

Step-by-Step Guide for DNS in Small Networks

Microsoft Corporation Published: January 2008 Author: Jim Groves Editor: Jim Becker

Abstract

This guide helps you implement Domain Name System (DNS) on the Windows Server® 2008 operating system in a small network. Windows Server 2008 uses DNS to translate computer names to network addresses. An Active Directory® domain controller can act as a DNS server that registers the names and addresses of computers in the domain and then provides the network address of a member computer when the domain controller receives a query with the name of the computer. This guide explains how to set up DNS on a simple network that consists of a single domain.



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

© 2008 Microsoft Corporation. All rights reserved.

Active Directory, SharePoint, Windows, Windows Server, Windows Vista, the Windows logo, and the Microsoft logo are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Step-by-Step Guide for DNS in Small Networks	5
Planning DNS	6
Understanding the DNS namespace	6
Designing a DNS namespace	8
Creating an Internet DNS domain name	9
Creating internal DNS domain names	9
Creating DNS computer names	9
Installing and Configuring AD DS and DNS	. 11
Configuring Client Settings	. 19
Advanced DNS Configuration	. 27
Adding resource records	. 28
Automatically removing outdated resource records	. 29
Troubleshooting DNS	. 31

Step-by-Step Guide for DNS in Small Networks

Domain Name System (DNS) is a system for naming computers and network services that maps those names to network addresses and organizes them into a hierarchy of domains. DNS naming is used on TCP/IP networks, such as the Internet and most corporate networks, to locate computers and services by using user-friendly names. When a user enters the DNS name of a computer in an application, DNS can look up the name and provide other information that is associated with the computer, such as its IP address or services that it provides for the network. This process is called name resolution.

Name systems, such as DNS, make it easier to use network resources by providing users with a way to refer to a computer or service by a name that is easy to remember. DNS looks up that name and provides the numeric address that operating systems and applications require to identify the computer on a network. For example, users enter www.microsoft.com instead of the numeric IP address of the server to identify a Microsoft Web server on the Internet. The name is resolved when the DNS client software on the user's computer sends a request to a DNS server that the user's computer is configured to use. If the DNS server has been configured to respond authoritatively with the address of the requested host, it replies to the request directly. Otherwise, the DNS server passes the request on to another server that can provide the address or a referral to another DNS server that can help provide the address. This is where the name hierarchy comes into play: If a DNS server does not know which server is configured with the address, it can request the server that is responsible for maintaining addresses of servers at each level in the hierarchy until it locates the authoritative server. For example, if the DNS server does not know which server is responsible for the server named www.microsoft.com, the DNS server can ask the server that is responsible for supplying the names of DNS servers in the .com domain to provide the address of the server that is responsible for providing the addresses of DNS servers in the microsoft.com domain. The original DNS server can then query that server for the address of the computer named www.microsoft.com.

DNS requires little ongoing maintenance for small businesses, which typically have one to four DNS servers. (Medium-size organizations usually have 4 to 14 DNS servers.) DNS problems, however, can affect server availability for your entire network. Most DNS problems occur because DNS settings are configured incorrectly or obsolete records remain on the DNS servers. By following the procedures in this guide, you can avoid such problems when you deploy DNS in a simple network that is based on the Windows Server® 2008 operating system.

This guide explains how to install and configure a basic DNS implementation in a network that consists of a single, new Active Directory® Domain Services (AD DS) domain. The guide then addresses some advanced issues that medium-size organizations may have to consider. Finally, it includes some basic DNS troubleshooting steps that you can take if you suspect that your environment has problems with DNS.

In this guide

- Planning DNS
- Installing and Configuring AD DS and DNS
- <u>Configuring Client Settings</u>
- Advanced DNS Configuration
- <u>Troubleshooting DNS</u>

Planning DNS

Domain Name System (DNS) is the primary method for name resolution in Windows Server® 2008 and for other versions of Microsoft® Windows® operating systems, such as Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. DNS is a requirement for deploying the Active Directory Domain Services (AD DS) server role. Integrating DNS with AD DS makes it possible for DNS servers to take advantage of the security, performance, and fault-tolerance capabilities of AD DS.

Typically, you organize your DNS namespace (that is, the association of domains, subdomains, and hosts) in a way that supports your plan for using AD DS to organize the computers on your network.

Understanding the DNS namespace

The following illustration shows how the DNS namespace is organized.



A DNS name consists of two or more parts separated by periods, or "dots" (.). The last (rightmost) part of the name is called the top-level domain (TLD). Other parts of the name are subdomains of the TLD or another subdomain. The names of the TLDs are either functional or geographical. Subdomains usually refer to the organization that owns the domain name.

Functional TLDs suggest the purpose of the organization that has registered a subdomain in the TLD. The following table shows some of the most common functional TLD names.

Functional TLD	Typically used by
.com	Commercial entities, such as corporations, to register DNS domain names
.edu	Educational institutions, such as colleges, and public and private schools
.gov	Government entities, such as federal, state, and local governments
.net	Organizations that provide Internet services, such as Internet service providers (ISPs)

Functional TLD	Typically used by
.org	Private, nonprofit organizations

Geographical TLDs indicate the country or region where the organization that registered the domain is located. For example, an organization that wants to show that it is located in Canada registers its Internet domain name in the .ca TLD, and an organization that wants to show that it is located in Brazil registers its Internet domain name in the .br TLD.

Most organizations that want to have an Internet presence for a Web site or that want to send and receive e-mail messages, for example, register an Internet domain name that is a subdomain of a TLD. Usually, they choose a subdomain name based on their organization's name, such as contoso.com or treyresearch.net. Most small organizations work with their Internet service provider (ISP) to register their domain name, although you can also register your domain name directly with a registrar that is listed at InterNIC (http://www.internic.com/regist.html).

Registering an Internet domain name reserves the name for the exclusive use of the organization and configures DNS servers on the Internet to provide the appropriate IP address when those servers are queried for that name. That is, it creates the equivalent of a telephone directory entry for the Internet domain name. But instead of providing a telephone number for the name, it provides the IP address that a computer requires to access the computers in the registered domain.

The DNS namespace is not limited to only the publicly registered Internet domain names. Organizations that have networks with their own DNS servers can create domains for their internal use. As the next section explains, these internal DNS namespaces can be—but are not required to be—subdomains of a public Internet domain name.

Designing a DNS namespace

You can design an external namespace that is visible to Internet users and computers. You can also design an internal namespace that is visible only to users and computers that are in your internal network.

Organizations that require an Internet presence and an internal namespace must deploy both an internal and an external DNS namespace and manage each namespace separately. In this case, we recommend that you make your internal domain a subdomain of your external domain. For example, an organization that has an external domain name of contoso.com might use the internal domain name corp.contoso.com. Using an internal domain that is a subdomain of an external domain has the following advantages:

- Requires you to register only one name with an Internet name authority even if you later decide to make part of your internal namespace publicly accessible.
- Ensures that all of your internal domain names are globally unique.
- Simplifies administration by enabling you to administer internal and external domains separately.

Allows you to use a firewall between the internal and external domains to secure your DNS deployment.

If you want to deploy an AD DS domain for each division in your organization, you can use your internal domain as a parent for additional child domains that you create to manage those divisions. Child domain names are immediately subordinate to the domain name of the parent. For example, a child domain for a manufacturing division that you add to the us.corp.contoso.com namespace might have the domain name manu.us.corp.contoso.com.

Creating an Internet DNS domain name

An Internet DNS domain name has a TLD name, such as .com, .org, or .edu, and a unique subdomain name that the domain owner chooses. For example, a company named Contoso Corporation would probably choose contoso.com as its Internet domain name.

Before you register an Internet DNS domain, conduct a preliminary search of the Internet to confirm that the DNS domain name that you want to use is not already registered to another organization. If the domain name that you want to use is available, contact your Internet service provider (ISP) to confirm that the domain name is available and to help you register your domain name. Your ISP might set up a DNS server on its own network to host the DNS zone for your domain name or it might help you set up a DNS server on your network for this purpose.

Creating internal DNS domain names

For your internal domains, create names that are related to your registered Internet DNS domain name. For example, if you register the Internet DNS domain name contoso.com for your organization, use a DNS domain name such as corp.contoso.com for the internal, fully qualified DNS domain name and use CORP as the NetBIOS name.

If you want to deploy DNS in a private network, but you do not plan to create an external namespace, you should still register the DNS domain name that you create for your internal domain. If you do not register the name, and you later attempt to use it on the Internet or you use it to connect to a network that is connected to the Internet, the name might be unavailable.

Creating DNS computer names

When you create DNS names for the computers on your network, develop and follow a logical DNS computer-naming convention. This makes it possible for users to remember easily the names of computers on public and private networks, which facilitates access to network resources.

Use the following guidelines when you create DNS names:

- Select computer names that are easy for users to remember.
- Identify the owner of a computer in the computer name.

For example, andrew-dixon indicates that Andrew Dixon uses the computer, and pubs-server indicates that the computer is a server that belongs to the Publications department.

• As an alternative, select names that describe the purpose of the computer.

For example, a file server named past-accounts-1 indicates that the file server stores information related to past accounts.

- Do not use capitalization to convey the owner or purpose of a computer.
 DNS is not case sensitive.
- Match the AD DS domain name to the primary DNS suffix of the computer name.
 The primary DNS suffix is the part of the DNS name that appears after the host name.
- Use unique names for all computers in your organization.

Do not assign the same computer name to different computers in different DNS domains. For example, do not use such names as server1.acct.contoso.com and server1.hr.contoso.com. Also, do not use the same computer name when a computer is configured to run different operating systems. For example, if a computer can run Windows Server 2008 or Windows Vista, do not use the same computer name for both operating systems.

• Use ASCII characters to ensure interoperability with computers running versions of Windows earlier than Windows 2000.

For computer and domain names, use only the characters A through Z, 0 through 9, and the hyphen (-). Do not use the hyphen as the first character in a name.

In particular, the following characters are not allowed in DNS names:

- comma (,)
- tilde (~)
- colon (:)
- exclamation point (!)
- at sign (@)
- number sign (#)
- dollar sign (\$)
- percent sign (%)
- caret (^)
- ampersand (&)
- apostrophe (')
- period (.), except as a separator between names
- parentheses (())
- braces ({})
- underscore (_)
- The number of characters in a name must be between 2 and 24.
- Avoid nonstandard TLDs such as .local. Using a nonstandard TLD will prevent you from being able to register your domain name on the Internet.

Installing and Configuring AD DS and DNS

When you create a new Active Directory Domain Services (AD DS) domain, the Active Directory Domain Services Installation Wizard installs the Domain Name System (DNS) server role by default. This ensures that DNS and AD DS are configured properly for integration with each other.

Important

Before you install AD DS and DNS on the first domain controller server in a new domain, ensure that the IP address of the server is static; that is, that it is not assigned by Dynamic Host Configuration Protocol (DHCP). DNS servers and Active Directory domain controllers must have static addresses to ensure that clients can locate the servers reliably.

To install DNS with AD DS in a new domain

- 1. Click Start, point to Administrative tools, and then click Server Manager.
- 2. In the tree pane, click **Roles**.
- 3. In the results pane, click Add Roles.

🏪 Server Manager			
<u>File Action View H</u> elp			
Server Manager (CONTOSO-SVR1)	Dolec		
Roles Roles Diagnostics Diagnostics Storage	View the health of the roles installed on your server and add or remove roles and features.		
	Roles Summary	Roles Summary Help	
	Roles: 0 of 17 installed	Add Roles	
× >	Conf	gure refresh	

4. On the Before You Begin page, click Next.

Add Roles Wizard	X
Before You Begin	
Before You Begin Server Roles Confirmation Progress Results	This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site. Defore you continue, verify that: The Administrator account has a strong password Network settings, such as static IP addresses, are configured The tast security updates from Windows Update are installed If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again. To continue, click Next. If you page by default
	< Previous Next > Instali Cancel

5. On the Select Server Roles page, click **Active Directory Domain Services**, and then click **Next**.

Add Roles Wizard		X
Select Server Ro	les	
Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Pederation Services Active Directory Rederation Services Active Directory Rights Management Services Application Server DHCP Server DHS Server Print Services Quoties Print Services DDI Services UDDI Services Windows Deployment Services Windows SharePoint Services Windows SharePoint Services Windows SharePoint Services Windows SharePoint Services	Description: Active Directory Domain Services (AD) D5) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process. t Install Cancel

- 6. On the Active Directory Domain Services page, read the information and then click Next.
- 7. On the **Confirm Installation Selections** page, read the information and then click **Install**.
- 8. After AD DS installation has completed, on the **Installation Results** page, click **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).**

Add Roles Wizard	X
Installation Resu	lts
Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results	The following roles, role services, or features were installed successfully: Informational message below Active Directory Domain Services Installation succeeded The following role services were installed: Active Directory Domain Controller Image: Ima
	Print, e-mail, or save the installation report
	< Previous Next > Close Cancel

- 9. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
- 10. On the **Choose a Deployment Configuration** page, click **Create a new domain in a new forest**, and then click **Next**.

hoose a You c	a Deployment Configuration an create a domain controller for an existing forest or for a new forest.	
ОB	isting forest	
	○ Add a domain controller to an existing domain	
	C Create a new domain in an existing forest This server will become the first domain controller in the new domain.	
۰Ö	eate a new <u>d</u> omain in a new forest	
More	about possible deployment configurations	

11. On the **Name the Forest Root Domain** page, type the full DNS name (such as corp.contoso.com) for the new domain, and then click **Next**.

Active Directory Domain Services Installation Wizard	×
Name the Forest Root Domain The first domain in the forest is the forest root domain. Its name is also the name of the forest.	
Type the fully qualified domain name (FQDN) of the new forest root domain.	
EQDN of the forest root domain:	
corp.contoso.com	
Example: corp.contoso.com	
< <u>B</u> ack <u>N</u> ext > Car	icel

- 12. On the Set Forest Functional Level page, select Windows Server 2008, and then click Next.
- 13. On the **Additional Domain Controller Options** page, make sure that **DNS server** is selected, and then click **Next**.

ditional Domain Controller Options	ation wizard		
Select additional options for this domain con	troller.		
DNS server			
🔽 Global catalog			
<u><u>Read-only domain controller (RODC)</u></u>			
Additional information:			
The first domain controller in a forest must cannot be an RODC.	be a global catalo	g server and	<u> </u>
The first domain controller in a forest must cannot be an RODC. We recommend that you install the DNS S controller.	be a global catalo Server service on th	g server and he first domain	A
The first domain controller in a forest must cannot be an RODC. We recommend that you install the DNS S controller. More about <u>additional domain controller op</u>	be a global catalo Gerver service on th <u>itions</u>	g server and he first domain	<u> </u>

📝 Note

A message box informs you that a delegation for this DNS server cannot be created. This is normal and expected for the first domain controller in a new forest. Click **Yes** to proceed.

Active	Directory Domain Services Installation Wizard	×
	A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain corp.contoso.com. Otherwise, no action is required. Do you want to continue?	
	<u>Y</u> es <u>N</u> o	

14. On the Location for Database, Log Files, and SYSVOL page, type the location in which you want to install the database, log, and system volume (SYSVOL) folders, or click Browse to choose a location, and then click Next.

📝 Note

You can safely accept the default locations unless you know that you have a reason to change them.

Active Directory Domain Services Installation Wizard	×
Location for Database. Log Files, and SYSVOL Specify the folders that will contain the Active Directory domain controlle database, log files, and SYSVOL.	er 📕
For better performance and recoverability, store the database and log fil volumes.	es on separate
Database folder:	
C:\Windows\NTDS	B <u>r</u> owse
Log files folder:	
C:\Windows\NTDS	Br <u>o</u> wse
SYSVOL folder:	
C:\Windows\SYSVOL	Bro <u>w</u> se
More about placing Active Directory Domain Services files	
< <u>B</u> ack <u>N</u> ext >	Cancel

15. On the **Directory Services Restore Mode Administrator Password** page, type a password to use to log on to the server in Directory Services Restore Mode, confirm the password, and then click **Next**.

arctive Directory Domain Services Installation Wizard			
Directory Services Restore Mode Administrator Password			
The Directory Services Restore Mode Administrator account is different from the domain Administrator account.			
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.			
Password:			
Confirm password:			
More about Directory Services Restore Mode password			
< <u>B</u> ack <u>N</u> ext > Cancel			

- 16. Review the **Summary** page, and then click **Next** to begin the installation.
- 17. After the AD DS installation completes, click **OK** to restart the computer.

Configuring Client Settings

By default, Domain Name System (DNS) clients are configured to allow Dynamic Host Configuration Protocol (DHCP) to automatically assign the clients' IP addresses, DNS server addresses, and other settings. The TCP/IP configuration steps in this section are required only if a DHCP server is not available.

Configure the following settings for each DNS client:

- TCP/IP settings for DNS
- Host name and domain membership

The following procedures require you to log on with an account that belongs to the Administrators group on the client computer.

To configure client settings on a computer running Windows XP

- 1. On the computer that you want to configure to use DNS, click **Start**, point to **Control Panel**, and then click **Network Connections**.
- 2. Right-click the network connection that you want to configure, and then click **Properties**.
- 3. On the General tab, click Internet Protocol (TCP/IP), and then click Properties.

🚣 Local Area Connection Properties	? ×		
General Authentication Advanced			
Connect using:			
B 3Com 3C905TX-based Ethernet Ada	ure		
This connection uses the following items:			
Client for Microsoft Networks			
🗆 🔲 Network Load Balancing			
🗹 📮 File and Printer Sharing for Microsoft Networks			
Internet Protocol (TCP/IP)			
Install Uninstall Proper	ties		
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.			
Show icon in notification area when connected			
Notify me when this connection has limited or no connection	ctivity		
OK	Cancel		

- 4. Click Use the following IP address.
- 5. In **IP address**, type the address of the client computer.
- 6. In **Subnet mask**, type the subnet mask of the domain controller.
- 7. In **Default gateway**, type the address of the default gateway of the domain controller.
- 8. Click Use the following DNS server addresses.
- 9. In **Preferred DNS server**, type the IP address of the DNS server that you installed in Installing and Configuring AD DS and DNS.



Do not use the IP address of a DNS server that is provided by your Internet service provider (ISP) as a primary or alternate DNS server.

- 10. Click OK, and then click Close.
 - Note

It is not necessary to restart the computer at this time if you intend to change the computer's name or domain membership in the following steps.

- 11. In Control Panel, double-click System.
- 12. On the Computer Name tab, click Change.
- 13. In **Computer name**, type the name of the computer (the host name).
- 14. Click **Domain**, and then type the name of the domain that you want the computer to join.

Computer Name Changes	<u>?</u> ×
You can change the name and the membership of this computer. Changes may affect access to network resourc	ces.
<u>C</u> omputer name:	
pubs-server	
Full computer name: pubs-server.wingroup.windeploy.ntdev.microsoft.com	
<u>M</u> ore	
Member of	
• Domain:	_
corp.contoso.com	
© <u>W</u> orkgroup:	
OK Cano	;el

- 15. If a second **Computer Name Changes** dialog box appears, in **User Name**, type the domain name and user name of an account that has permission to join computers to the domain.
- 16. In **Password**, type the password of the account.

Separate the domain name and user name with a backslash, for example, *domain\user_name*.

Computer Name Cha	anges 🥂 🗙
	G
Enter the name and p to join the domain.	password of an account with permission
<u>U</u> ser name:	🔮 corp.contoso.com\admin 💌 🗾
Password:	•••••
	OK Cancel

17. Click **OK** to close all dialog boxes.

To configure client settings on a computer running Windows Vista

- 1. On the computer that you want to configure to use DNS, click **Start**, and then click **Control Panel**.
- 2. In Control Panel, click Network and Internet.
- 3. Click Network and Sharing Center. In the Tasks pane, click Manage network connections.

🚱 🔵 🗢 👱 « Network and Inte	rnet Network and Sharing Center	er 👻 😽 Search	م
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> ools <u>H</u> elp			
Tasks View computers and devices	Network and Sharing Ce	enter	2
Connect to a network		_	View full map
Manage wireless networks			🍋
Set up a connection or network	NEWCOMPLITE	R default	Internet
Manage network connections	(This computer)	internet
Diagnose and repair	💐 default (Private network)		Customize
	Access	Local and Internet	
	Connection	Local Area Connection	View status
	Sharing and Discovery		
	Network discovery	o On	$\overline{\mathbf{v}}$
	File sharing	On On	$\overline{\mathbf{v}}$
	Public folder sharing	◎ Off	$\overline{\mathbf{v}}$
See also	Printer sharing	◎ Off	\odot
Bluetooth Devices	Password protected sharing	On	\odot
Infrared	Media sharing	⊖ Off	\odot
Internet Options Windows Firewall Windows Mobile Device Center	Show me all the files and folde Show me all the shared netwo	rs I am sharing k folders on this computer	

- 4. Right-click the network connection that you want to configure, and then click **Properties**.
- 5. On the **Networking** tab, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

📮 Local Area Connection Properties	x		
Networking Sharing			
Connect using:			
Intel(R) PRO/1000 PL Network Connection			
<u>C</u> onfigure			
This connection uses the following items:			
Client for Microsoft Networks	۱۱		
🗹 📕 QoS Packet Scheduler			
File and Printer Sharing for Microsoft Networks			
Internet Protocol Version 6 (TCP/IPv6)			
Internet Protocol Version 4 (TCP/IPv4)			
Link-Layer Topology Discovery Mapper I/O Driver			
Link-Layer Topology Discovery Responder			
Install Uninstall Properties			
Description	ъL		
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.			
OK Cancel			

- 6. Click Use the following IP address.
- 7. In **IP address**, type the address of the client computer.
- 8. In Subnet mask, type the subnet mask of the domain controller.
- 9. In **Default gateway**, type the address of the default gateway of the domain controller.
- Click Use the following DNS server addresses, and in Preferred DNS server, type the IP address of the domain controller that you installed in <u>Installing and Configuring AD DS</u> and DNS.

🚸 Important

Do not use the IP address of a DNS server that is provided by your ISP as a primary or alternate DNS server.

- 11. Click OK to exit.
- 12. If **Internet Protocol Version 6 (TCP/IPv6)** is selected, click it, and then click **Properties**. Perform the same steps as for TCP/IPv4, and then click **OK** and **Close**.

📝 Note

It is not necessary to restart the computer at this time if you intend to change the computer's name or domain membership in the following steps.

13. In Control Panel, click System and Maintenance, and then click System.



14. Under Computer name, domain, and workgroup settings, click Change settings.



- 15. On the Computer Name tab, click Change.
- 16. In **Computer name**, type the name of the computer (the host name).

Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources. <u>More information</u>
Computer name:
pubs-server
Full computer name: pubs-server More
<u>Domain:</u>
corp.contoso.com
© <u>W</u> orkgroup: WORKGROUP
OK Cancel

- 17. Click **Domain**, and then type the name of the domain that you created in <u>Installing and</u> <u>Configuring AD DS and DNS</u>.
- 18. If the Computer Name Changes dialog box appears:
 - In **User Name**, type the domain name and user name of an account that has permission to join computers to the domain.
 - In **Password**, type the password of the account. Separate the domain name and user name with a backslash, for example, *domain\user_name*.
- 19. Click **OK** to close all dialog boxes.

Advanced DNS Configuration

In most cases, deploying Active Directory Domain Services (AD DS)–integrated Domain Name System (DNS) on a small, Windows-based network requires little configuration beyond the initial setup. Occasionally, however, you may have to perform additional configuration tasks, such as adding resource records to handle unusual situations or configuring automatic removal of outdated resource records.

Adding resource records

Resource records store information about specific network computers, such as the names, IP addresses, and services that the computers provide. In most cases, Windows-based computers use dynamic update to update their resource records on DNS servers. This dynamic update process eliminates the need for an administrator to manage the resource records. However, if your network contains computers that are not Windows-based or if it contains computers that you want to designate to handle e-mail, you may have to add host (A) resource records to the zone on your DNS server.

😍 Important

When the Active Directory Domain Services Installation Wizard installs and configures DNS on the new domain controller, it creates resource records that are necessary for the correct operation of the DNS server on the domain controller. Do not remove or change these resource records. Change or remove only those resource records that you add yourself.

Host (A) resource records associate the DNS domain name of a computer (or host) to its IP address. You do not need to have a host (A) resource record for all computers, but you must have one for any computer that shares resources on a network and that must be identified by its DNS domain name.

- Windows 2000, Windows XP, and Windows Server 2003 clients and servers use the Dynamic Host Configuration Protocol (DHCP) Client service to dynamically register and update their host (A) resource records in DNS when an IP configuration change occurs.
- Windows Vista and Windows Server 2008 clients use the DNS Client service to dynamically
 register and update their host (A) resource records in DNS when an IP configuration change
 occurs.
- You can manually create a host (A) resource record for a static TCP/IP client computer (or for a computer running non-Windows operating systems) by using the DNS Manager administrative tool.

To add a host (A) resource record to a DNS zone

- 1. On the DNS server, click Start, point to Administrative Tools, and then click DNS.
- 2. In the console tree, right-click the applicable DNS zone, and then click New Host (A).
- 3. In **Name (uses parent domain if blank)**, type the name of the computer (host) for which you are creating a host (A) resource record.
- 4. In **IP address**, type the address of the computer for which you want to create a host (A) resource record.

🕀 Important

Make sure that you type the address correctly and that you assign it as a static address (not one that is assigned by DHCP). If the address is incorrect or changes, client computers cannot use DNS to locate the host.

Automatically removing outdated resource records

The ability of DHCP to register host (A) and pointer (PTR) resource records automatically whenever you add a new device to the network simplifies network administration. However, it has one drawback: unless you remove those resource records, they remain in the DNS zone database indefinitely. Although this is not a problem with static networks, it negatively affects networks that change frequently (for example, a network to which you add or remove portable computers) because the accumulation of resource records can prevent host names from being reused.

Fortunately, DHCP services and the Windows Server 2008 DNS server cooperate to help prevent this problem from happening. You can configure the DNS server to track the age of each dynamically-assigned record and to periodically remove records that are older than the number of days that you specify. This process is known as *scavenging*.

The age of a resource record is based on when it was created or last updated. By default, computers running Windows send a request to the DNS server to update their records every 24 hours.

📝 Note

To prevent unnecessary replication, you can configure the Windows Server 2008 DNS server to ignore update requests for a period of time that you specify.

In this manner, Windows-based computers notify the DNS server that they are still on the network and that their records are not subject to scavenging.

Because scavenging can cause problems on a network if it is not configured correctly, Windows Server 2008 disables scavenging by default. We recommend that you enable scavenging with default settings if you frequently add computers to or remove computers from your network.

To enable scavenging on a DNS server

- 1. On the DNS server on which you want to enable scavenging, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- 2. In the console tree, click the applicable DNS server.
- 3. On the Action menu, click Properties.
- 4. Click the **Advanced** tab, select **Enable automatic scavenging of stale records**, and then click **OK**.

moso-be-i mopercies	?	
Debug Logging Even Interfaces Forward	t Logging Monitoring Security ers Advanced Root Hints	
Server version number:		
Server options:		
BIND secondaries	bles forwarders)	
Fail on load if bad zone dat	а	
✓Enable round robin ✓Enable netmask ordering		
Secure cache against pollu	tion	
Name checking:	tion Multibyte (UTF8)	
Name checking:	tion Multibyte (UTF8) From Active Directory and registry	
Name checking: Load zone data on startup: ✓ Enable automatic scaveng	tion Multibyte (UTF8) From Active Directory and registry ing of stale records	
 ☑ Enable network ordering ☑ Secure cache against pollu ☑ Mame checking: ☑ Load zone data on startup: ☑ Enable automatic scaveng Scavenging period: 	tion Multibyte (UTF8) From Active Directory and registry ing of stale records 7 days	
Name checking: Load zone data on startup: Enable automatic scaveng Scavenging period:	tion Multibyte (UTF8) From Active Directory and registry ing of stale records 7 days	
 ☑ Enable network ordering ☑ Secure cache against pollu ☑ Mame checking: ☑ Load zone data on startup: ☑ Enable automatic scaveng Scavenging period: 	tion Multibyte (UTF8) From Active Directory and registry ing of stale records 7 days <u>Reset to Default</u>	

- 5. On the Action menu, click Set Aging/Scavenging for All Zones.
- 6. Click the **Scavenge stale resource records** check box, and then click **OK**.

Server Aging/Scave	enging Propertie	25	? ×
🔽 Scavenge stale re	esource records		
No-refresh interval			
The time between and the moment w	the most recent r when the timestam	efresh of a record o may be refreshe	timestamp d again.
<u>N</u> o-refresh interva	al: 7	days	•
Refresh interval The time between can be refreshed scavenged. The re record refresh per	the earliest mome and the earliest mo efresh interval mu: riod.	nt when a record I oment when the re st be longer than t	timestamp cord can be he maximum
<u>R</u> efresh	7	days	•
		OK	Cancel

7. In the Server Aging/Scavenging Confirmation dialog box, select Apply these settings to the existing Active Directory-integrated zones, and then click OK.

Server Aging/Scavenging Confirmation
Default settings for new Active Directory-integrated zones:
Scavenge stale resource records: Enabled
Apply these settings to the existing Active Directory-integrated zones
OK Cancel

Troubleshooting DNS

Most often, Domain Name System (DNS) configuration problems are exposed when one or more DNS client computers cannot resolve host names.

To troubleshoot DNS problems, you must determine the scope of the problem. To do this, you use the **ping** command on multiple clients to resolve the names of hosts on the intranet and the Internet, and to test overall network connectivity. Run the following commands on several DNS client computers and with several target computers, and then note the results:

- **ping** DNS_server_ip_address
- **ping** *internal_host_ip_address*, where *internal_host_ip_address* is the IP address of a computer that exists in the client's domain
- **ping** *internal_host_name*, where *internal_host_name* is the fully qualified domain name (FQDN) of the computer
- **ping** *Internet_host_name*, where *Internet_host_name* is the name of a computer that exists on the Internet.

📝 Note

It is not important whether an Internet computer responds to the **ping** command. What is important is that DNS can resolve the name that you specify to an IP address.

The results of these tests suggest the nature of the problem. The following table shows possible results, causes, and solutions.

ping command result	Possible cause	Possible solution
Multiple clients cannot resolve any intranet or Internet names	This result suggests that the clients cannot access the assigned DNS server. This might be the result of general network problems, particularly if the ping command using IP addresses fails. Otherwise, if you have configured the clients to obtain DNS server addresses automatically, you might not have configured the Dynamic Host Configuration Protocol (DHCP) servers on the network properly.	Review the configuration of the DHCP servers on the network.
Multiple clients cannot resolve intranet names, but they can resolve Internet names	This result suggests that host (A) resource records, or records such as service locator (SRV) resource records, do not exist in the DNS zone database. Also see "One client only cannot resolve intranet names, only	Ensure that the appropriate resource records exist and that you have configured the DNS server properly to receive automatic updates. If the target host names are located in a particular child zone, ensure that you have configured delegation of

ping command result	Possible cause	Possible solution
	Internet names."	that zone properly. To test registration of records for a domain controller, use the dcdiag /test:dns /v /s:domain_controller command.
One client only cannot resolve any intranet or Internet names	If the ping command using IP addresses fails, this result indicates that the client computer cannot connect to the network. If the ping command using IP addresses succeeds, but the ping command cannot resolve DNS domain names, the TCP/IP settings of the client may be incorrect.	Ensure that the client computer is physically connected to the network and that the network adapter for the computer functions properly, or correct the TCP/IP settings, as necessary. To correct the settings, see <u>Configuring Client Settings</u> .
One client only cannot resolve intranet names, only Internet names	If you previously configured the client computer to connect directly to the Internet, its TCP/IP properties might be configured to use an external DNS server, such as a DNS server from an Internet service provider (ISP). In most cases, the client should not use a DNS server from an ISP as either the preferred or alternate DNS server because the DNS server at the ISP is not able to resolve internal names. Using a DNS server from an ISP in the TCP/IP configuration of a client can also cause problems with conflicting internal and external namespaces.	To correct the settings, see <u>Configuring Client Settings</u> .

If you have ruled out all of these potential problems for a particular client and still cannot resolve DNS names, use the procedures in <u>Configuring Client Settings</u> to verify the DNS client settings. Then, at a command prompt, type **ipconfig /all** to view the current TCP/IP configuration.

If the client does not have a valid TCP/IP configuration, you can perform one of the following tasks:

- For dynamically configured clients, use the **ipconfig /renew** command to manually force the client to renew its IP address configuration with the DHCP server.
- For statically configured clients, modify the client TCP/IP properties to use valid configuration settings or to complete its DNS configuration for the network.