one instance of either ServerManagerCmd or Server Manager can add or remove components at the same time.

Getting Started with ServerManagerCmd

You can manage roles, role services, and features using the following commands and command-line syntaxes:

- **-query** Obtains a detailed list of the server's current state with regard to roles, role services, and features. If *SaveFile.xml* is specified, the query results are displayed and saved to the named file, in XML format. Optionally, you can use -q instead of -query.

  ```
  ServerManagerCmd -query [SaveFile.xml] [-logPath LogFile.txt]
  ```

- **-install** Installs the named role, role service, or feature. The -allSubFeatures or -a parameter allows you to install all subordinate role services and features of the named component. The -setting or -s parameter allows you to configure required settings to specific values. Optionally, you can use -i instead of -install.

  ```
  ServerManagerCmd -install ComponentName [-setting SettingName=SettingValue]
  [-allSubFeatures] [-resultPath Results.xml] [-restart] | -whatIf]
  [-logPath LogFile.txt]
  ```

- **-inputPath** Adds or removes roles, role services, and features as specified in an XML answer file. Optionally, you can use -ip instead of -inputPath.

  ```
  ServerManagerCmd -inputPath AnswerFile.xml [-resultPath Results.xml] [-restart]
  | -whatIf] [-logPath LogFile.txt]
  ```

- **-remove** Removes the named role, role service, or feature. Optionally, you can use -r instead of -remove.

  ```
  ServerManagerCmd -remove ComponentName [-resultPath Results.xml]
  [-restart] | -whatIf] [-logPath LogFile.txt]
  ```

- **-version** Lists the version of the Server Manager command-line utility being used. Optionally, you can use -v instead of -version.

  ```
  ServerManagerCmd -version
  ```

Each of the commands accepts additional parameters and parameter values. Most commands and parameters have short forms that can be used instead of the full name. You can use the -logPath or -l parameter to log error details to a named log file. With the -install and -remove commands, you can use the -whatif or -w command to display the operations that would be performed if the command were executed. With the -install and -remove commands, you can use the -resultPath or -rp command to write standard output results to a named file in XML format. With the -install and -remove commands, you also can use the -restart command to restart the computer automatically (if restarting is necessary to complete the operation).

The parameter values that can be used with commands include:

- **AnswerFile.xml** Uses the XML-formatted answer file to determine what components to add or remove.

- **SaveFile.xml** Saves the standard output results to a named file in XML format. The results are still displayed and it is important to note that results do not include errors, which are written separately to standard error output.
- **ComponentName** Identifies the role, role service, or feature to work with.
- **SettingName** Identifies a required setting by its name.
- **SettingValue** Sets the configuration value for a setting.
- **LogFile** Sets the name of the text file to which log error details should be written.
- **Results.xml** Saves the results of the install or remove operation to a named file in XML format. Results are still displayed.

Table 7-3 provides a quick reference for the long and short form parameters for ServerManagerCmd.

Table 7-3 Long and Short Form Parameters for ServerManagerCmd

Operation	Parameter	Short Form
Change log path	-logPath	-l
Determine what if	-whatif	-w
Display version	-version	-v
Install component	-install	-i
Install from answer file	-inputPath	-ip
Query current state	-query	-q
Remove component	-remove	-r
Restart if necessary	-restart	
Saves the results	-resultPath	-rp
Specify required setting	-setting	-s

Understanding Component Names

Just about every installable role, role service, and feature has a component name. This name identifies the component so it can be manipulated from the command-line. Remember, supplemental components are made available by downloading and installing their installer packages from the Microsoft Web site.

Table 7-4 provides a hierarchical listing of the component names associated with roles, related role services, and related subcomponents. When you are installing a role, you can use the -allSubFeatures parameter to install all the subordinate role services and features listed under the role. When you are installing a role service, you can use the -allSubFeatures parameter to install all the subordinate features listed under the role service.

Table 7-4 Component Names for Key Roles and Role Services

Component Name	Role	Service	Feature
AD-Certificate	Active Directory Certificate Services		
ADCS-Cert-Authority		Certification Authority	
ADCS-Web-Enrollment		Certification Authority Web Enrollment	
ADCS-Online-Cert		Online Responder	
ADCS-Device-Enrollment		Network Device Enrollment Service	
	Active Directory Domain Services		
ADDS-Domain-Controller		Active Directory Domain Controller	
ADDS-Identity-Mgmt		Identity Management For UNIX	
ADDS-NIS			Server For Network Information Services
ADDS-NIS			Password Synchronization
ADDS-IDMU-Tools			Administration Tools
	Active Directory Federation Services		
ADFS-Federation		Federation Service	
ADFS-Proxy		Federation Service Proxy	
ADFS-Web-Agents		AD FS Web Agents	
ADFS-Claims			Claims-Aware Agent
ADFS-Windows-Token			Windows Token-Based Agent
ADLDS	Active Directory Lightweight Directory Services		
DHCP	DHCP Server		
DNS	DNS Server		
Fax	Fax Server		
	File Services		
FS-FileServer		File Server	
FS-DFS		Distributed File System	
FS-DFS-Namespace			DFS Namespaces
FS-DFS-Replication			DFS Replication
FS-Resource-Manager		File Server Resource Manager	
FS-NFS-Services		Services For Network File System	
FS-Search-Service		Windows Search Service	
FS-Win2003-Services		Windows Server 2003 File Services	
FS-Replication			File Replication Service

Component Name	Role	Service	Feature
FS-Indexing-Service			Indexing Service
NPAS	Network Policy And Access Services		
NPAS-Policy-Server		Network Policy Server	
NPAS-RRAS-Services		Routing And Remote Access Services	
NPAS-RRAS			Remote Access Service
NPAS-Routing			Routing
NPAS-Health		Health Registration Authority	
NPAS-Host-Cred		Host Credential Authorization Protocol	
Print-Services	Print Services		
Print-Server		Print Server	
Print-LPD-Service		LPD Service	
Print-Internet		Internet Printing	
Terminal-Services	Terminal Services		
TS-Terminal-Server		Terminal Server	
TS-Licensing		TS Licensing	
TS-Session-Broker		TS Session Broker	
TS-Gateway		TS Gateway	
TS-Web-Access		TS Web Access	
WDS	Windows Deployment Services		
WDS-Deployment		Deployment Server	
WDS-Transport		Transport Server	

Table 7-5 provides a hierarchical listing of the component names associated with features and related subfeatures. When you are installing a feature, you can use the -allSubFeatures parameter to install all the subordinate second-level and third-level features listed under the feature. When you are installing a second-level feature, you can use the -allSubFeatures parameter to install all the subordinate third-level features listed under the second-level feature.

Note

An asterisk following the feature command indicates the feature has unlisted subordinate features that generally are installed together by adding the -allSubFeatures parameter.

Table 7-5 Component Names for Features and Subfeatures

Component Name	Feature	Second-Level Feature	Third-Level Feature
NET-Framework*	.NET Framework 3.0 Features		
BitLocker	BitLocker Drive Encryption		
BITS	BITS Server Extensions		
CMAK	Connection Manager Administration Kit		
Desktop-Experience	Desktop Experience		
Failover-Clustering	Failover Clustering		
GPMC	Group Policy Management		
Internet-Print-Client	Internet Printing Client		
ISNS	Internet Storage Name Server		
LPR-Port-Monitor	LPR Port Monitor		
MSMQ*	Message Queuing		
Multipath-IO	Multipath I/O		
NLB	Network Load Balancing		
PNRP	Peer Name Resolution Protocol		
qWave	Quality Windows Audio Video Experience		
Remote-Assistance	Remote Assistance		
RDC	Remote Differential Compression		
RSAT	Remote Server Administration Tools		
RSAT-Role-Tools		Role Administration Tools	
RSAT-ADCS*			Active Directory Certificate Services Tools
RSAT-ADDS*			Active Directory Domain Services Tools
RSAT-ADLDS			Active Directory Lightweight Directory Services Tools
RSAT-RMS			Active Directory Rights Management Services Tools
RSAT-DHCP			DHCP Server Tools
RSAT-DNS-Server			DNS Server Tools
RSAT-Fax			Fax Server Tools
RSAT-File-Services*			File Services Tools
RSAT-NPAS*			Network Policy And Access Services Tools

Component Name	Feature	Second-Level Feature	Third-Level Feature
RSAT-Print-Services			Print Services Tools
RSAT-TS*			Terminal Services Tools
RSAT-UDDI			UDDI Services Tools
RSAT-Web-Server			Web Server (IIS) Tools
RSAT-WDS			Windows Deployment Services Tools
RSAT-Feature-Tools		Feature Administration Tools	
RSAT-BitLocker			BitLocker Drive Encryption Tools
RSAT-Bits-Server			BITS Server Extensions Tools
RSAT-Clustering			Failover Clustering Tools
RSAT-NLB			Network Load Balancing Tools
RSAT-SMTP			SMTP Server Tools
RSAT-WINS			WINS Server Tools
Removable-Storage	Removable Storage Manager		
RPC-over-HTTP-Proxy	RPC over HTTP Proxy		
Simple-TCPIP	Simple TCP/IP Services		
SMTP-Server	SMTP Server		
SNMP-Services	SNMP Services		
SNMP-Service		SNMP Service	
SNMP-WMI-Provider		SNMP WMI Provider	
Storage-Mgr-SANS	Storage Manager For SANs		
Subsystem-UNIX-Apps	Subsystem For UNIX-Based Applications		
Telnet-Client	Telnet Client		
Telnet-Server	Telnet Server		
TFTP-Client	TFTP Client		
Windows-Internal-DB	Windows Internal Database		
PowerShell	Windows PowerShell		
Backup-Features	Windows Server Backup Features		
Backup		Windows Server Backup	
Backup-Tools		Command-Line Tools	

Component Name	Feature	Second-Level Feature	Third-Level Feature
WSRM	Windows System Resource Manager		
WINS-Server	WINS Server		
Wireless-Networking	Wireless LAN Service		

Determining the Installed Roles, Role Services, and Features

You can determine the roles, roles services, and features that are installed on a server by typing **servermanagercmd -query** at an elevated command prompt. Each installed role, role service, and feature is highlighted and marked as such, and following the display name of each role, role service, and feature is the management naming component in brackets. In the output, roles and role services are listed before features as shown in the following example:

```
----- Roles -----
[X] Active Directory Certificate Services  [AD-Certificate]
    [X] Certification Authority  [ADCS-Cert-Authority]
    [X] Certification Authority Web Enrollment  [ADCS-Web-Enrollment]
    [ ] Online Responder  [ADCS-Online-Cert]
    [ ] Network Device Enrollment Service  [ADCS-Device-Enrollment]
[X] Active Directory Domain Services
    [X] Active Directory Domain Controller  [ADDS-Domain-Controller]
    [ ] Identity Management for UNIX  [ADDS-Identity-Mgmt]
        [ ] Server for Network Information Services  [ADDS-NIS]
        [ ] Password Synchronization  [ADDS-Password-Sync]
        [ ] Administration Tools  [ADDS-IDMU-Tools]

...

----- Features -----
[X] .NET Framework 3.0 Features  [NET-Framework]
    [X] .NET Framework 3.0  [NET-Framework-Core]
    [ ] XPS Viewer  [NET-XPS-Viewer]
    [X] WCF Activation  [NET-Win-CFAC]
        [X] HTTP Activation  [NET-HTTP-Activation]
        [X] Non-HTTP Activation  [NET-Non-HTTP-Activ]
[X] BitLocker Drive Encryption  [BitLocker]
[X] BITS Server Extensions  [BITS]
```

For the purposes of documenting a server's configuration, you can save the output in a file as standard text using the redirection symbol (>) as shown in this example:

```
servermanagercmd -query > MySavedResults.txt
```

Here, you save the output to a file named MySavedResults.txt. If you want to save the results as an XML-formatted file, simply follow the -query command with the name of the XML file, such as:

```
servermanagercmd -query MySaveFile.xml
```

Saving the output to an XML file makes the file easier to manipulate using automation techniques.

Installing Components Using ServerManagerCmd

You can install roles, role services, and features by typing **servermanagercmd -install *ComponentName*** at an elevated command prompt, where *ComponentName* is the name of the component to install as listed in Table 7-4 or Table 7-5. You can install subordinate components by including the -allSubFeatures parameter as shown in the following example:

```
servermanagercmd -install fs-dfs -allsubfeatures
```

Here, you install the Distributed File System role service as well as the subordinate DFS Namespaces and DFS Replication role services. The output for a successful installation should look similar to the following:

```
Start Installation...
[Installation] Succeeded: [File Services] Distributed File System.
[Installation] Succeeded: [File Services] DFS Namespaces.
[Installation] Succeeded: [File Services] DFS Replication.
<100/100>

Success: Installation succeeded.
```

Should a restart be required to complete an installation, you can have ServerManagerCmd restart the computer by including the -restart parameter. To test the installation prior to performing that actual operation, you can use the -whatif parameter. If you are trying to install components that are already installed you'll see a note stating that no changes were made, such as:

```
NoChange: No changes were made because the roles, role services and features specified
are already installed, or have already been removed from the local computer.
```

If an error occurs and ServerManagerCmd is not able to perform the operation specified, you'll see an error. Generally, error text is shown in red and includes an error flag and error text, such as:

```
WriteError: Failed to write the log file: . Access to the path 'C:\Windows\logs\
ServerManager.log' is denied.
```

This error indicates that ServerManagerCmd couldn't perform the operation because it couldn't gain write access to the log file. Other common errors you'll see are related to invalid arguments passed on the command line, such as:

```
ArgumentNotValid: Invalid parameters. Only specify either -install or -remove.
ArgumentNotValid: Invalid role, role service, or feature: 'fs-dfsd'. The name was not
found.
```

> **Note**
>
> If you forget to run the command prompt as an administrator, you'll see an error stating that Server Manager can be run only by a member of the built-in Administrators group on the local computer. You'll need to run the command prompt with elevated permissions to resolve this error.

When you install components, ServerManagerCmd writes extended logging information to %SystemRoot%\Logs\Servermanager.log. This logging information details every operation performed by ServerManagerCmd. You can write the detailed information to an alternate location by including the -logPath or -l parameter. In this example, you write the logging information to C:\Logs\Install.log:

```
servermanagercmd -install fs-dfs -allsubfeatures -logPath c:\logs\install.log
```

Removing Components Using ServerManagerCmd

You can uninstall roles, role services, and features by typing **servermanagercmd -remove *ComponentName*** at an elevated command prompt, where *ComponentName* is the name of the component to uninstall as listed in Table 7-4 or Table 7-5. You can uninstall subordinate components by including the -allSubFeatures parameter as shown in the following example:

```
servermanagercmd -remove fs-dfs -allsubfeatures
```

Here, you uninstall the Distributed File System role service as well as the subordinate DFS Namespaces and DFS Replication role services, and the output for a successful removal should look similar to the following:

```
Start Removal...
[Removal] Succeeded: [File Services] Distributed File System.
[Removal] Succeeded: [File Services] DFS Namespaces.
[Removal] Succeeded: [File Services] DFS Replication.
<100/100>

Success: Removal succeeded.
```

Should a restart be required to complete a removal, you can have ServerManagerCmd restart the computer by including the -restart parameter. As with installation, you can test the removal prior to performing that actual operation using the -whatif parameter. If you are trying to remove components that aren't installed, you'll see a note stating that no changes were made, such as:

```
NoChange: No changes were made because the roles, role services and features specified
are already installed, or have already been removed from the local computer.
```

If an error occurs and ServerManagerCmd is not able to perform the operation specified, you'll see an error. During the removal process, ServerManagerCmd writes extended logging information to %SystemRoot%\Logs\Servermanager.log. As with the installation process, you can write the detailed information to an alternate location by including the -logPath or -l parameter.

CHAPTER 21

Managing TCP/IP Networking

As an administrator, you enable networked computers to communicate by using the basic networking protocols built into Windows Server 2008. The key protocol you'll use is Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is actually a collection of protocols and services used for communicating over a network. It's the primary protocol used for internetwork communications. Compared to configuring other networking protocols, configuring TCP/IP communications is fairly complicated, but TCP/IP is the most versatile protocol available.

> **Note**
>
> Group Policy settings can affect your ability to install and manage TCP/IP networking. The key policies you'll want to examine are in User Configuration\Administrative Templates\Network\Network Connections and Computer Configuration\Administrative Templates\System\Group Policy. Group Policy is discussed in Chapter 36, "Managing Group Policy."

Installing TCP/IP Networking

If you want to install networking on a computer, you must install TCP/IP networking and a network adapter. Windows Server 2008 uses TCP/IP as the default wide area network (WAN) protocol. Normally, networking is installed during Windows Server 2008 setup. You can also install TCP/IP networking through local area connection properties. Although name resolution can be performed using DNS, WINS, or LLMNR, the preferred technique on Windows Server 2008 domains is DNS.

Preparing for Installation of TCP/IP Networking

Before you can configure TCP/IP networking on individual computers, you need the following information:

- **Domain name** The name of the domain in which the computer will be located. This can be a parent or a child domain.

- **IP address type, value, or both** The IP address information to assign to the computer, which can include both IPv4 and IPv6 addressing details.
- **Subnet mask** The subnet mask for the IPv4 network to which the computer is attached.
- **Subnet prefix length** The subnet prefix length for the IPv6 network to which the computer is attached.
- **Default gateway address** The address of the router or routers that will function as the computer's gateway.
- **DNS server address** The address of the DNS server or servers that provide DNS name resolution services on the network.
- **WINS server address** The address of the WINS server or servers that provide WINS name resolution services on the network.

If you are unsure of any of this information, you should ask the IT staff. In many cases, even if you are an administrator, there is a specific person you must ask for the IP address setup that should be used. Typically, this is your organization's network administrator and it is that person's job to maintain the spreadsheet or database that shows how IP addresses are assigned within the organization.

If no one in your organization has this role yet, this role should be assigned to someone or jointly managed to ensure that IP addresses are assigned following a specific plan. The plan should detail the following information:

- The address ranges that are reserved for network equipment and hardware and which individual IP addresses in this range are currently in use
- The address ranges that are reserved for DHCP and as such cannot be assigned using a static IP address
- The address ranges that are for static IP addresses and which individual IP addresses in this range are currently in use

Installing Network Adapters

Network adapters are hardware devices that are used to communicate on networks. You can install and configure network adapters by following these steps:

1. Configure the network adapter following the manufacturer's instructions. For example, you might need to use the software provided by the manufacturer to modify the Interrupt setting or the Port setting of the adapter.
2. If installing an internal network interface card, shut down the computer, unplug it, and install the adapter card in the appropriate slot on the computer. When you're finished, plug the computer in and start it.

3. Windows Server 2008 should detect the new adapter during startup. If you have a separate driver disc for the adapter, insert it now. Otherwise, you might be prompted to insert a driver disc.
4. If Windows Server 2008 doesn't detect the adapter automatically, follow the installation instructions in Chapter 8, "Managing and Troubleshooting Hardware."
5. If networking services aren't installed on the system, install them as described in the next section.

Installing Networking Services (TCP/IP)

If you're installing TCP/IP after installing Windows Server 2008, log on to the computer using an account with Administrator privileges and then follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections.
3. In Network Connections, right-click the connection you want to work with and then select Properties.
4. This displays the Local Area Connection Properties dialog box, shown in Figure 21-1.

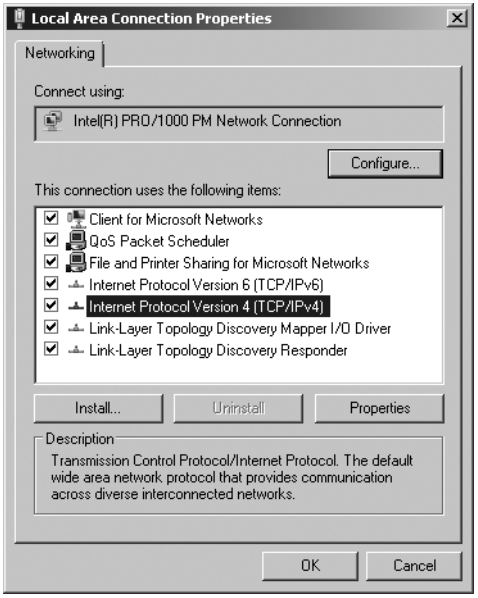


Figure 21-1 Install and configure TCP/IP in the Local Area Connection Properties dialog box.

5. If Internet Protocol Version 6 (TCP/IPv6), Internet Protocol Version 4 (TCP/IPv4), or both aren't shown in the list of installed components, you'll need to install them. Click Install. Select Protocol, and then click Add. In the Select Network Protocol dialog box, select the protocol to install and then click OK. If you are installing both TCP/IPv6 and TCP/IPv4, repeat this procedure for each protocol.
6. In the Local Area Connection Properties dialog box, make sure that the following are selected as appropriate: Internet Protocol Version 6 (TCP/IPv6), Internet Protocol Version 4 (TCP/IPv4), or both. Then click OK.
7. As necessary, follow the instructions in the next section for configuring local area connections for the computer.

Configuring TCP/IP Networking

A local area connection is created automatically if a computer has a network adapter and is connected to a network. If a computer has multiple network adapters and is connected to a network, you'll have one local area connection for each adapter. If no network connection is available, you should connect the computer to the network or create a different type of connection, as explained in "Managing Network Connections" on page 671.

Computers use IP addresses to communicate over TCP/IP. Windows Server 2008 provides the following ways to configure IP addressing:

Manually IP addresses that are assigned manually are called static IP addresses. Static IP addresses are fixed and don't change unless you change them. You'll usually assign static IP addresses to Windows servers, and when you do this, you'll need to configure additional information to help the server navigate the network.

Dynamically A DHCP server (if one is installed on the network) assigns dynamic IP addresses at startup, and the addresses might change over time. Dynamic IP addressing is the default configuration.

Alternatively (IPv4 only) When a computer is configured to use DHCPv4 and no DHCPv4 server is available, Windows Server 2008 assigns an alternate private IP address automatically. By default, the alternate IPv4 address is in the range from 169.254.0.1 to 169.254.255.254 with a subnet mask of 255.255.0.0. You can also specify a user-configured alternate IPv4 address, which is particularly useful for laptop users.

> **Note**
>
> Unless an IP address is specifically reserved, DHCP servers assign IP addresses for a specific period of time, known as an *IP address lease*. If this lease expires and cannot be renewed, then the client assigns itself an automatic private IP address.

> **Note**
>
> To perform most TCP/IP configuration tasks, you must be a member of the Administrators group.

Configuring Static IP Addresses

When you assign a static IP address, you need to tell the computer the IP address you want to use, the subnet mask for this IP address, and, if necessary, the default gateway to use for internetwork communications. An IP address is a numeric identifier for a computer. IP addressing schemes vary according to how your network is configured, but they're normally assigned based on a particular network segment.

IPv6 addresses and IPv4 addresses are very different. With IPv6, the first 64 bits represent the network ID and the remaining 64 bits represent the network interface. With IPv4, a variable number of the initial bits represent the network ID and the rest of the bits represent the host ID. For example, if you're working with IPv4 and a computer on the network segment 192.168.10.0 with a subnet mask of 255.255.255.0, the first 24 bits represent the network ID and the address range you have available for computer hosts is from 192.168.10.1 to 192.168.10.254. In this range, the address 192.168.10.255 is reserved for network broadcasts.

If you're on a private network that is indirectly connected to the Internet, you should use private IPv6 addresses. Link-local unicast addresses are private IPv6 addresses. All link-local unicast addresses begin with FE80.

If you're on a private network that is indirectly connected to the Internet, you should use private IPv4 addresses. Table 21-1 summarizes private network IPv4 addresses.

Table 21-1 Private IPv4 Network Addressing

Private Network ID	Subnet Mask	Network Address Range
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.255

All other IPv4 network addresses are public and must be leased or purchased. If the network is connected directly to the Internet and you've obtained a range of IPv4 addresses from your Internet service provider, you can use the IPv4 addresses you've been assigned.

Using the PING Command to Check an Address

Before you assign a static IP address, you should make sure that the address isn't already in use or reserved for use with DHCP. With the PING command, you can check to see whether an address is in use. Open a command prompt and type **ping**, followed by the IP address you want to check.

To test the IPv4 address 10.0.10.12, you would use the following command:

```
ping 10.0.10.12
```

To test the IPv6 address FEC0::02BC:FF:BECB:FE4F:961D, you would use the following command:

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

If you receive a successful reply from the PING test, the IP address is in use and you should try another one. If no current host on the network uses this IP address, the PING command output should be similar to the following:

```
Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

You can then use the IP address.

> **Note**
>
> Pinging an IP address will work as long as all the hosts are active and reachable on the network at the time you ping the address. However, a firewall could be blocking your PING request. More important is to plan the assignment of static addresses to machines on your network carefully.

Configuring a Static IPv4 or IPv6 Address

One local area network (LAN) connection is available for each network adapter installed. These connections are created automatically. To configure static IP addresses for a particular connection, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then select Properties.
3. Double-click Internet Protocol Version 6 (TCP/IPv6) or Internet Protocol Version 4 (TCP/IPv4) as appropriate for the type of IP address you are configuring.

4. For an IPv6 address, do the following:
   - Select Use The Following IPv6 Address and then type the IPv6 address in the IPv6 Address text box. The IPv6 address you assign to the computer must not be used anywhere else on the network.
   - Press the Tab key. The Subnet Prefix Length field ensures that the computer communicates over the network properly. Windows Server 2008 should insert a default value for the subnet prefix into the Subnet Prefix Length text box. If the network doesn't use variable-length subnetting, the default value should suffice. If your network does use variable-length subnets, you'll need to change this value as appropriate for your network.
5. For an IPv4 address, do the following:
   - Select Use The Following IP Address and then type the IPv4 address in the IP Address text box. The IPv4 address you assign to the computer must not be used anywhere else on the network.
   - Press the Tab key. The Subnet Mask field ensures that the computer communicates over the network properly. Windows Server 2008 should insert a default value for the subnet prefix into the Subnet Mask text box. If the network doesn't use variable-length subnetting, the default value should suffice. If your network does use variable-length subnets, you'll need to change this value as appropriate for your network.
6. If the computer needs to access other TCP/IP networks, the Internet, or other subnets, you must specify a default gateway. Type the IP address of the network's default router in the Default Gateway text box.
7. DNS is needed for domain name resolution. Select Use The Following DNS Server Addresses and then type a preferred address and an alternate DNS server address in the text boxes provided.
8. When you're finished, click OK three times to save your changes. Repeat this process for other network adapters and IP protocols you want to configure.
9. With IPv4 addressing, configure WINS as necessary, following the technique outlined in "Configuring WINS Resolution" on page 669.

Configuring Dynamic IP Addresses and Alternate IP Addressing

Many organizations use DHCP servers to dynamically assign IPv4 and IPv6 addresses. To receive an IPv4 or IPv6 address, client computers use a limited broadcast to advertise that they need to obtain an IP address. DHCP servers on the network acknowledge the request by offering the client an IP address. The client acknowledges the first offer it receives, and the DHCP server in turn tells the client that it has succeeded in leasing the IP address for a specified amount of time.

The message from the DHCP server can, and typically does, include the IP addresses of the default gateway, the preferred and alternate DNS servers, and the preferred and

alternate WINS servers. This means these settings wouldn't need to be manually configured on the client computer.

DHCP Is Primarily for Clients

Dynamic IP addresses aren't for all hosts on the network, however. Typically, you'll want to assign dynamic IP addresses to workstations and, in some instances, member servers that perform noncritical roles on the network. But if you use dynamic IP addressing for member servers, these servers should have reservations for their IP addresses. For any server that has a critical network role or provides a key service, you'll definitely want to use static IP addresses. Finally, with domain controllers and DHCP servers, you must use static IP addresses, so don't try to assign dynamic IP addresses to these servers.

Although you can use static IP addresses with workstations, most workstations use dynamic addressing, alternative IP addressing, or both. You configure dynamic and alternative addressing by following these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, one LAN connection is shown for each network adapter installed. These connections are created automatically. If you don't see a LAN connection for an installed adapter, check the driver for the adapter. It might be installed incorrectly. Right-click the connection you want to work with and then select Properties.
3. Double-click Internet Protocol Version 6 (TCP/IPv6) or Internet Protocol Version 4 (TCP/IPv4) as appropriate for the type of IP address you are configuring.
4. Select Obtain An IPv6 Address Automatically or Obtain An IP Address Automatically as appropriate for the type of IP address you are configuring. If desired, select Obtain DNS Server Address Automatically. Or select Use The Following DNS Server Addresses and then type a preferred and alternate DNS server address in the text boxes provided.
5. When you use dynamic IPv4 addressing with desktop computers, you should configure an automatic alternative address. To use this configuration, on the Alternate Configuration tab, select Automatic Private IP Address. Click OK, click Close, and then skip the remaining steps.
6. When you use dynamic IPv4 addressing with mobile computers, you'll usually want to configure the alternative address manually. To use this configuration, on the Alternate Configuration tab, select User Configured and then type the IP address you want to use in the IP Address text box. The IP address that you assign to the computer should be a private IP address, as shown in Table 20-1 on page 631, and it must not be in use anywhere else when the settings are applied.

7. With dynamic IPv4 addressing, complete the alternate configuration by entering a subnet mask, default gateway, DNS, and WINS settings. When you're finished, click OK twice.

INSIDE OUT **Disabling APIPA**

Whenever DHCP is used, APIPA is enabled by default. If you don't want a computer to use APIPA, you can either assign a static TCP/IP address or disable APIPA. For example, if your network uses routers or your network is connected to the Internet without a NAT or proxy server, you might not want to use APIPA. You can disable APIPA in the Registry.

On Windows 2000 or later, you can disable APIPA by creating the IPAutoconfiguration-Enabled as a DWORD value-entry under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*AdapterGUID*, where *AdapterGUID* is the globally unique identifier (GUID) for the computer's network adapter. Set the value to 0×0.

If you create the IPAutoconfigurationEnabled as a DWORD value-entry, you can enable APIPA at any time by changing the value to 0×1.

For more information about disabling APIPA, see Microsoft Knowledge Base article 220874.

Configuring Multiple IP Addresses and Gateways

Using advanced TCP/IP settings, you can configure a single network interface on a computer to use multiple IP addresses and multiple gateways. This allows a computer to appear to be several computers and to access multiple logical subnets to route information or to provide internetworking services.

To provide fault tolerance in case of a router outage, you can choose to configure Windows Server 2008 computers so that they use multiple default gateways. When you assign multiple gateways, Windows Server 2008 uses the gateway metric to determine which gateway is used and at what time. The gateway metric indicates the routing cost of using a gateway. The gateway with the lowest routing cost, or metric, is used first. If the computer can't communicate with this gateway, Windows Server 2008 tries to use the gateway with the next lowest metric.

The best way to configure multiple gateways depends on the configuration of your network. If your organization's computers use DHCP, you'll probably want to configure the additional gateways through settings on the DHCP server. If computers use static IP addresses or you want to set gateways specifically, assign them by following these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.

2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then select Properties.

3. Double-click Internet Protocol Version 6 (TCP/IPv6) or Internet Protocol Version 4 (TCP/IPv4) as appropriate for the type of IP address you are configuring.

4. Click Advanced to open the Advanced TCP/IP Settings dialog box. Figure 21-2 shows advanced settings for IPv4. The dialog box for IPv6 is similar.

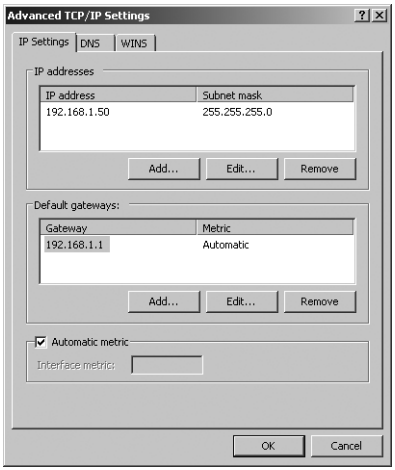


Figure 21-2 Configure multiple IP addresses and gateways in the Advanced TCP/IP Settings dialog box.

5. To add an IP address, click Add below IP Addresses to display the TCP/IP Address dialog box. After you type the IP address in the IP Address field, enter the subnet mask in the Subnet Mask field for IPv4 addresses or the subnet prefix length in the Subnet Prefix Length field for IPv6 addresses. Click Add to return to the Advanced TCP/IP Settings dialog box. Repeat this step for each IP address you want to add.

6. The Default Gateways panel shows the current gateways that have been manually configured (if any). To add a default gateway, click Add below Default Gateways to display the TCP/IP Gateway Address dialog box. Type the gateway address in the Gateway field. By default, Windows Server 2008 automatically assigns a metric to the gateway, which determines in which order the gateway is used. To assign the metric manually, clear the Automatic Metric check box, and then enter a metric in the field provided. Click Add, and then repeat this step for each gateway you want to add.

7. Click OK three times to close the open dialog boxes.

Configuring DNS Resolution

DNS is a host name resolution service that you can use to determine the IP address of a computer from its host name. This lets users work with host names, such as *http://www.msn.com* or *http://www.microsoft.com*, rather than an IP address, such as 192.168.5.102 or 192.168.12.68. DNS is the primary name service for Windows Server 2008 and the Internet.

As with gateways, the best way to configure DNS depends on the configuration of your network. If computers use DHCP, you'll probably want to configure DNS through settings on the DHCP server. If computers use static IP addresses or you want to configure DNS specifically for an individual user or system, you'll want to configure DNS manually.

Basic DNS Settings

You can configure basic DNS settings by following these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then select Properties.
3. Double-click Internet Protocol Version 6 (TCP/IPv6) or Internet Protocol Version 4 (TCP/IPv4) as appropriate for the type of IP address you are configuring.
4. If the computer is using DHCP and you want DHCP to specify the DNS server address, select Obtain DNS Server Address Automatically. Otherwise, select Use The Following DNS Server Addresses and then type primary and alternate DNS server addresses in the text boxes provided.
5. Click OK three times to save your changes.

Advanced DNS Settings

You configure advanced DNS settings on the DNS tab of the Advanced TCP/IP Settings dialog box, shown in Figure 21-3. You use the fields of the DNS tab as follows:

DNS Server Addresses, In Order Of Use Use this area to specify the IP address of each DNS server that is used for domain name resolution. Click Add if you want to add a server IP address to the list. Click Remove to remove a selected server address from the list. Click Edit to edit the selected entry. You can specify multiple servers for DNS resolution. Their priority is determined by the order. If the first server isn't available to respond to a host name resolution request, the next DNS server in the list is accessed, and so on. To change the position of a server in the list box, select it and then click the up or down arrow button.

Append Primary And Connection Specific DNS Suffixes Normally, this option is selected by default. Select this option to resolve unqualified computer names

in the primary domain. For example, if the computer name Gandolf is used and the parent domain is microsoft.com, the computer name would resolve to gandolf.microsoft.com. If the fully qualified computer name doesn't exist in the parent domain, the query fails. The parent domain used is the one set in the System Properties dialog box, on the Computer Name tab. (Click System And Maintenance\System in Control Panel, then click Change Settings and view the Computer Name tab to check the settings.)

Append Parent Suffixes Of The Primary DNS Suffix This option is selected by default. Select this check box to resolve unqualified computer names using the parent/child domain hierarchy. If a query fails in the immediate parent domain, the suffix for the parent of the parent domain is used to try to resolve the query. This process continues until the top of the DNS domain hierarchy is reached. For example, if the computer name Gandolf is used in the dev.microsoft.com domain, DNS would attempt to resolve the computer name to gandolf.dev.microsoft.com. If this didn't work, DNS would attempt to resolve the computer name to gandolf.microsoft.com.

Append These DNS Suffixes (In Order) Select this option to set specific DNS suffixes to use rather than resolving through the parent domain. Click Add if you want to add a domain suffix to the list. Click Remove to remove a selected domain suffix from the list. Click Edit to edit the selected entry. You can specify multiple domain suffixes, which are used in order. If the first suffix doesn't resolve properly, DNS attempts to use the next suffix in the list. If this fails, the next suffix is used, and so on. To change the order of the domain suffixes, select the suffix and then click the up or down arrow button to change its position.

DNS Suffix For This Connection This option sets a specific DNS suffix for the connection that overrides DNS names already configured for use on this connection. You'll usually set the DNS domain name through the System Properties dialog box, on the Computer Name tab.

Register This Connection's Addresses In DNS Select this check box if you want all IP addresses for this connection to be registered in DNS under the computer's fully qualified domain name. This option is selected by default.

> **Note**
>
> Dynamic DNS updates are used in conjunction with DHCP to enable a client to update its A (Host Address) record if its IP address changes, and to enable the DHCP server to update the PTR (Pointer) record for the client on the DNS server. You can also configure DHCP servers to update both the A and PTR records on the client's behalf. Dynamic DNS updates are supported only by BIND 5.1 or higher DNS servers as well as server editions of Microsoft Windows.

Use This Connection's DNS Suffix In DNS Registration Select this check box if you want all IP addresses for this connection to be registered in DNS under the parent domain.

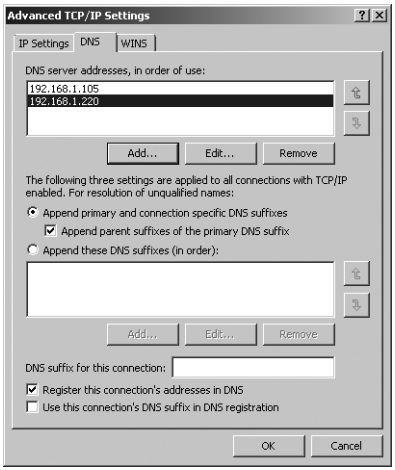


Figure 21-3 Configure advanced DNS settings on the DNS tab of the Advanced TCP/IP Settings dialog box.

Configuring WINS Resolution

You use WINS to resolve network basic input/output system (NetBIOS) computer names to IPv4 addresses. You can use WINS to help computers on a network determine the address of other computers on the network. If a WINS server is installed on the network, you can use the server to resolve computer names. Although WINS is supported on all versions of Windows, Windows Server 2008 primarily uses WINS for backward compatibility.

You can also configure Windows Server 2008 computers to use the local file LMHOSTS to resolve NetBIOS computer names. However, LMHOSTS is consulted only if normal name resolution methods fail. In a properly configured network, these files are rarely used. Thus, the preferred method of NetBIOS computer name resolution is WINS in conjunction with a WINS server.

As with gateways and DNS, the best way to configure WINS depends on the configuration of your network. If computers use DHCP, you'll probably want to configure WINS through settings on the DHCP server. If computers use static IPv4 addresses or you want to configure WINS specifically for an individual user or system, you'll want to configure WINS manually.

You can manually configure WINS by following these steps:

1. Access the Advanced TCP/IP Settings dialog box for IPv4 and click the WINS tab as shown in Figure 21-4. In the WINS Addresses, In Order Of Use panel, you can specify the IPv4 addresses of each WINS server that is used for NetBIOS name

resolution. Click Add if you want to add a server IPv4 address to the list. Click Remove to remove a selected server from the list. Click Edit to edit the selected entry.

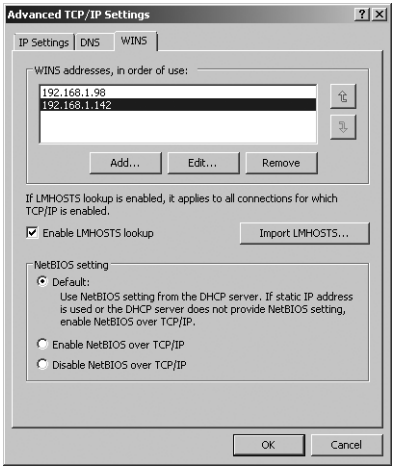


Figure 21-4 Configure WINS resolution for NetBIOS computer names on the WINS tab of the Advanced TCP/IP Settings dialog box.

2. You can specify multiple servers, which are used in order, for WINS resolution. If the first server isn't available to respond to a NetBIOS name resolution request, the next WINS server on the list is accessed, and so on. To change the position of a server in the list box, select it and then click the up or down arrow button.

3. To enable LMHOSTS lookups, select the Enable LMHOSTS Lookup check box. If you want the computer to use an existing LMHOSTS file defined somewhere on the network, retrieve this file by clicking Import LMHOSTS. You generally will use LMHOSTS only when other name resolution methods fail.

4. WINS name resolution requires NetBIOS over TCP/IP services. Select one of the following options to configure WINS name resolution using NetBIOS:
   - If you use DHCP and dynamic addressing, you can get the NetBIOS setting from the DHCP server. Select Default: Use NetBIOS Setting From The DHCP Server.
   - If you use a static IP address or the DHCP server does not provide NetBIOS settings, select Enable NetBIOS Over TCP/IP.
   - If WINS and NetBIOS are not used on the network, select Disable NetBIOS Over TCP/IP. This eliminates the NetBIOS broadcasts that would otherwise be sent by the computer.

5. Click OK three times. As necessary, repeat this process for other network adapters.

> **Note**
>
> LMHOSTS files are maintained locally on a computer-by-computer basis, which can eventually make them unreliable. Rather than relying on LMHOSTS, ensure that your DNS and WINS servers are configured properly and are accessible to the network for centralized administration of name resolution services.

Managing Network Connections

Local area connections make it possible for computers to access resources on the network and the Internet. One local area connection is created automatically for each network adapter installed on a computer. This section examines techniques you can use to manage these connections.

Checking the Status, Speed, and Activity for Local Area Connections

To check the status of a local area connection, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then click Status.
3. This displays the Local Area Connection Status dialog box. If the connection is disabled or the media is unplugged, you won't be able to access this dialog box. Enable the connection or connect the network cable to resolve the problem and then try to display the status dialog box again.

The General tab of this dialog box, shown in Figure 21-5, provides useful information regarding the following:

- **IPv4 Connectivity** The current IPv4 connection state and type. You'll typically see the status as Local when connected to an internal network or Not Connected when not connected to a network.
- **IPv6 Connectivity** The current IPv6 connection state and type. You'll typically see the status as Local when connected to an internal network or Not Connected when not connected to a network.
- **Media State** The state of the media. Because the status dialog box is available only when the connection is enabled, you'll typically see this as Enabled.

- **Duration** The amount of time the connection has been established. If the duration is fairly short, the user either recently connected to the network or the connection was recently reset.
- **Speed** The speed of the connection. This should read 10.0 megabits per second (Mbps) for 10-Mbps connections, 100.0 Mbps for 100-Mbps connections, and 1 gigabit per second (Gbps) for 1-gigabit connections. An incorrect setting can affect the computer's performance.
- **Bytes** The number of bytes sent and the number received by the connection. As the computer sends or receives packets, you'll see the computer icons light up to indicate the flow of traffic.

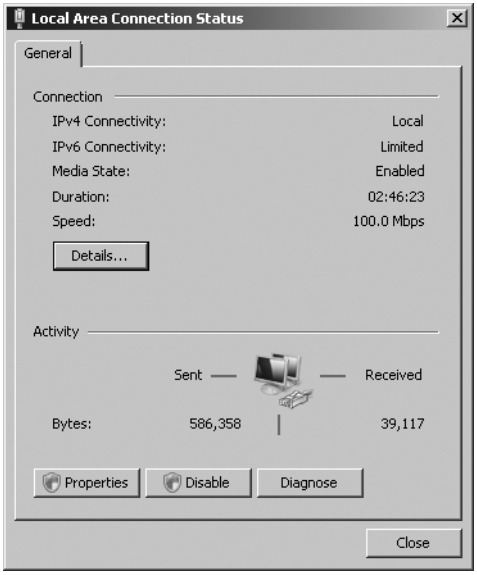


Figure 21-5 The General tab of the Local Area Connection Status dialog box provides access to summary information regarding connections, properties, and support.

Viewing Network Configuration Information

In Windows Server 2008, you can view the current configuration for network adapters in several ways. To view configuration settings using the Local Area Connection Status dialog box, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then click Status. This displays the Local Area Connection Status dialog box. If the connection is disabled or the media is unplugged, you won't be able to access this

dialog box. Enable the connection or connect the network cable to resolve the problem and then try to display the status dialog box again.

3. Click Details to view detailed information about the IP address configuration, including:
   - **Physical Address** The machine or Media Access Control (MAC) address of the network adapter. This address is unique for each network adapter.
   - **IPv4 IP Address** The IPv4 address assigned for IPv4 networking.
   - **IPv4 Subnet Mask** The subnet mask used for IPv4 networking.
   - **IPv4 Default Gateways** The IPv4 address of the default gateways used for IPv4 networking.
   - **IPv4 DNS Servers** IP addresses for DNS servers used with IPv4 networking.
   - **IPv4 WINS Servers** IP addresses for WINS servers used with IPv4 networking.
   - **IPv4 DHCP Server** The IP address of the DHCPv4 server from which the current lease was obtained (DHCPv4 only).
   - **Lease Obtained** A date and time stamp for when the DHCPv4 lease was obtained (DHCPv4 only).
   - **Lease Expires** A date and time stamp for when the DHCPv4 lease expires (DHCPv4 only).

You can also use the IPCONFIG command to view advanced configuration settings. To do so, follow these steps:

1. Click Start and type **cmd** in the Search field.
2. Press Enter.
3. At the command line, type **ipconfig /all** to see detailed configuration information for all network adapters configured on the computer.

> **Note**
>
> The command prompt is started in standard user mode. This is not an elevated command prompt.

Enabling and Disabling Local Area Connections

Local area connections are created and connected automatically. If you want to disable a connection so that it cannot be used, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.

2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection and select Disable to deactivate the connection and disable it.
3. If you want to enable the connection later, right-click the connection in Network Connections and select Enable.

If you want to disconnect from a network or start another connection, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection and select Disconnect. Typically, only remote access connections have a Disconnect option.
3. If you want to activate the connection later, right-click the connection in Network Connections and select Connect.

Renaming Local Area Connections

Windows Server 2008 initially assigns default names for local area connections. In Network Connections, you can rename the connections at any time by right-clicking the connection, selecting Rename, and then typing a new connection name. If a computer has multiple local area connections, proper naming can help you and others better understand the uses of a particular connection.

Troubleshooting and Testing Network Settings

Windows Server 2008 includes many tools for troubleshooting and testing TCP/IP connectivity. This section looks at automated diagnostics, basic tests that you should perform whenever you install or modify a computer's network settings, and techniques for resolving difficult networking problems involving DHCP and DNS. The final section shows you how to perform detailed network diagnostics testing.

Diagnosing and Resolving Local Area Connection Problems

Occasionally network cables can get unplugged or the network adapter might experience a problem that temporarily prevents it from working. After you plug the cable back in or solve the adapter problem, the connection should automatically reconnect. To diagnose local area connection problems, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.

2. In Network And Sharing Center, click Manage Network Connections.
3. Right-click the connection you want to work with and select Diagnose.

Windows Network Diagnostics will then try to identify the problem. A list of possible solutions is provided for identifiable configuration problems. Some solutions provide automated fixes that you can execute by clicking the solution. Other solutions require manual fixes, such as might be required if you need to reset a network router or broadband modem. If your actions don't fix the problem, refer to other appropriate parts of this troubleshooting section.

Diagnosing and Resolving Internet Connection Problems

Because of the many interdependencies between services, protocols, and configuration settings, troubleshooting network problems can be difficult. Fortunately, Windows Server 2008 includes a powerful network diagnostics tool for pinpointing problems that relate to the following:

- General network connectivity problems
- Internet service settings for e-mail, newsgroups, and proxies
- Settings for modems, network clients, and network adapters
- DNS, DHCP, and WINS configuration
- Default gateways and IP addresses

To diagnose Internet connection problems, follow these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. Click Diagnose And Repair.

Windows Network Diagnostics will then try to identify the problem. If identifiable configuration problems exist, a list of possible solutions is provided. Some solutions provide automated fixes that you can execute by clicking the solution. Other solutions require manual fixes, such as might be required if you need to reset a network router or broadband modem. If your actions don't fix the problem, refer to other appropriate parts of this troubleshooting section.

Performing Basic Network Tests

Whenever you install a new computer or make configuration changes to the computer's network settings, you should test the configuration. The most basic TCP/IP test is to use the PING command to test the computer's connection to the network. PING is a command-line command. To use it, type **ping <*host*>** at the command prompt, where <*host*> is either the computer name or the IP address of the host computer you're trying to reach.

With Windows Server 2008, you can use the following methods to test the configuration using PING:

- **Try to ping IP addresses** If the computer is configured correctly and the host you're trying to reach is accessible to the network, PING should receive a reply, as long as pinging is allowed by the computer's firewall. If PING can't reach the host or is blocked by a firewall, PING times out.
- **On domains that use WINS, try to ping NetBIOS computer names** If NetBIOS computer names are resolved correctly by PING, the NetBIOS facilities, such as WINS, are correctly configured for the computer.
- **On domains that use DNS, try to ping DNS host names** If fully qualified DNS host names are resolved correctly by PING, DNS name resolution is configured properly.

You might also want to test network browsing for the computer. If the computer is a member of a Windows Server 2008 domain and computer browsing is enabled throughout the domain, log on to the computer and then use Windows Explorer or Network Explorer to browse other computers in the domain. Afterward, log on to a different computer in the domain and try to browse the computer you just configured. These tests tell you if the DNS resolution is being handled properly in the local environment. If you can't browse, check the configuration of the DNS services and protocols.

In some cases, discovering and sharing might be set to block discovery. You'll need to allow discovery to resolve this by following these steps:

1. Click Start and then click Network.
2. In Network Explorer, click Network And Sharing Center on the toolbar.
3. If Network Discovery is set to Off, expand the Sharing And Discovery panel using the Expand button, click Turn On Network Discovery, and then click Apply to turn on this feature.

Diagnosing and Resolving IP Addressing Problems

The current IP address settings of a computer can be obtained as discussed in "Viewing Network Configuration Information" on page 672. If a computer is having problems accessing network resources or communicating with other computers, an IP addressing problem might exist. Take a close look at the IP address currently assigned, as well as other IP address settings, and use the following tips to help in your troubleshooting:

- If the IPv4 address currently assigned to the computer is in the range 169.254.0.1 to 169.254.255.254, the computer is using Automatic Private IP Addressing (APIPA). An automatic private IP address is assigned to a computer when it is configured to use DHCP and its DHCP client cannot reach a DHCP server. When using APIPA, Windows Server 2008 will automatically periodically check for

a DHCP server to become available. If a computer doesn't eventually obtain a dynamic IP address, the network connection usually has a problem. Check the network cable, and if necessary trace the cable back to the switch or hub into which it connects.

- If the IPv4 address and the subnet mask of the computer are currently set as 0.0.0.0, the network is either disconnected or someone attempted to use a static IP address that duplicated another IP address already in use on the network. In this case, you should access Network Connections and determine the state of the connection. If the connection is disabled or disconnected, this should be shown. Right-click the connection and select Enable or Diagnose as appropriate. If the connection is already enabled, you will need to modify the IP address settings for the connection.
- If the IP address is dynamically assigned, make sure that another computer on the network isn't using the same IP address. You can do this by disconnecting the network cable for the computer that you are working with and pinging the IP address in question. If you receive a response from the PING test, you know that another computer is using the IP address. This computer probably has an improper static IP address or a reservation that isn't set up properly.
- If the IP address appears to be set correctly, check the subnet mask, gateway, DNS, and WINS settings by comparing the network settings of the computer you are troubleshooting with those of a computer that is known to have a good network configuration. One of the biggest problem areas is the subnet mask. When subnetting is used, the subnet mask used in one area of the network might look very similar to that of another area of the network. For example, the subnet mask in one IPv4 area might be 255.255.255.240, and it might be 255.255.255.248 in another IPv4 area.

When you are using static IP addressing, you can check the current IPv4 or IPv6 settings by entering **ipconfig /all** at a command prompt. The display of the ipconfig /all command includes IPv4/IPv6 addresses, default routers, and DNS servers for all interfaces. You can also check IPv4 and IPv6 addressing separately. To check the IPv4 addressing configuration, enter **netsh interface ipv4 show address**s. To check IPv6 addressing, enter **netsh interface ipv6 show address**. To use Netsh to show the configuration of a remote computer use the **-r *RemoteComputerName*** command line option. For example, to display the configuration of the remote computer named CORPSERVER26, you would enter **netsh -r corpserver26 interface ipv4 show address**.

To make changes to the configuration of IP interfaces, use the **netsh interface ipv4 set interface** and **netsh interface ipv6 set interface** commands. To add the IP addresses of DNS servers, use the **netsh interface ipv4 add dns** and **netsh interface ipv6 add dns** commands.

Diagnosing and Resolving Routing Problems

As part of troubleshooting, you can verify the reachability of local and remote destinations. You can ping your default router by its IPv4 or IPv6 address. You can obtain the local IPv4 address of your default router by entering **netsh interface ipv4 show routes**. You can obtain the link-local IPv6 address of your default router by entering **netsh interface ipv6 show routes**. Pinging the default router tests whether you can reach local nodes and whether you can reach the default router, which forwards IP packets to remote nodes.

When you ping the default IPv6 router, you must specify the zone identifier (ID) for the interface on which you want the ICMPv6 Echo Request messages to be sent. The zone ID for the default router is listed when you enter the ipconfig /all command.

If you are able to ping your default router, ping a remote destination by its IPv4 or IPv6 address. If you are unable to ping a remote destination by its IP address, there might be a routing problem between your node and the destination node. Enter **tracert -d *IPAddress*** to trace the routing path to the remote destination You use the -d command-line option to speed up the response by preventing Tracert from performing a reverse DNS query on every near-side router interface in the routing path.

The inability to reach a local or remote destination might be due to incorrect or missing routes in the local IP routing table. To view the local IP routing table, enter the **netsh interface ipv4 show routes** or **netsh interface ipv6 show routes** command. Use the command output to verify that you have a route corresponding to your local subnet. The route with the lowest metric is used first. If you have multiple default routes with the same lowest metric, you might need to modify your IP router configuration so that the default route with the lowest metric uses the interface that connects to the correct network.

You can add a route to the IP routing table by using the **netsh interface ipv4 add route** or **netsh interface ipv6 add route** command. To modify an existing route, use the **netsh interface ipv4 set route** or the **netsh interface ipv6 set route** command. To remove an existing route, use the **netsh interface ipv4 delete route** or **netsh interface ipv6 delete route** command.

If you suspect a problem with router performance, use the **pathping -d *IPAddress*** command to trace the path to a destination and display information on packet losses for each router in the path. You use the -d command-line option to speed up the response by preventing Pathping from performing a reverse DNS query on every near-side router interface in the routing path.

INSIDE OUT

Checking IPSec policies and Windows Firewall

The problem with reaching a destination node might be due to the configuration of Internet Protocol Security (IPSec) or packet filtering. Check for IPSec policies that have been configured on the computer having the problem, on intermediate IPv6 routers, and on the destination computer. On computers running Windows XP or later, IPSec is configured using Windows Firewall With Advanced Security.

In many cases, packet filtering is configured to allow specific types of traffic and discard all others, or to discard specific types of traffic and accept all others. Because of this, you might be able to view Web pages on a Web server, but not ping the Web server by its host name or IP address.

Each network connection configured on a computer can be enabled or disabled in the Windows Firewall. When enabled, IPv4 and IPv6 drop incoming requests. During troublehshooting, you can disable the Windows Firewall for a specific IPv4 or IPv6 interface with the **netsh interface ipv4 set interface interface=NameOrIndex firewall=disabled** and **netsh interface ipv6 set interface interface=NameOrIndex firewall=disabled** commands. You can also completely turn off the Windows Firewall with the **netsh firewall set opmode disable** command. Don't forget to reenable the firewall when you are done troubleshooting.

Releasing and Renewing DHCP Settings

DHCP servers can assign many network configuration settings automatically, including IP addresses, default gateways, primary and secondary DNS servers, primary and secondary WINS servers, and more. When computers use dynamic addressing, they are assigned a lease on a specific IP address. This lease is good for a specific time period and must be renewed periodically. When the lease needs to be renewed, the computer contacts the DHCP server that provided the lease. If the server is available, the lease is renewed and a new lease period is granted. You can also renew leases manually as necessary on individual computers or by using the DHCP server itself.

Problems that prevent network communications can occur during the lease assignment and renewal process. If the server isn't available and cannot be reached before a lease expires, the IP address can become invalid. If this happens, the computer might use the alternate IP address configuration to set an alternate address, which in most cases has settings that are inappropriate and prevent proper communications. To resolve this problem, you'll need to release and then renew the DHCP lease.

Another type of problem occurs when users move around to various offices and subnets within the organization. While moving from location to location, their computers might obtain DHCP settings from the wrong server. When the users return to their offices, the computer might seem sluggish or perform incorrectly because of the settings assigned by the DHCP server at another location. If this happens, you'll need to release and then renew the DHCP lease.

You can use the graphical interface to release and renew DHCP leases by following these steps:

1. Click Start and then click Network. In Network Explorer, click Network And Sharing Center on the toolbar.
2. In Network And Sharing Center, click Manage Network Connections. In Network Connections, right-click the connection you want to work with and then select Diagnose.
3. After Windows Network Diagnostics tries to identify the problem, a list of possible solutions is provided. If the computer has one or more dynamically assigned IP addresses, one of the solutions should be Automatically Get New IP Settings.... Click this option.

You can also follow these steps to use the IPCONFIG command to renew and release settings:

1. Start an elevated command prompt.
2. To release the current settings for all network adapters, type **ipconfig /release** at the command line. Then renew the lease by typing **ipconfig /renew**.
3. To renew a DHCP lease for all network adapters, type **ipconfig /renew** at the command line.
4. You can check the updated settings by typing **ipconfig /all** at the command line.

> **Note**
>
> If a computer has multiple network adapters and you only want to work with one or a subset of the adapters, specify all or part of the connection name after the **ipconfig /renew** or **ipconfig /release** command. Use the asterisk as a wildcard to match any characters in a connection's name. For example, if you want to renew the lease for all connections with names starting with *Loc*, type the command **ipconfig /renew Loc***. If you want to release the settings for all connections containing the word *Network*, type the command **ipconfig /release *Network***.

Diagnosing and Resolving Name Resolution Issues

When you can reach a destination using an IP address but not reach a host using a host name, you might have a problem with host name resolution. Typically, name resolution issues have to do with improper configuration of the DNS client or problems with DNS registration. You can use the following tasks to troubleshoot problems with DNS name resolution:

- Verify DNS configuration

- Test DNS name resolution with the Ping tool
- Use the Nslookup tool to view DNS server responses
- Display and flush the DNS client resolver cache

On the computer having DNS name resolution problems, verify the following information:

- Host name
- The primary DNS suffix
- DNS suffix search list
- Connection-specific DNS suffixes
- DNS servers

You can obtain this information by entering **ipconfig /all** at a command prompt. To obtain information about which DNS names should be registered in DNS, enter **netsh interface ip show dns**.

Computers running Windows Vista and Windows Server 2008 support DNS traffic over IPv6. By default, IPv6 configures the well-known site-local addresses of DNS servers at FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2, and FEC0:0:0:FFFF::3. To add the IPv6 addresses of your DNS servers, use the properties of the Internet Protocol Version 6 (TCP/IPv6) component in Network Connections or **the netsh interface ipv6 add dns** command. To register the appropriate DNS names as IP address resource records with DNS dynamic update, use the **ipconfig /registerdns** command. Computers running Windows XP or Windows Server 2003 do not support DNS traffic over IPv6.

TCP/IP checks the DNS client resolver cache before sending DNS name queries. The DNS resolver cache maintains a history of DNS lookups that have been performed when a user accesses network resources using TCP/IP. This cache contains forward lookups, which provide host name to IP address resolution, and reverse lookups, which provide IP address to host name resolution. After a DNS entry is stored in the resolver cache for a particular DNS host, the local computer no longer has to query external servers for DNS information on that host. This enables the computer to resolve DNS requests locally, providing a quicker response.

How long entries are stored in the resolver cache depends on the Time to Live (TTL) value assigned to the record by the originating server. To view current records and see the remaining TTL value for each record, type **ipconfig /displaydns** in an elevated command prompt. These values are given as the number of seconds that a particular record can remain in the cache before it expires. These values are continually being counted down by the local computer. When the TTL value reaches zero, the record expires and is removed from the resolver cache.

Occasionally, you'll find that you need to clear out the resolver cache to remove old entries and enable computers to check for updated DNS entries before the normal expiration and purging process takes place. Typically, this happens because server IP

addresses have changed and the current entries in the resolver cache point to the old addresses rather than the new ones. Sometimes the resolver cache itself can get out of sync, particularly when DHCP has been misconfigured.

> **Note**
>
> Skilled administrators know that several weeks in advance of the actual change, they should start to decrease the TTL values for DNS records that are going to be changed. Typically, this means reducing the TTL from a number of days (or weeks) to a number of hours, which allows for quicker propagation of the changes to computers that have cached the related DNS records. After the change is completed, administrators should restore the original TTL value to reduce renewal requests.

In most cases, you can resolve problems with the DNS resolver cache by either flushing the cache or reregistering DNS. When you flush the resolver cache, all DNS entries are cleared out of the cache and new entries are not created until the next time the computer performs a DNS lookup on a particular host or IP address. When you reregister DNS, Windows Server 2008 attempts to refresh all current DHCP leases and then performs a lookup on each DNS entry in the resolver cache. By looking up each host or IP address again, the entries are renewed and reregistered in the resolver cache. You'll generally want to flush the cache completely and allow the computer to perform lookups as needed. Reregister DNS only when you suspect problems with DHCP and the DNS resolver cache.

You can test DNS name resolution by pinging a destination using its host name or fully qualified domain name (FQDN). If an incorrect IP address is shown, you can flush the DNS resolver cache and use the Nslookup tool to determine the set of addresses returned in the DNS Name Query Response message.

You can use the IPCONFIG command to flush and reregister entries in the DNS resolver cache by following these steps:

1. Start an elevated command prompt.
2. To clear out the resolver cache, type **ipconfig /flushdns** at the command line.
3. To renew DHCP leases and reregister DNS entries, type **ipconfig /registerdns** at the command line.
4. When the tasks are complete, you can check your work by typing **ipconfig /displaydns** at the command line.

To start Nslookup, enter **Nslookup** at a command prompt. At the Nslookup > prompt, use the **set d2** command to get detail information about DNS response messages. Then, use Nslookup to look up the desired FQDN. Look for A and AAAA records in the detailed display of the DNS response messages.

With IPv6, the DNS client maintains a neighbor's cache of recently resolved link-layer addresses as well as a standard resolver cache. To display the current contents of the neighbor cache, enter **netsh interface ipv6 show neighbors**. To flush the neighbor's cache, enter **netsh interface ipv6 delete neighbors**.

For IPv6, the DNS client also maintains a destination cache. The destination cache stores next-hop IPv6 addresses for destinations. To display the current contents of the destination cache, enter **netsh interface ipv6 show destinationcache** command. To flush the destination cache, enter **netsh interface ipv6 delete destinationcache**.

Index

B

C

D

F

H

L

M

N

P

S

T

U

V

W

Z