Microsoft Windows Server System

DNS Step-by-Step Guide

Microsoft Corporation

Published: October 2005

Authors: Andrea Weiss and Jim Groves

Editors: Justin Hall and Carolyn Eller

Abstract

This document can help you implement Domain Name System (DNS) on Microsoft® Windows Server™ 2003 on a small network. DNS is the main way that Windows Server 2003 translates computer names to network addresses. An Active Directory®-based domain controller also 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 queried with the computer's name.

This guide explains how to set up DNS on a simple network consisting of a single domain.

Microsoft

Contents

Domain Name System Step-by-Step Guide

Domain Name System (DNS) is a system for naming computers and network services that organizes them into a hierarchy of domains. DNS naming is used on TCP/IP networks, such as the Internet, 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 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 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 server's numeric IP address to identify the Microsoft Web server on the Internet.

DNS requires little ongoing maintenance for small and medium-sized businesses, which typically have one to four DNS servers (larger medium-sized organizations usually have between four and 14 DNS servers). DNS problems, however, can affect availability for your entire network. Most DNS problems arise because of DNS settings that are incorrectly configured. By following the procedures in this guide, you can avoid such problems when you deploy DNS in a simple Microsoft® Windows Server™ 2003–based network.

This guide explains how to install and configure a basic DNS implementation in a network that consists of a single new Active Directory® domain. It then addresses some advanced topics that medium-sized organizations might need to consider. Finally, it includes some basic DNS troubleshooting steps you can take if you suspect your environment is having problems with DNS.

In This Guide

- Troubleshooting DNS (DNS Step-by-Step)

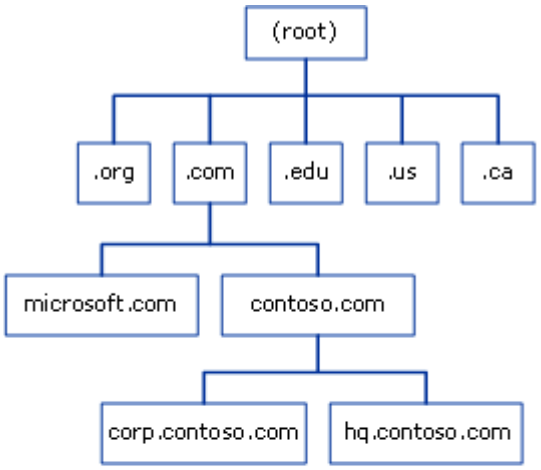
Planning DNS

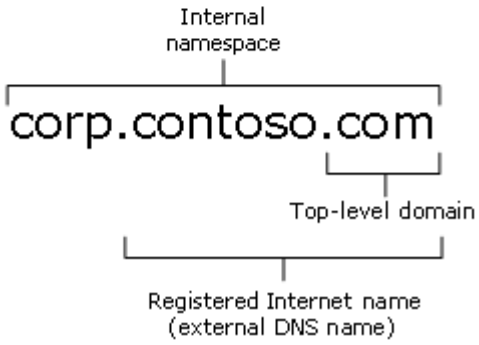
DNS is the primary method for name resolution in the Microsoft® Windows Server™ 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition operating systems (collectively referred to as "Windows Server 2003" in this guide). DNS is a requirement for deploying the Active Directory® directory service. Integrating DNS with Active Directory enables DNS servers to take advantage of the security, performance, and fault tolerance capabilities of Active Directory.

Typically, you organize your DNS namespace (the association of domains, subdomains, and hosts) in a way that supports how you plan to use Active Directory to organize the computers on your network. For more information about using Active Directory to organize your network, see "Designing the Active Directory Logical Structure" in Designing and Deploying Directory and Security Services on Microsoft Windows Server 2003 TechCenter (http://go.microsoft.com/fwlink/?LinkId=50361) or on Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=50360).

Understanding the DNS Namespace

DNS is a hierarchical naming system. A DNS name includes the names of all of the DNS namespaces that it belongs to. The following illustration shows how the DNS namespace is organized.





The DNS namespace begins with a logical root domain that is not named, partly because it is implicit in all DNS names. The root domain in turn contains a limited number of subdomains that help organize the DNS namespace. These subdomains are called top-level domains (TLDs) because they are the highest-level or most inclusive part of the DNS namespace that people use. The names of these top-level domains are either functional or geographical.

Functional top-level domains suggest the purpose of the organization that has registered a subdomain in the top-level domain. Some of the most common functional top-level domain names are:

- The .com top-level domain, which is usually used to register DNS domain names that belong to commercial entities, such as corporations.
- The .edu top-level domain, which is most often used by educational institutions, such as colleges and public and private schools.

- The .gov top-level domain, which is used by government entities, including federal, state, and local governments.
- The .net top-level domain, which is often used by organizations that provide Internet services, such as Internet service providers (ISPs).
- The .org top-level domain, which is typically used for private, nonprofit organizations.

Geographical top-level domains indicate the country or region where the organization that registered the domain is located. For example, an organization that wants to emphasize that it is located in Canada would register its Internet domain name in the .ca top-level domain, while an organization that wants to show that it is based in Brazil would register its Internet domain name in the .br top-level domain.

Most organizations that want to have an Internet presence, such as for a Web site or sending and receiving e-mail, register an Internet domain name that is a subdomain of a top-level domain. Usually they choose a subdomain name based on their organization's name, such as contoso.com or microsoft.com. 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 Internet Protocol (IP) address when they are queried for that name. In other words, 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 just 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, and you can also design an internal namespace that is accessible only to users and computers that are within the internal network.

Organizations that require an Internet presence as well as an internal namespace must deploy both an internal and an external DNS namespace and manage each namespace separately. In this case, it is recommended that you make your internal domain a subdomain of your external domain. Using an internal domain that is a subdomain of an external domain:

- 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.

For example, an organization that has an external domain name of contoso.com might use the internal domain name corp.contoso.com.

You can use your internal domain as a parent for additional child domains that you create to manage divisions within your company, in cases where you are deploying an Active Directory domain for each division. Child domain names are immediately subordinate to the domain name of the parent. For example, a child domain for a manufacturing division that is added 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 is composed of a top-level domain name (such as .com, .org, or .edu) and a unique subdomain name chosen by the domain owner. For example, a company named Contoso Corporation would probably choose contoso.com as its Internet domain name.

When you have selected your Internet DNS domain, conduct a preliminary search of the Internet to confirm that the DNS domain name that you selected is not already registered to another organization. If you do not find that your domain name is already registered to another organization, contact your Internet service provider (ISP) to confirm that the domain name is available and to help you register your domain name. Your ISP will probably 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 relative to your registered Internet DNS domain name. For example, if you have registered 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 are deploying DNS in a private network and do not plan to create an external namespace, you should nevertheless consider registering the DNS domain name that you create for your internal domain. If you do not register the name and later attempt to

use it on the Internet, or connect to a network that is connected to the Internet, you might find that the name is unavailable.

Creating DNS Computer Names

It is important to develop a practical DNS computer-naming convention for computers on your network. This enables users to remember the names of computers on public and private networks easily, and therefore facilitates access to network resources.

Use the following guidelines when creating names for the DNS computers in your Windows Server 2003 DNS infrastructure:

- Select computer names that are easy for users to remember.
- Identify the owner of a computer in the computer name. For example, john-doe indicates that John Doe uses the computer, and pubs-server indicates that the computer is a server that belongs to the Publications department.
- Alternatively, 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 character case to convey the owner or purpose of a computer. DNS is not case-sensitive.
- Match the Active Directory 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. For more information, see "Designing the Active Directory Logical Structure" in Designing and Deploying Directory and Security Services on Microsoft Windows Server 2003 TechCenter (http://go.microsoft.com/fwlink/?LinkId=50361) or on Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=50360).
- Use unique names for all computers in your organization. Do not assign the same computer name to different computers in different DNS domains.
- Use ASCII characters to ensure interoperability with computers running versions of Windows earlier than Windows 2000. For DNS computer names, use only the characters A–Z, a–z, 0–9, and the hyphen (-).

Installing and Configuring Active Directory and DNS

When you create a new domain, the Active Directory Installation Wizard installs DNS on the server by default. This ensures that DNS and Active Directory are configured properly for integration with each other.

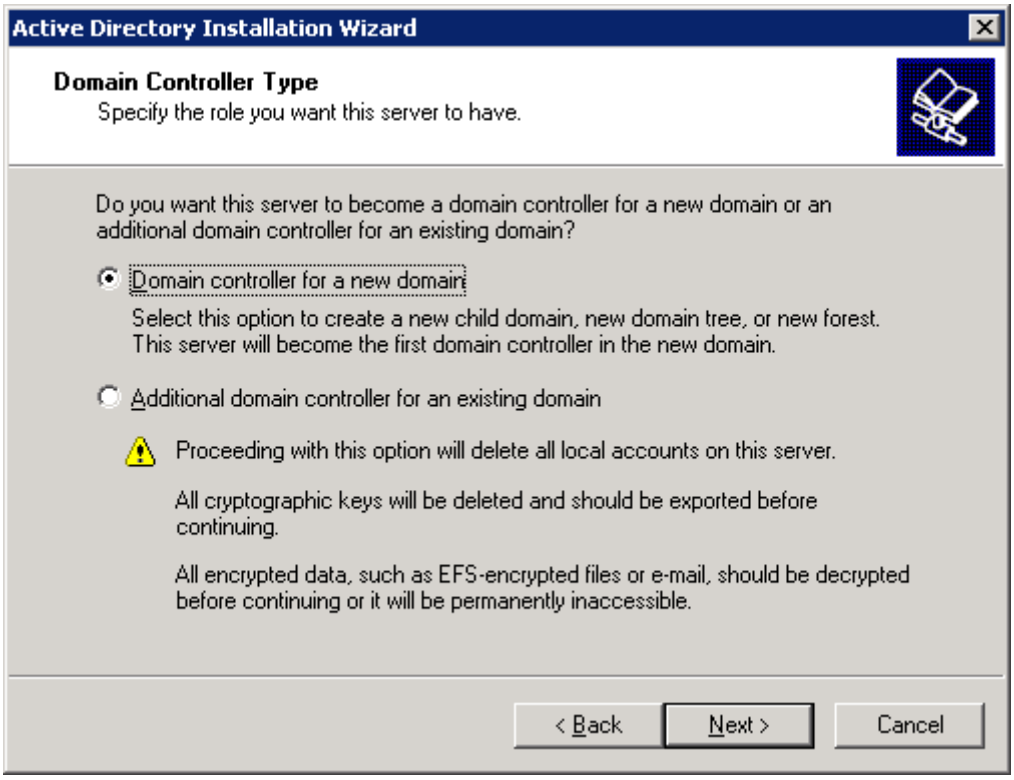
Important

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

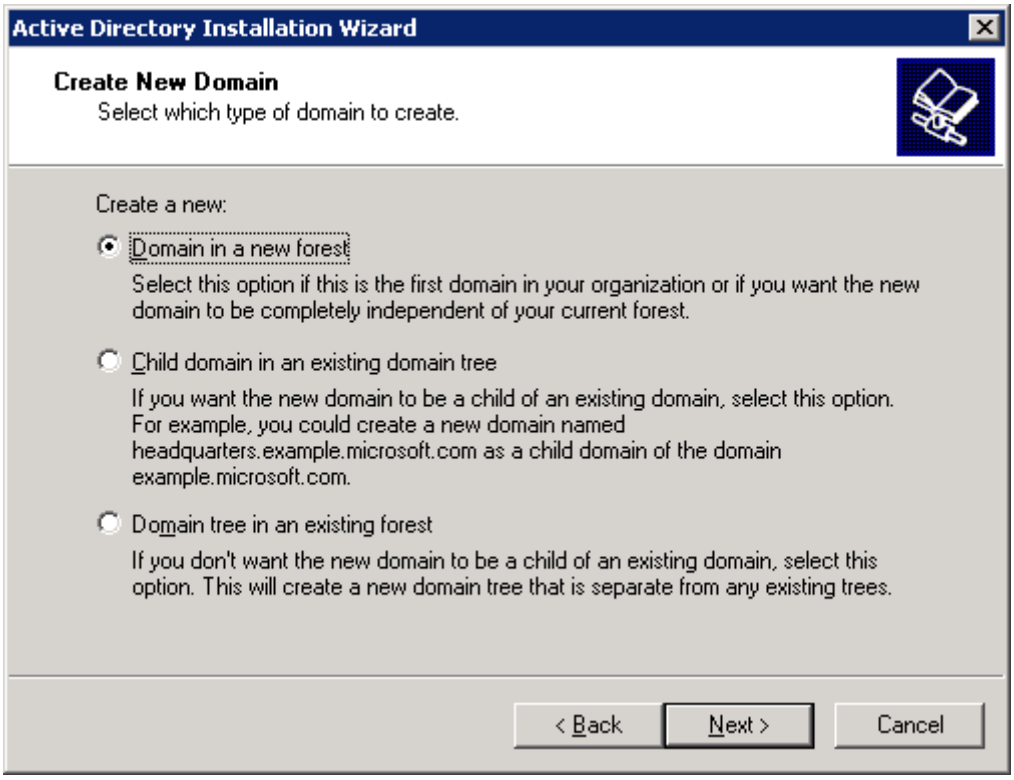
To install DNS with Active Directory in a new domain

1. Click **Start**, point to **Administrative tools**, and then click **Configure Your Server Wizard**.
2. On the **Manage Your Server** page, click **Add or remove a role**.
3. On the **Configure Your Server Wizard** page, click **Next**.
4. Click **Domain Controller (Active Directory)** and then click **Next**.
5. On the **Welcome to the Active Directory Installation Wizard** page, click **Next**.
6. On the **Operating System Compatibility** page, read the information and then click **Next**.

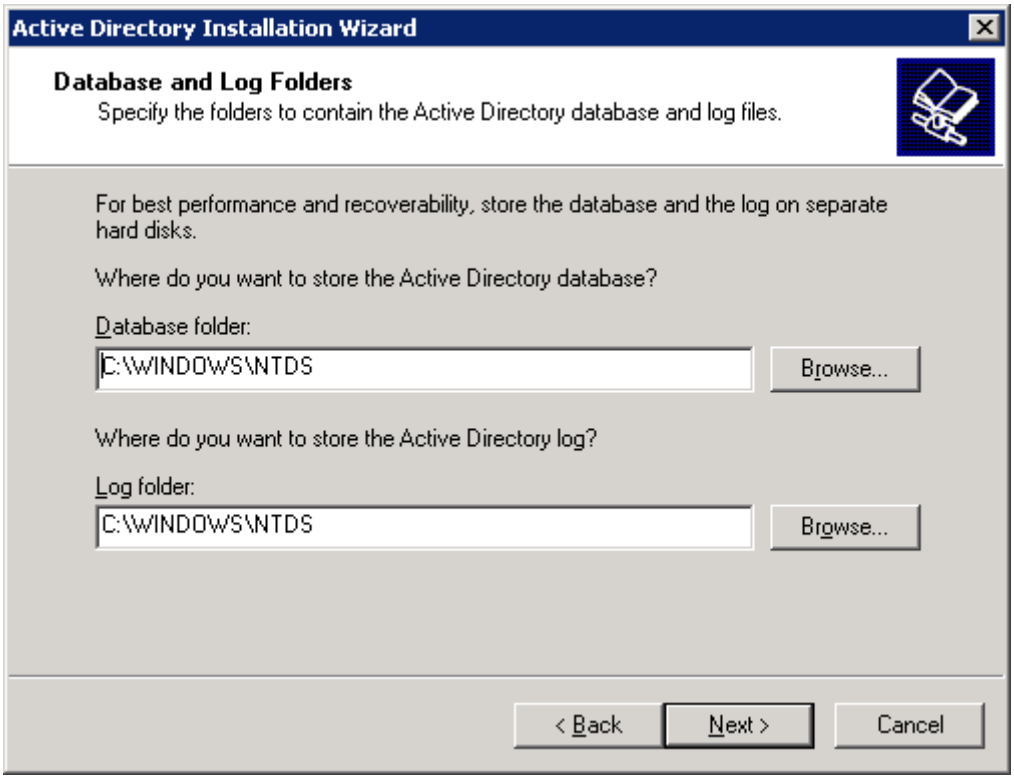
   If this is the first time you have installed Active Directory on a server running Windows Server 2003, click **Compatibility Help** for more information.
7. On the **Domain Controller Type** page, click **Domain controller for a new domain** and then click **Next**.



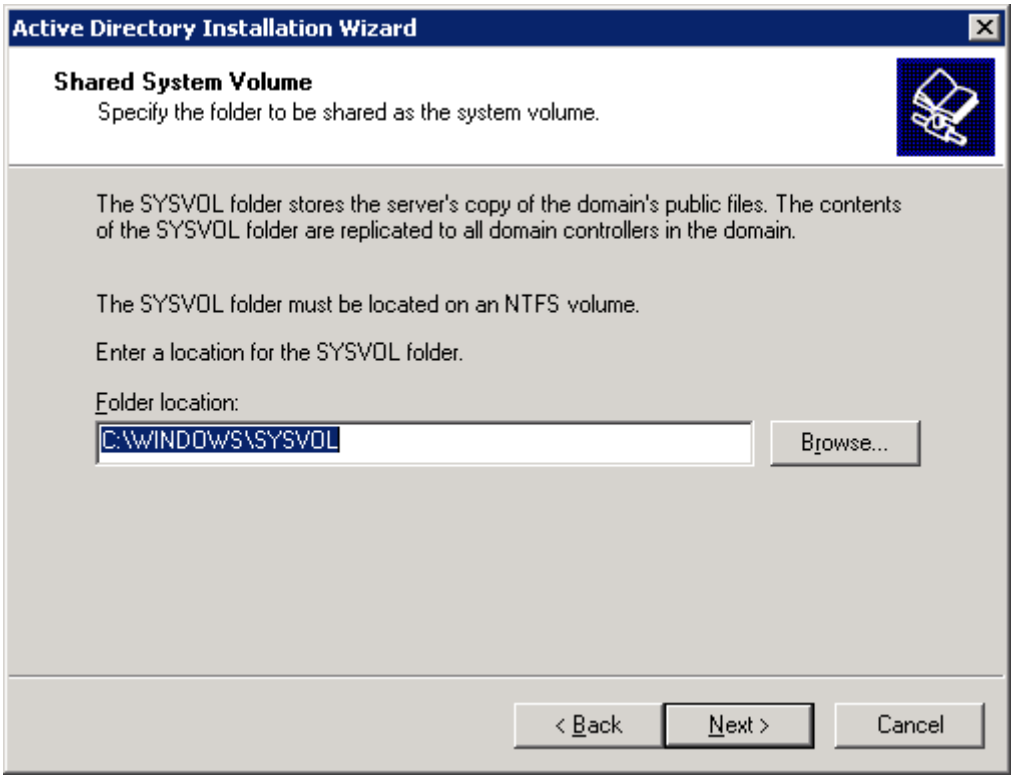
8. On the **Create New Domain** page, click **Domain in a new forest** and then click **Next**.



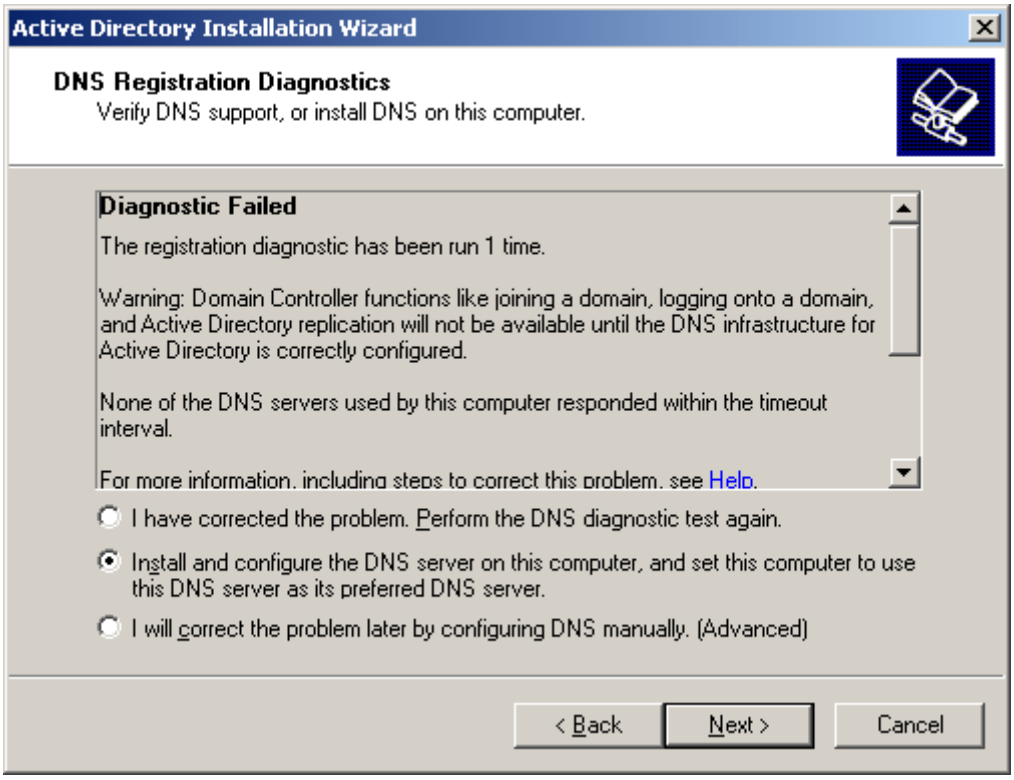
9. On the **New Domain Name** page, type the full DNS name (such as corp.contoso.com) for the new domain, and then click **Next**.
10. On the **NetBIOS Domain Name** page, verify the NetBIOS name (for example, CORP), and then click **Next**.
11. On the **Database and Log Folders** page, type the location in which you want to install the database and log folders, or click **Browse** to choose a location, and then click **Next**.



12. On the **Shared System Volume** page, type the location in which you want to install the SYSVOL folder, or click **Browse** to choose a location, and then click **Next**.

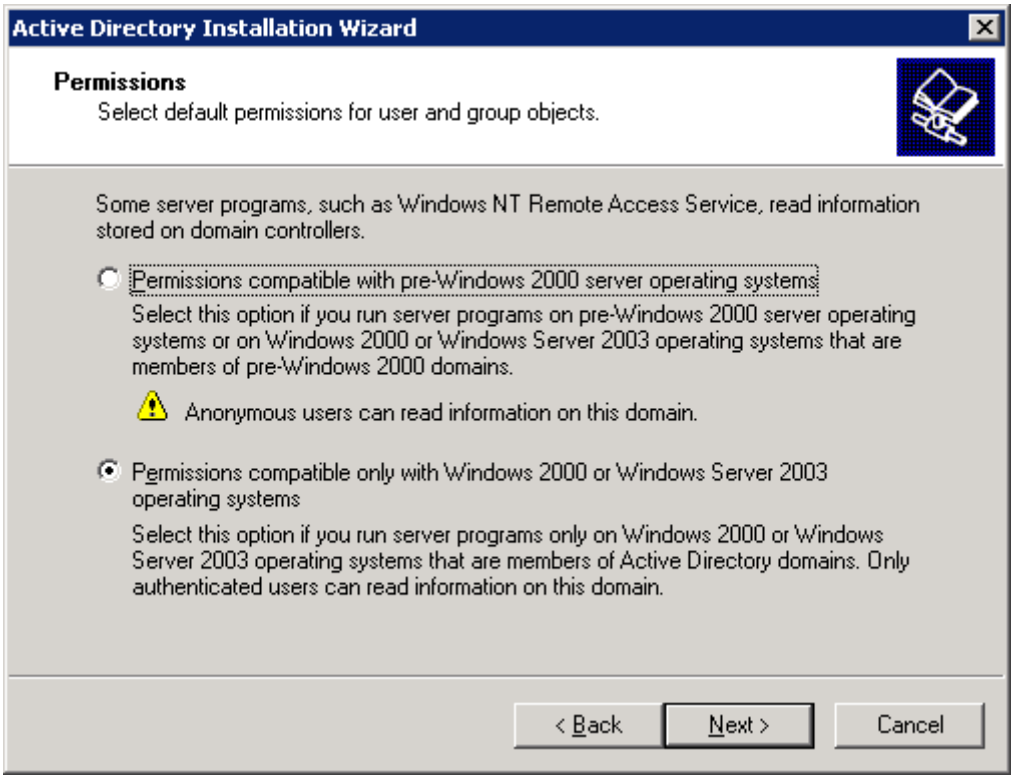


13. On the **DNS Registration Diagnostics** page, click **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server**, and then click **Next**.



14. On the **Permissions** page, select one of the following:

    - **Permissions compatible with pre-Windows 2000 Server operating systems**
    - **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**



15. On the **Directory Services Restore Mode Administrator Password** page, type a password that will be used to log on to the server in Directory Services Restore Mode, confirm the password, and then click **Next**.
16. Review the **Summary** page, and then click **Next** to begin the installation.
17. After the Active Directory installation completes, click **OK** to restart the computer.

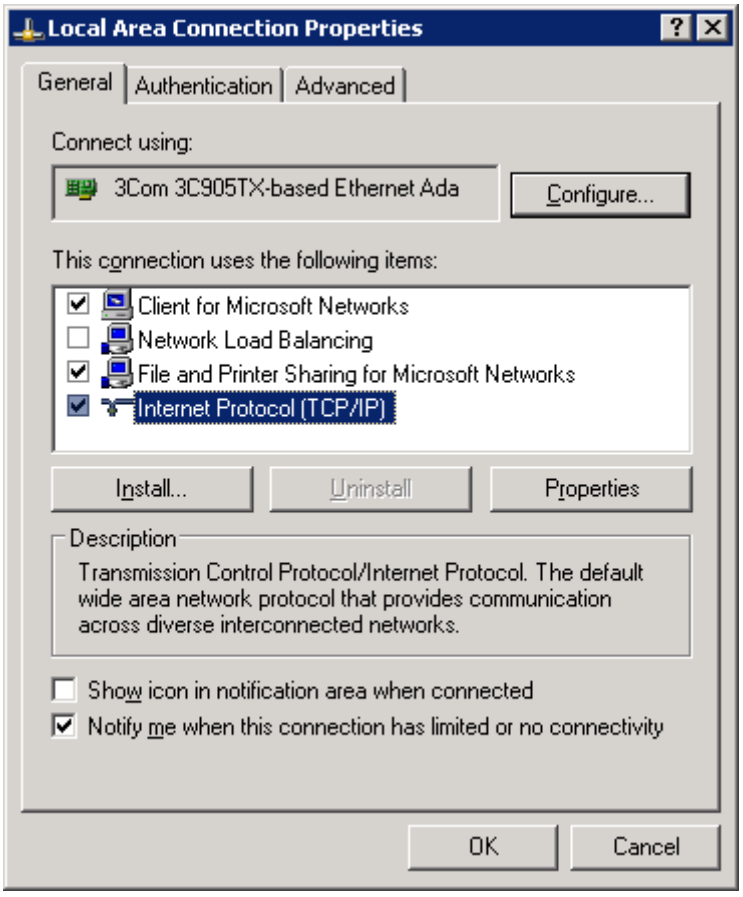
Configuring DNS Client Settings (DNS Step-by-Step)

Configure the following settings for each DNS client:

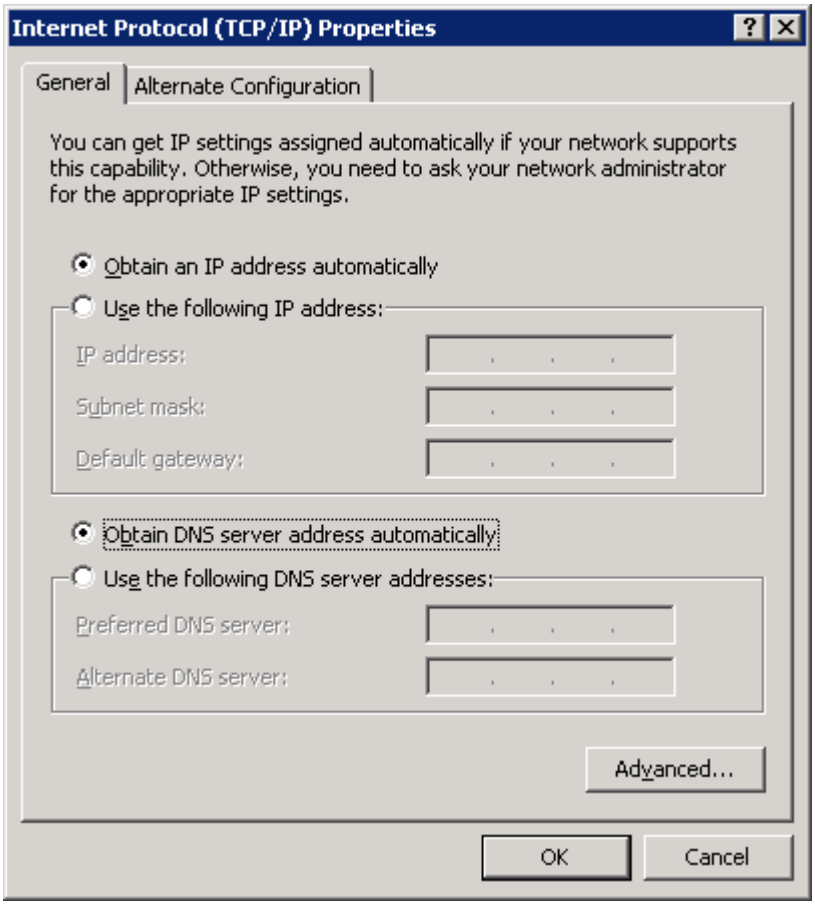
- TCP/IP settings for DNS
- Host name and domain membership

To configure DNS client settings

1. At the computer that you are configuring 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**.



4. If you want to obtain DNS server addresses from a DHCP server, click **Obtain DNS server address automatically**.



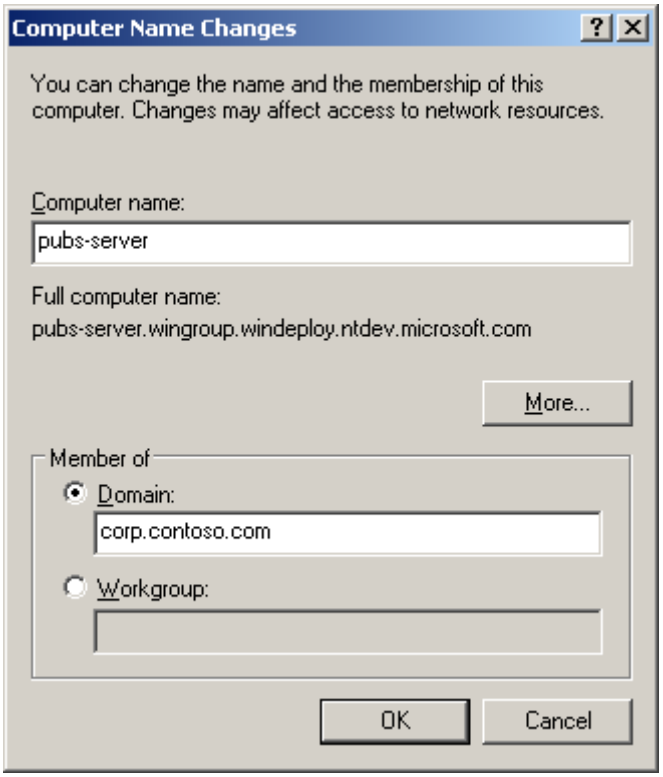
5. If you want to configure DNS server addresses manually, click **Use the following DNS server addresses**, and in **Preferred DNS server** and **Alternate DNS server**, type the Internet Protocol (IP) addresses of the preferred DNS server and alternate DNS server.
6. Click **OK** to exit.

   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.

7. In **Control Panel**, double-click **System**.
8. On the **Computer Name** tab, click **Change**.
9. In **Computer name**, type the name of the computer (the host name).

10. Click **Domain**, and then type the name of the domain you want the computer to join.



11. If **Computer Name Changes** appears, in **User Name**, type the domain name and user name of an account that is allowed to join computers to the domain, and in **Password**, type the password of the account. Separate the domain name and user name with a backslash (for example, domain\user_name).

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

Advanced DNS Configuration (DNS Step-by-Step)

In most cases, Active Directory–integrated DNS on a small, simple Windows-based network requires little configuration beyond the initial setup. Occasionally, however, you might need to perform some additional configuration tasks, such as adding resource records or configuring a DNS forwarder, to handle unusual situations.

Adding Resource Records

Resource records store information about specific network computers, such as their names, Internet Protocol (IP) addresses, and services that the computers provide. In most cases, Windows-based computers update their own resource records on DNS servers (using DNS dynamic update protocol, also known as dynamic DNS), eliminating the need for an administrator to manage them. However, if your network contains non-Windows-based computers or computers that you want to designate for handling e-mail, you might need to add the following resource records to the zone on your DNS server for these computers:

- **Host address (A)**. Maps a computer's DNS domain name to the computer's IP address.
- **Mail Exchanger (MX)**. Maps a DNS domain name to the name of a computer that exchanges or forwards e-mail.

Important

When the Active Directory Installation Wizard installs and configures DNS on the new domain controller, it creates resource records that are necessary for the proper 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 have added yourself.

Host A Resource Records

The host A resource records is used to associate the DNS domain name of a computer (or "host") to its IP address. The host A resource record is not required for all computers, but it is required for any computer that shares resources on a network and needs to be identified by its DNS domain name.

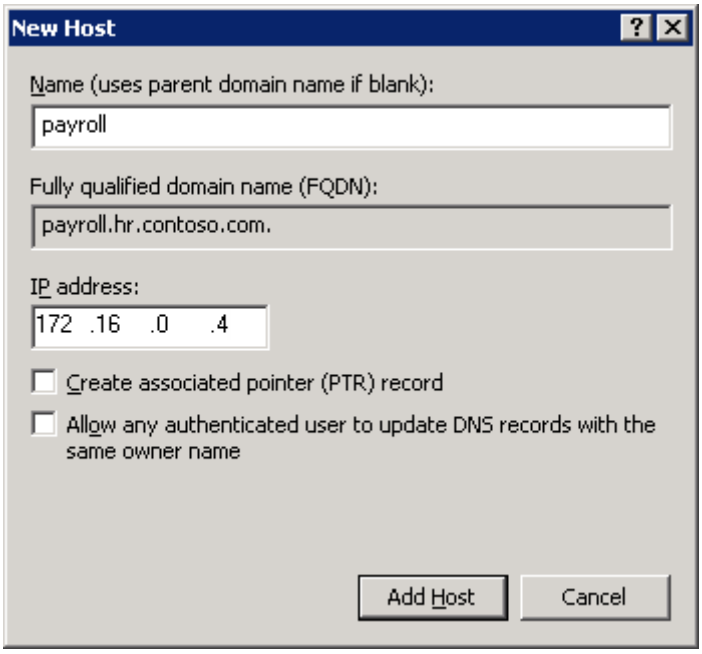
- Windows clients and servers use the Dynamic Host Configuration Protocol (DHCP) Client service to dynamically register and update their own A resource records in DNS when an IP configuration change occurs.
- DHCP–enabled client computers running earlier versions of Microsoft operating systems can have their A resource records registered and updated by proxy if they obtain their IP address lease from a qualified DHCP server. (Only the Windows 2000 and Windows Server 2003 DHCP Server service supports this feature.)
- You can manually create an A resource record for a static TCP/IP client computer or a computer running non-Windows operating systems by using the DNS snap-in.

To add a host A resource record to a zone

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

Important

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



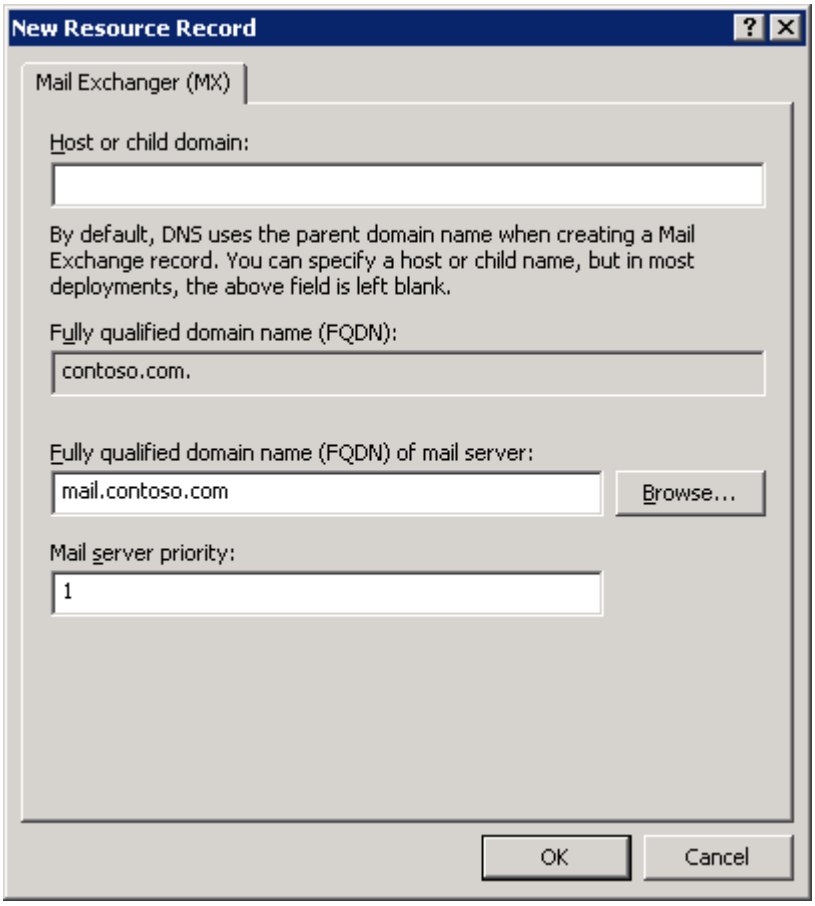
MX Resource Records

The MX resource record is used by e-mail applications to locate a mail server by using the DNS domain name that appears in the destination e-mail address for the recipient. For example, a DNS query for the name sales.corp.contoso.com can be used to find an MX resource record, which enables an e-mail application to forward or exchange mail to a user with the e-mail address user@sales.corp.contoso.com.

The MX resource record shows the fully qualified DNS domain name for the computer that processes e-mail for a domain. If multiple MX resource records exist, the DNS Client service attempts to contact the e-mail servers in the order of preference using the **Mail server priority** field. The lowest value has the highest priority, and the highest value has the lowest priority.

To add a mail exchanger MX resource record to a zone

1. At the DNS server, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree, right-click the applicable zone, and then click **New Mail Exchanger (MX)**.
3. In **Host or child domain**, type the name of the host or domain of the mail exchanger for this domain only if it is different from the parent domain; otherwise, leave this field blank.



4. In **Fully qualified domain name (FQDN) of mail server**, type the DNS domain name of an existing mail server that can function as a mail exchanger for the domain.
5. In **Mail server priority**, type a number between 0 and 65535 that indicates the priority of the mail server among other mail exchangers for this domain. The

mailer attempts to deliver mail to servers with lower priority numbers before attempting to deliver to servers with higher priority numbers.

Automatically Removing Outdated Resource Records

While the ability of DHCP to register A and PTR resource records automatically whenever a new device is added to the network makes life easier for the network administrator, it does have one drawback: Unless action is taken to remove them, those resource records will remain in the DNS zone database indefinitely. While this is not a problem with relatively static networks, it negatively affects networks that change frequently (with the addition and removal of portable computers, for example). This accumulation of records can result in poor performance of both the DNS server and DHCP services as both have to work around these stale (obsolete) host/address mappings. Eventually, the zone could even run out of addresses for computers that are subsequently added to the network.

Fortunately, Windows DHCP services and the Windows Server 2003 DNS server are designed to cooperate to help prevent this from happening. You can configure the DNS server to track the age of each dynamically assigned record and to periodically remove records older than a specified number of days, a process known as scavenging.

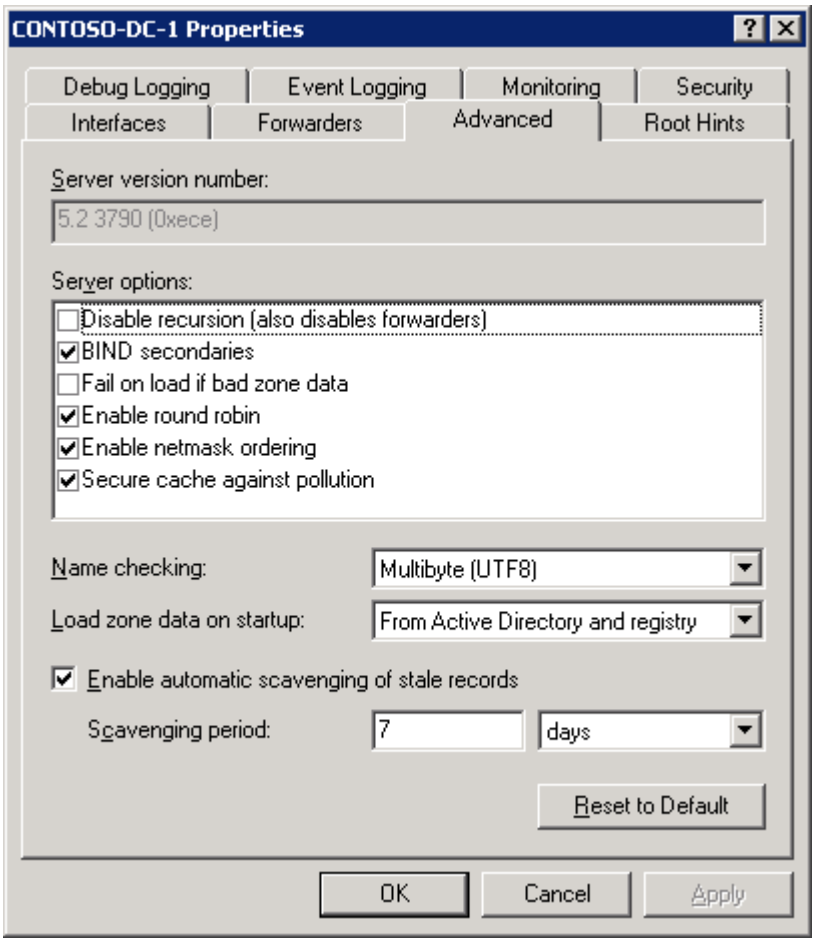
The age of a record is based on when it was created or last updated. By default, computers running Windows 2000, Windows XP, and Windows Server 2003 send a request to the DNS server to update their records every 24 hours. (To prevent unnecessary replication, the Windows Server 2003 DNS server can be configured to ignore these requests for a period of time.) The DNS server is thereby notified that the computers in question are still on the network and their records are not subject to scavenging.

Because scavenging can cause problems on a network when it is misconfigured, it is disabled by default in Windows Server 2003. Enabling scavenging with default settings is quite safe and is recommended if computers are frequently added to and removed from your network.

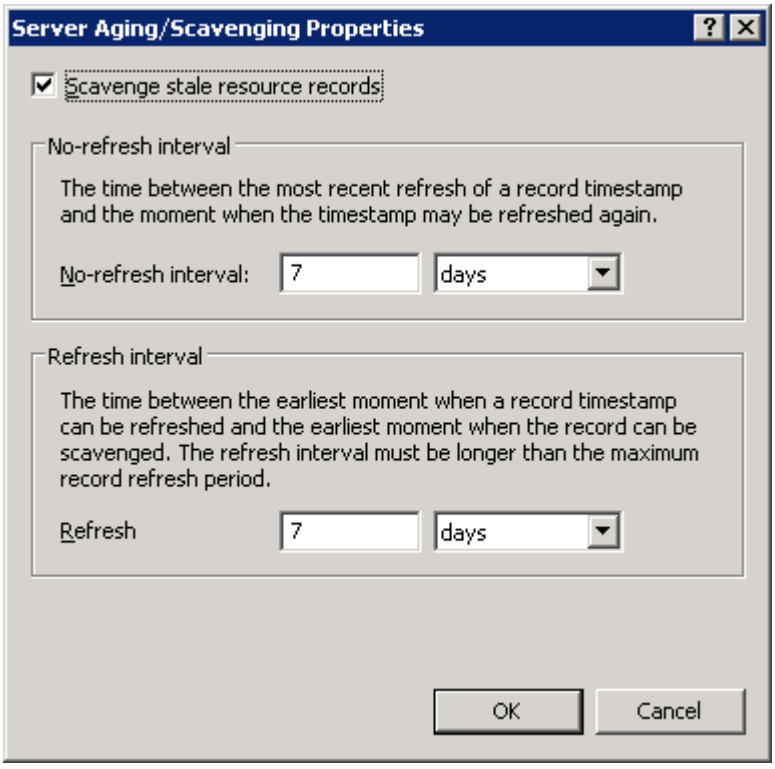
To enable scavenging on a DNS server

1. At the DNS server you want to enable scavenging on, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree, click the applicable DNS server.

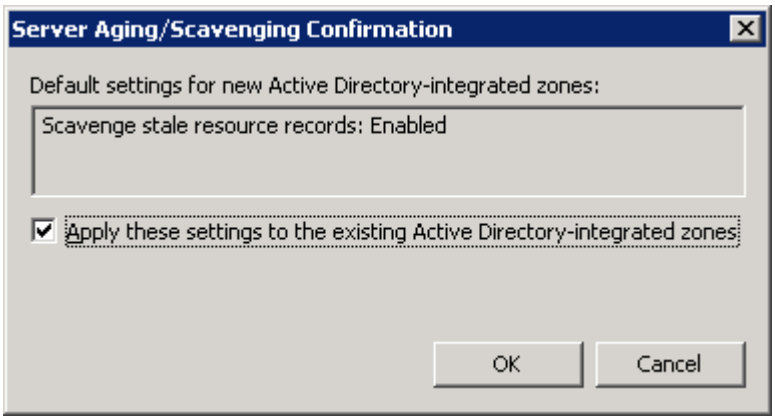
3. On the **Action** menu, click **Properties**.
4. Click the **Advanced** tab, select **Enable automatic scavenging of stale records**, and then click **OK**.



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



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



Configuring a Forwarder for Internet Access

A forwarder is a DNS server on a network that forwards DNS queries for external DNS names to DNS servers outside of that network. By using a forwarder, you can manage how names outside of your network are resolved, such as names on the Internet. When you designate a DNS server as a forwarder, you make that forwarder responsible for handling external traffic. If you are not using a firewall to isolate your network from the Internet, you should use a forwarder to provide Internet access to clients on your network.

Important

Connecting your network directly to the Internet without using a firewall to control external access to your network computers can result in serious security issues. Microsoft strongly recommends that you use a firewall instead of a forwarder to provide Internet connectivity for your network clients.

To configure a DNS server to use a forwarder

1. At the DNS server that you want to configure to use forwarders, 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. On the **Forwarders** tab, under **DNS domain**, click **All other domain names**.
5. Under **Selected domain's forwarder IP address list**, type the Internet Protocol (IP) address of a forwarder supplied by your Internet service provider (ISP), and then click **Add**.
6. Click **OK** to exit.

Troubleshooting DNS (DNS Step-by-Step)

Most often, DNS configuration problems are exposed when one or more DNS client computers are unable to resolve host names.

The first step in troubleshooting DNS problems is to determine the scope of the problem by using the **ping** command on multiple clients to resolve the names of hosts on the intranet and the Internet and to test overall network connectivity. Use the following

commands on several DNS client computers and with several different target computers, and note the results:

- **ping** *internal_host_ip_address*
- **ping** *internal_host_name*
- **ping** *Internet_host_name*

where *internal_host_ip_address* is the Internet Protocol (IP) address of a computer that exists in the client's domain, *internal_host_name* is the DNS domain name of the computer, and *Internet_host_name* is the name of a computer that exists on the Internet.

Note that it is not important whether an Internet computer responds to the **ping** request, only whether the specified name can be resolved to an IP address. The results of these tests will suggest the nature of the problem, as listed in the following table.

Ping Command Result	Possible Cause
Multiple clients cannot resolve any intranet or Internet names	This might indicate that the clients cannot access the assigned DNS server. This might be the result of general network problems, particularly if **ping** using IP addresses fails. Otherwise, if the clients are configured to obtain DNS server addresses automatically, the DHCP servers on the network might not be configured properly.
Multiple clients cannot resolve intranet names, but can resolve Internet names	This suggests that host (A) resource records or other records (such as SRV records) do not exist in the DNS zone database. Check to ensure that the appropriate resource records exist and that the DNS server is properly configured to receive automatic updates, as appropriate. If the target host names are located in a particular child zone, ensure that delegation of that zone is properly configured.

Ping Command Result	Possible Cause
Multiple clients cannot resolve Internet names, but can resolve intranet names	The designated forwarder of the DNS domain is unavailable, or the DNS server is not properly configured to use a forwarder. For more information about configuring a DNS server to use a forwarder, see Advanced DNS Configuration (DNS Step-by-Step) in this guide.
One client only cannot resolve any intranet or Internet names	If the **ping** command using IP addresses fails, this indicates that the client computer cannot connect to the network at all. Ensure that the client computer is physically connected to the network and that the network adapter for the computer is functioning properly. If the **ping** command using IP addresses succeeds, but **ping** cannot resolve DNS domain names, then the TCP/IP settings of the client are probably incorrect. To correct the settings, see Configuring DNS Client Settings (DNS Step-by-Step) in this guide.
One client only cannot resolve intranet names, only Internet names	If the client computer was previously configured 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 unable 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 Configuring DNS Client Settings (DNS Step-by-Step) in this guide.

If you have ruled out all of these potential problems for a particular client and still cannot resolve DNS names, use the following procedure to verify the DNS client settings.

To verify DNS client configuration in TCP/IP settings

1. Log on to the DNS client computer with the Administrator account.
2. Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
3. In **Network and Dial-up Connections**, right-click the local area connection that you want, and then click **Properties**.
4. In **Local Area Network Connection Properties**, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. If **Obtain an IP address automatically** is selected, type the following at a command prompt, and then press ENTER:

   ipconfig /all
6. Review the DNS server settings and verify that they are correct.

If the client does not have a valid TCP/IP configuration, you can either:

- 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 complete its DNS configuration for the network.