Active Directory & DNS Setup

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.

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

- Planning DNS
- Installing and Configuring Active Directory and DNS
- Configuring DNS Client Settings (DNS Step-by-Step)
- Advanced DNS Configuration (DNS Step-by-Step)

- Troubleshooting DNS (DNS Step-by-Step)

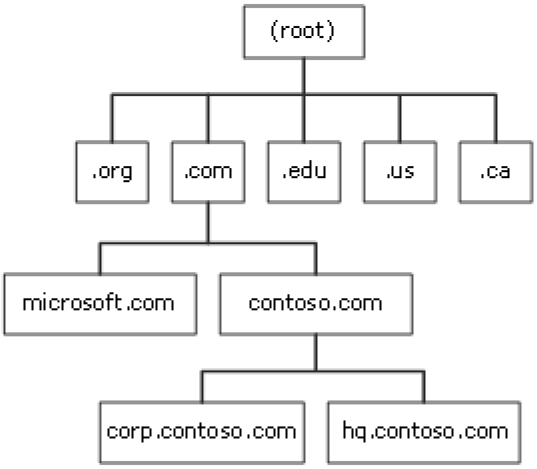
Planning DNS

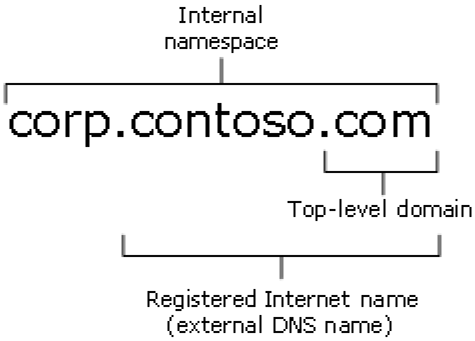
DNS is the primary method for name resolution in the Microsoft Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition operating systems (collectively referred to as "Windows Server 2003" in this guide). DNS is a requirement for deploying 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.

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.
- 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.

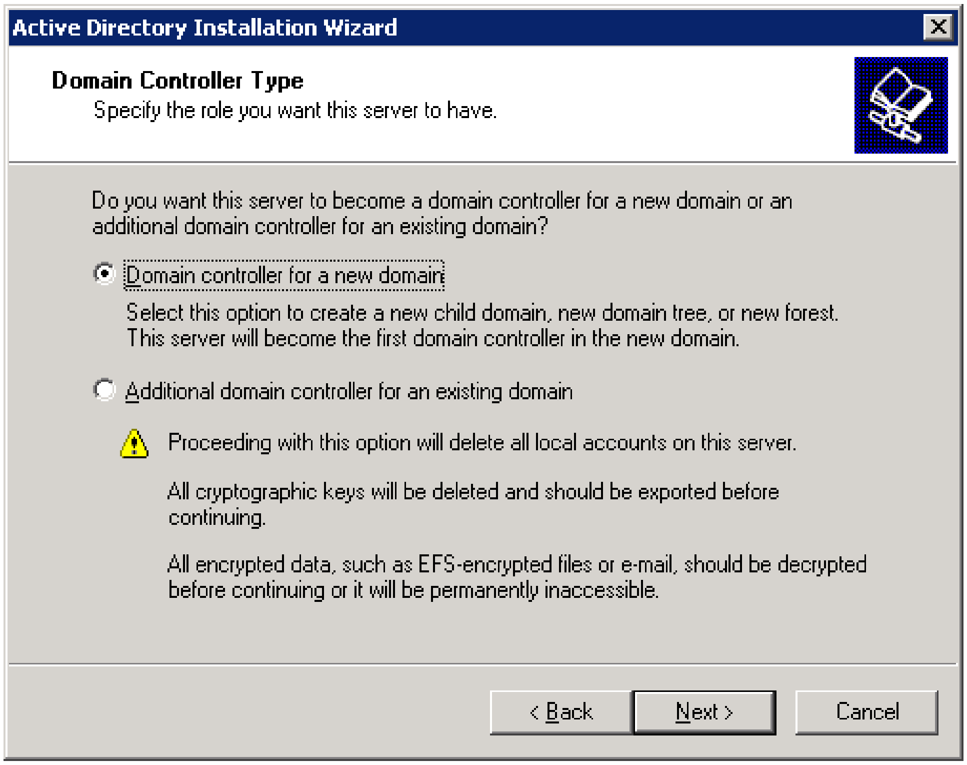
Important

> 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**.



Domain Controller Type

Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

● Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

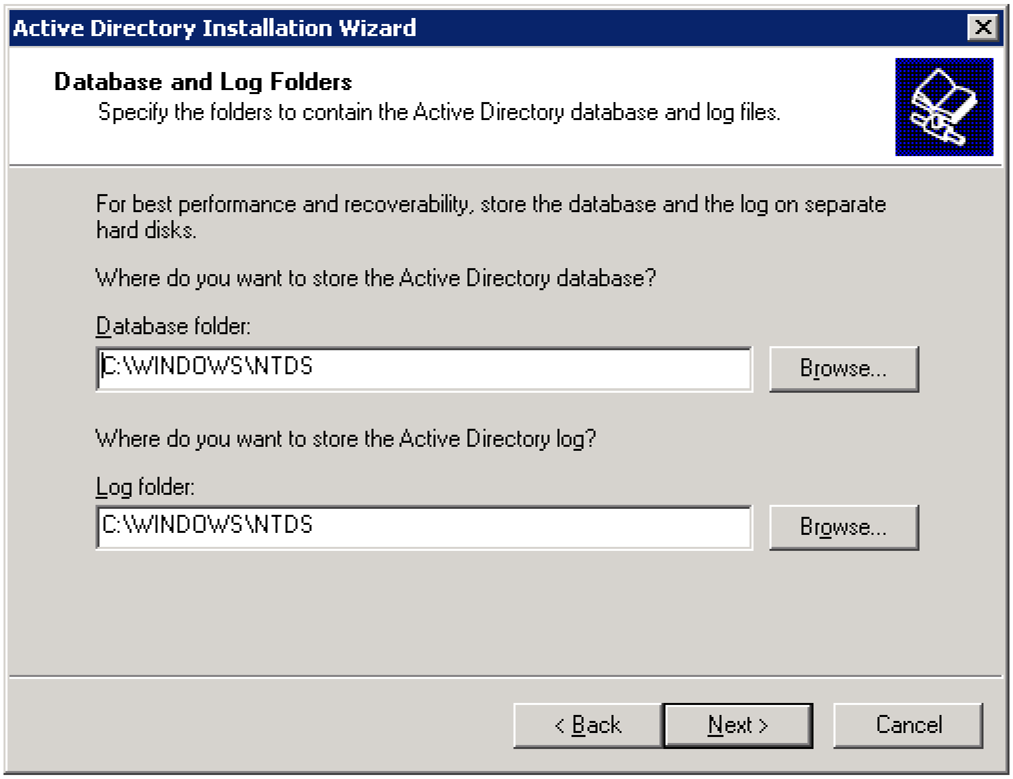
○ Additional domain controller for an existing domain

⚠ Proceeding with this option will delete all local accounts on this server.

All cryptographic keys will be deleted and should be exported before continuing.

All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

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**.



Active Directory Installation Wizard

Database and Log Folders
Specify the folders to contain the Active Directory database and log files.

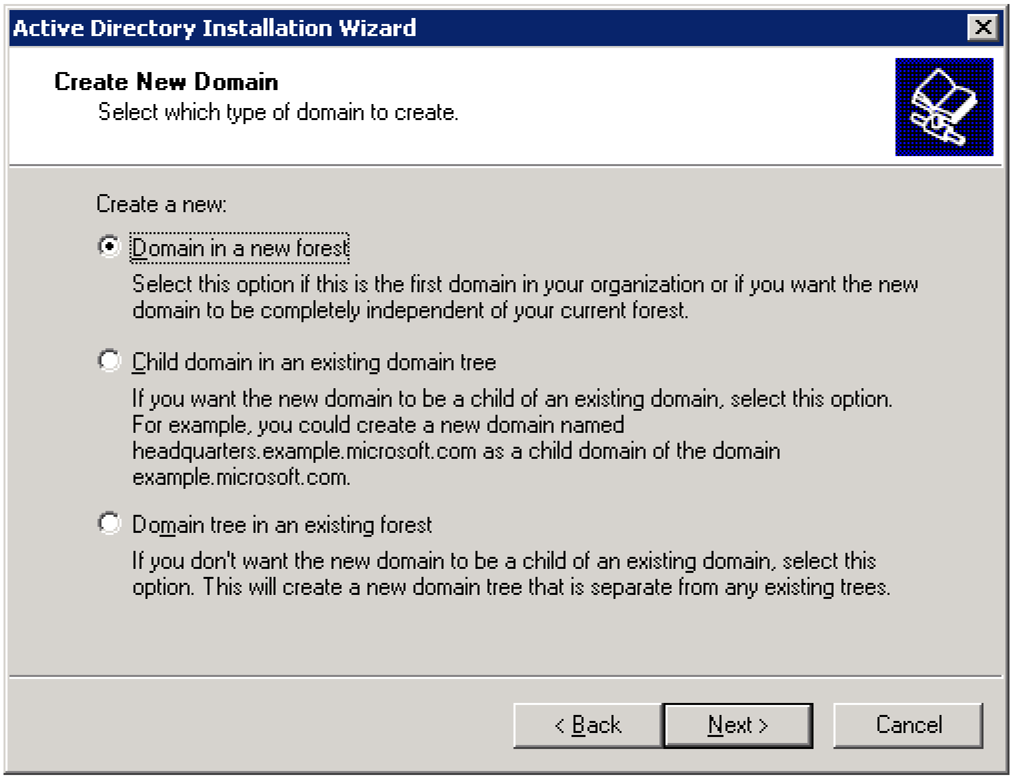
For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

Database folder:
C:\WINDOWS\NTDS

Where do you want to store the Active Directory log?

Log folder:
C:\WINDOWS\NTDS



Active Directory Installation Wizard

Create New Domain
Select which type of domain to create.

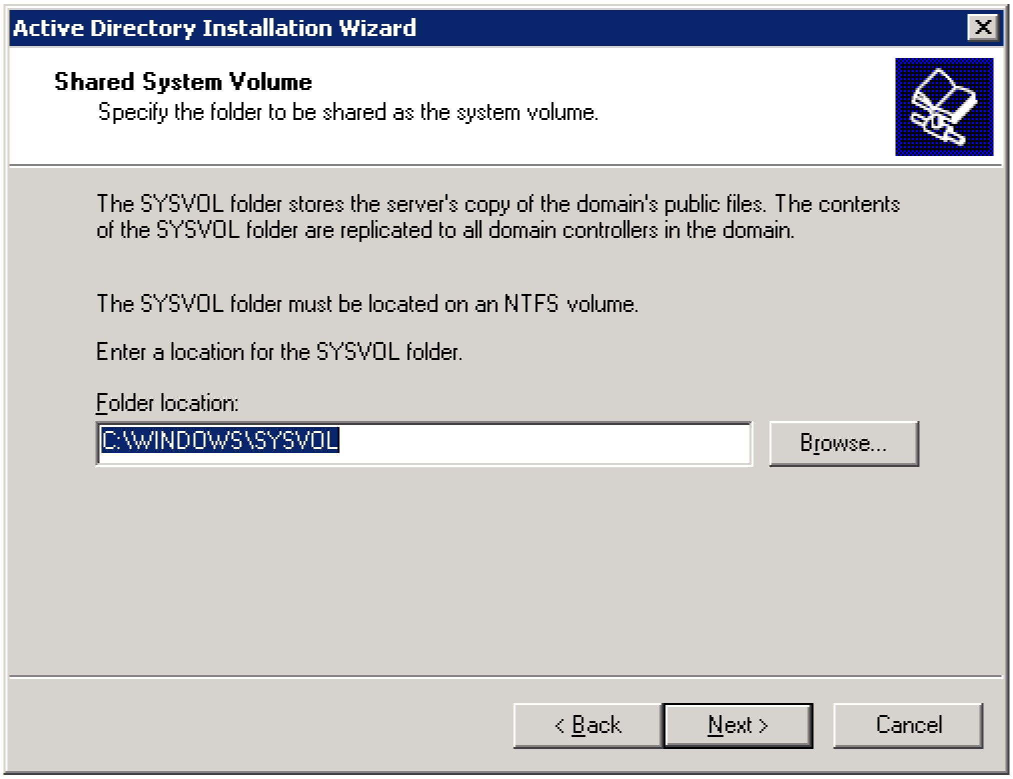
Create a new:

● Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.

○ Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.

○ Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.

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**.



Active Directory Installation Wizard

Shared System Volume

Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

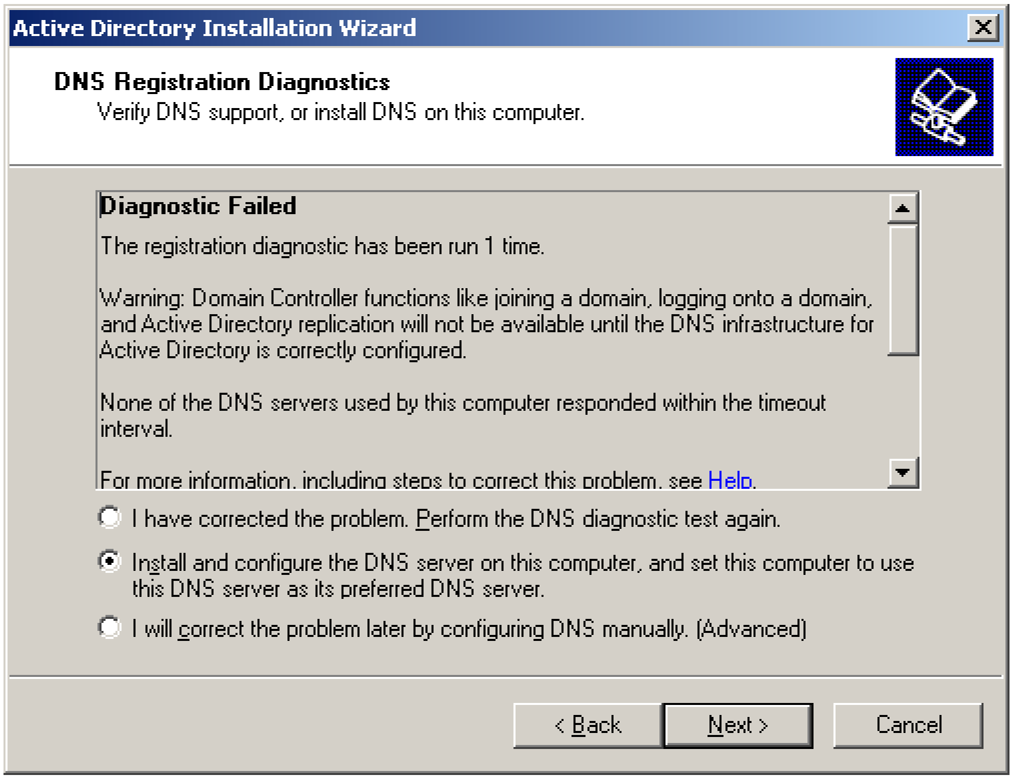
The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

Folder location:

C:\WINDOWS\SYSVOL

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**.



Active Directory Installation Wizard

DNS Registration Diagnostics

Verify DNS support, or install DNS on this computer.

Diagnostic Failed

The registration diagnostic has been run 1 time.

Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.

None of the DNS servers used by this computer responded within the timeout interval.

For more information, including steps to correct this problem, see Help.

○ I have corrected the problem. Perform the DNS diagnostic test again.

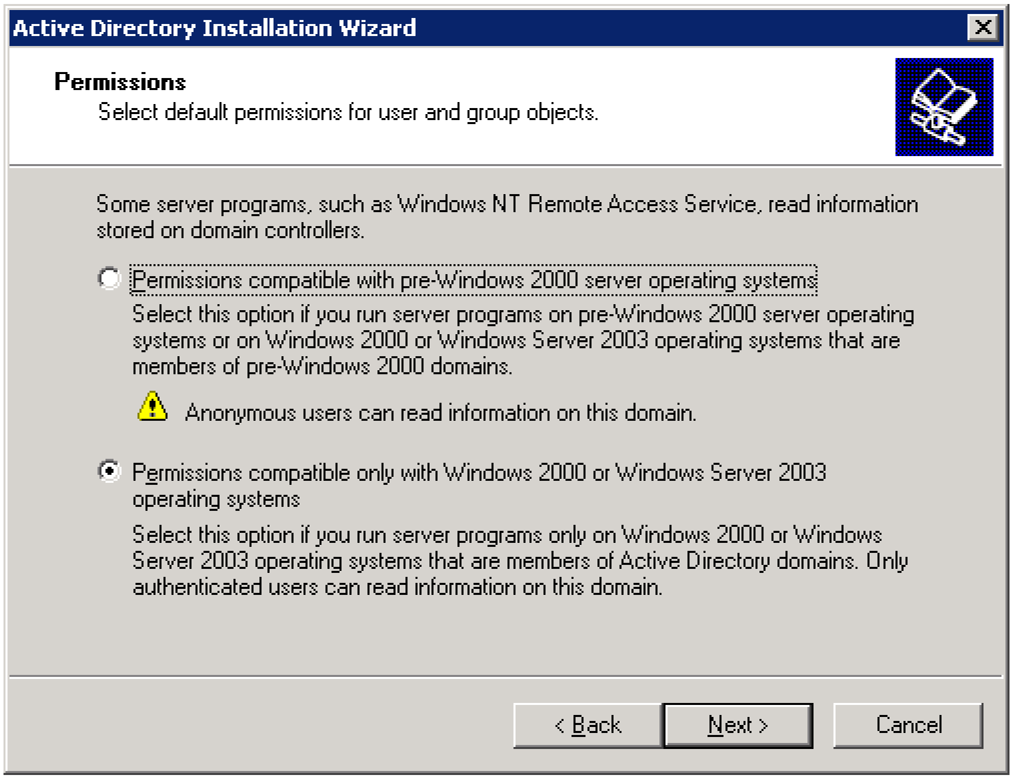
● Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.

○ I will correct the problem later by configuring DNS manually. (Advanced)

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**



Permissions

Select default permissions for user and group objects.

Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.

○ Permissions compatible with pre-Windows 2000 server operating systems

Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.

⚠ Anonymous users can read information on this domain.

● Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems

Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.

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.

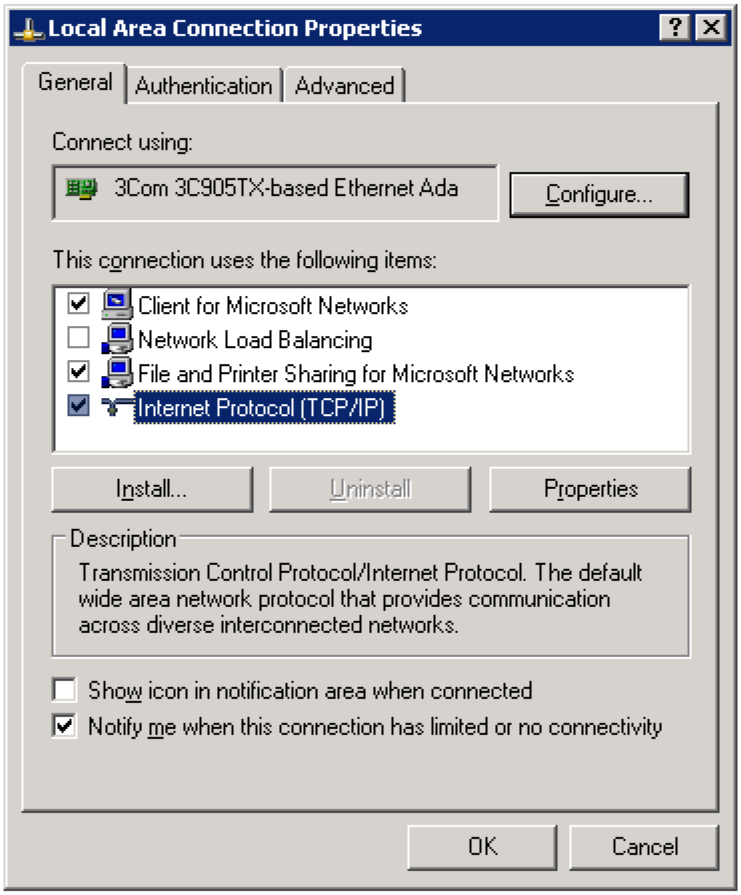
Configuring DNS Client Settings (DNS Step-by-Step)

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**.



Local Area Connection Properties

Connect using:

3Com 3C905TX-based Ethernet Ada

This connection uses the following items:

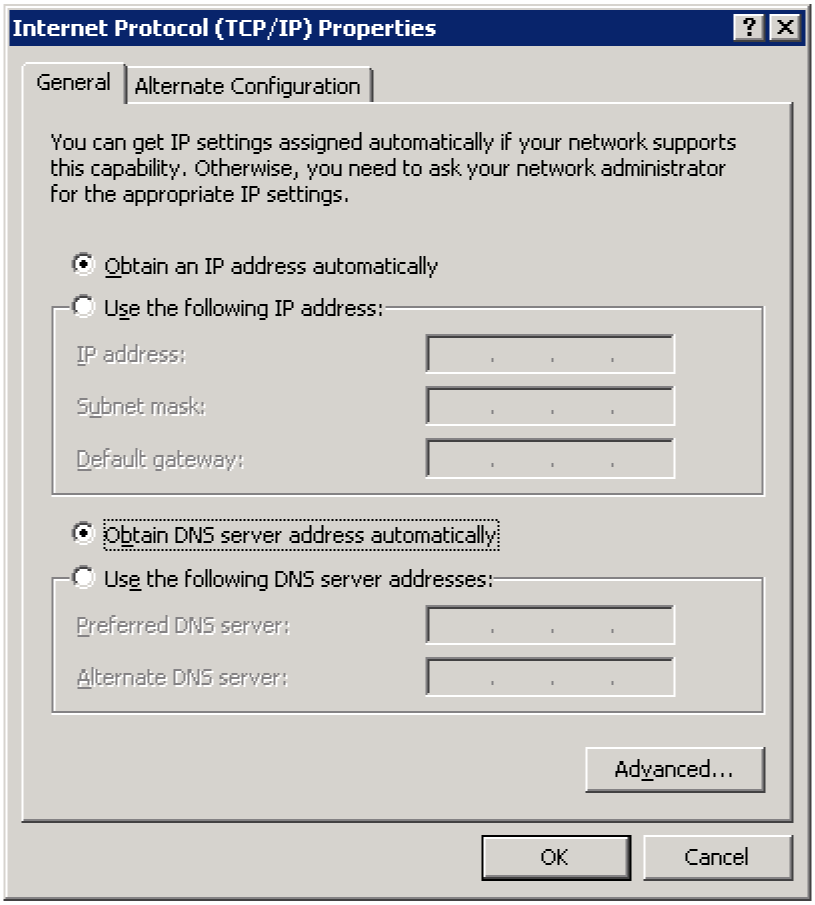
☑ Client for Microsoft Networks
☐ Network Load Balancing
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

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 connectivity

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

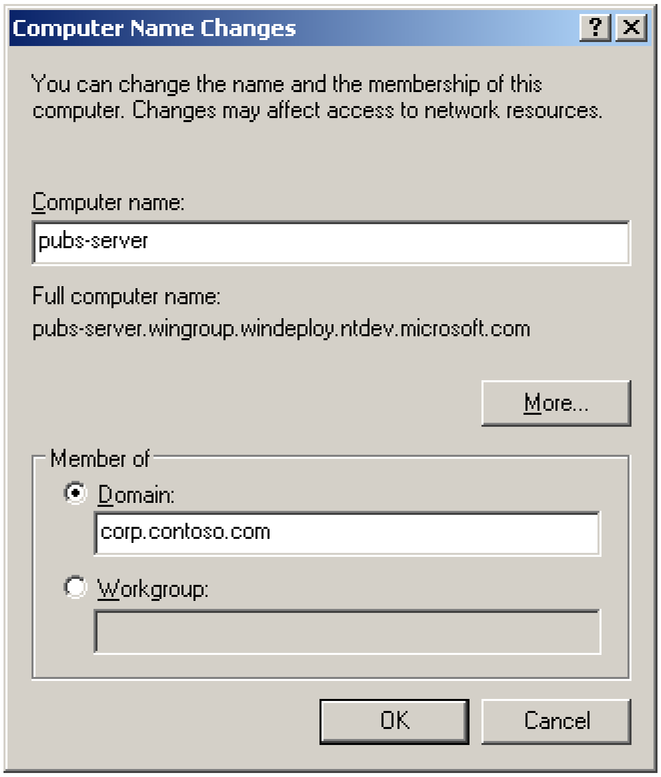
Alternate DNS server: . . .

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.



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: pubs-server

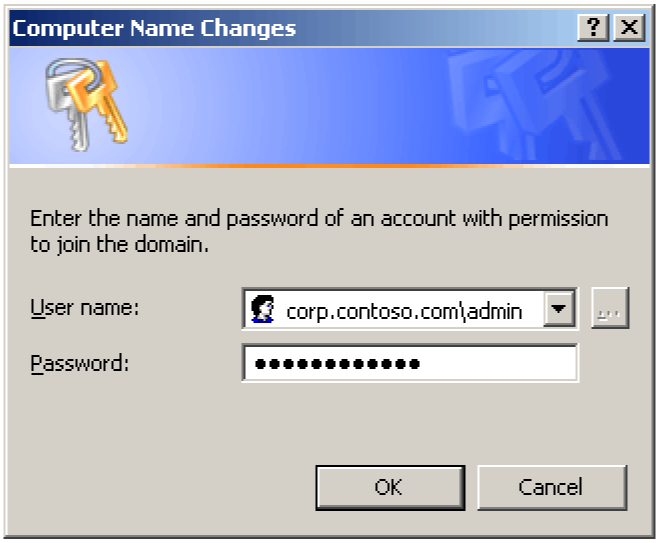
Full computer name:
pubs-server.wingroup.windeploy.ntdev.microsoft.com

Member of

● Domain: corp.contoso.com

○ Workgroup:

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\username).



Computer Name Changes

Enter the name and password of an account with permission to join the domain.

User name: corp.contoso.com\admin

Password: •••••••••••••

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

History of TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry standard suite of protocols that is designed for large networks consisting of network segments that are connected by routers. TCP/IP is the protocol that is used on the Internet, which is the collection of thousands of networks worldwide that connect research facilities, universities, libraries, government agencies, private companies, and individuals.

The roots of TCP/IP can be traced back to research conducted by the United States Department of Defense (DoD) Advanced Research Projects Agency (DARPA) in the late 1960s and early 1970s.

The following list highlights some important TCP/IP milestones:
□□□In 1970, ARPANET hosts started to use Network Control Protocol (NCP), a preliminary form of what would become the Transmission Control Protocol (TCP).

□□□In 1972, the Telnet protocol was introduced. Telnet is used for terminal emulation to connect dissimilar systems. In the early 1970s, these systems were different types of mainframe computers.

□□□In 1973, the File Transfer Protocol (FTP) was introduced. FTP is used to exchange files between dissimilar systems.

□□□In 1974, the Transmission Control Protocol (TCP) was specified in detail. TCP replaced NCP and provided enhanced reliable communication services.

□□□In 1981, the Internet Protocol (IP) (also known as IP version 4 [IPv4]) was specified in detail. IP provides addressing and routing functions for end-to-end delivery.

□□□In 1982, the Defense Communications Agency (DCA) and ARPA established the Transmission Control Protocol (TCP) and Internet Protocol (IP) as the TCP/IP protocol suite.

□□□In 1983, ARPANET switched from NCP to TCP/IP.

□□□In 1984, the Domain Name System (DNS) was introduced. DNS resolves domain names (such as www.example.com) to IP addresses (such as 192.168.5.18).

□□□In 1995, Internet service providers (ISPs) began to offer Internet access to businesses and individuals.

□□□In 1996, the Hypertext Transfer Protocol (HTTP) was introduced. The World Wide Web uses HTTP.

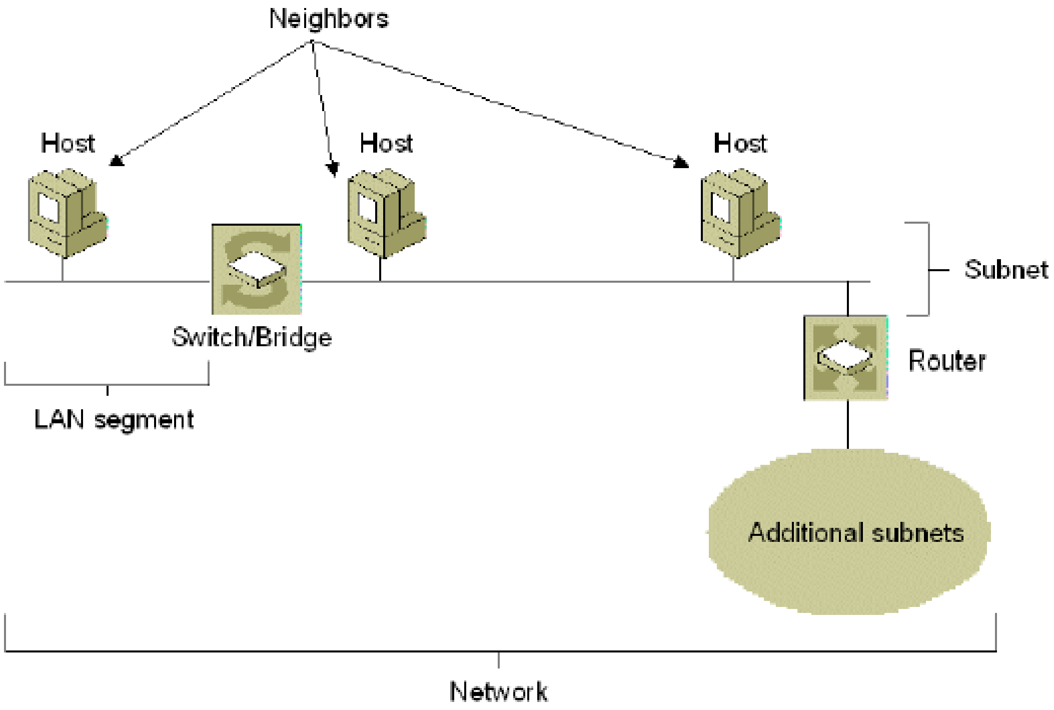
□□□In 1996, the first set of IP version 6 (IPv6) standards were published.

TCP/IP Terminology

The Internet standards use a specific set of terms when referring to network elements and concepts related to TCP/IP networking. These terms provide a foundation for subsequent chapters. Following figure illustrates the components of an IP network.

Common terms and concepts in TCP/IP are defined as follows:
□□□**Node** Any device, including routers and hosts, which runs an implementation of IP.

□□□**Router** A node that can forward IP packets not explicitly addressed to itself. On an IPv6 network, a router also typically advertises its presence and host configuration information.



□□□**Host** A node that cannot forward IP packets not explicitly addressed to itself (a non-router). A host is typically the source and the destination of IP traffic. A host silently discards traffic that it receives but that is not explicitly addressed to itself.

□□□**Upper-layer protocol** A protocol above IP that uses IP as its transport. Examples include Internet layer protocols such as the Internet Control Message Protocol (ICMP) and Transport layer protocols such as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). (However, Application layer protocols that use TCP and UDP as their transports are not considered upper-layer protocols. File Transfer Protocol [FTP] and Domain Name System [DNS] fall into this category).

□□□**LAN segment** A portion of a subnet consisting of a single medium that is bounded by bridges or Layer 2 switches.

□□□**Subnet** One or more LAN segments that are bounded by routers and use the same IP address prefix. Other terms for subnet are network segment and link.

□□□**Network** Two or more subnets connected by routers. Another term for network is internetwork.

□□□**Neighbor** A node connected to the same subnet as another node.

□□□**Interface** The representation of a physical or logical attachment of a node to a subnet. An example of a physical interface is a network adapter. An example of a logical interface is a tunnel interface that is used to send IPv6 packets across an IPv4 network.

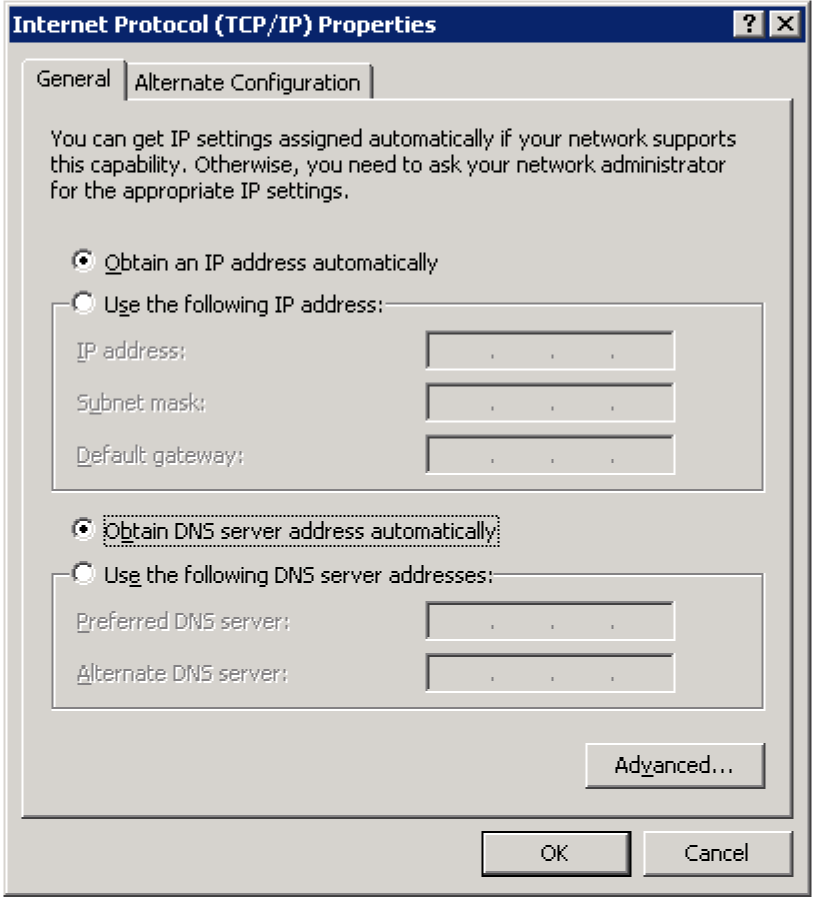
□□□**Address** An identifier that can be used as the source or destination of IP packets and that is assigned at the Internet layer to an interface or set of interfaces.

□□□**Packet** The protocol data unit (PDU) that exists at the Internet layer and comprises an IP header and payload.
Windows includes both an IPv4-based and an IPv6-based TCP/IP component.

Configuring the IPv4-based TCP/IP Component in Windows

The IPv4-based TCP/IP component in Windows Server 2003 and Windows XP is installed by default and appears as the Internet Protocol (TCP/IP) component in the Network Connections folder. Unlike in previous versions of Windows, you cannot uninstall the Internet Protocol (TCP/IP) component. However, you can restore its default configuration by using the **netsh interface ip reset** command. For more information about Netsh commands.

The Internet Protocol (TCP/IP) component can be configured to obtain its configuration automatically or from manually specified settings. By default, this component is configured to obtain an address configuration automatically.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 1-2 The General tab of the properties dialog box for the Internet Protocol (TCP/IP) component

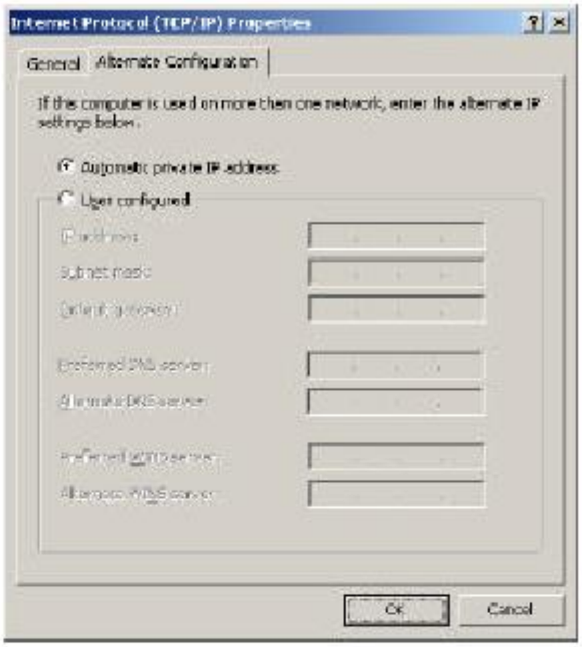
Properties dialog box.

Automatic Configuration

If you specify automatic configuration, the Internet Protocol (TCP/IP) component attempts to locate a Dynamic Host Configuration Protocol (DHCP) server and obtain a configuration when Windows starts.

Many TCP/IP networks use DHCP servers that are configured to allocate TCP/IP configuration information to clients on the network

If the Internet Protocol (TCP/IP) component fails to locate a DHCP server, TCP/IP checks the setting on the **Alternate Configuration** tab. Figure 1-3 shows this tab.



Internet Protocol (TCP/IP) Properties

If this computer is used on more than one network, enter the alternate IP settings below.

● Automatic private IP address

○ User configured

Figure 1-3 The Alternate Configuration tab of the Internet Protocol (TCP/IP) component

This tab contains two options:

□□□**Automatic Private IP Address** If you choose this option, Automatic Private IP Addressing (APIPA) is used. The Internet Protocol (TCP/IP) component automatically chooses an IPv4 address from the range169.254.0.1 to 169.254.255.254, using the subnet mask of 255.255.0.0. The DHCP client ensures that the IPv4 address that the Internet Protocol (TCP/IP) component has chosen is not already in use. If the address is in use, the Internet Protocol (TCP/IP) component chooses another IPv4 address and repeats this process for up to 10 addresses. When the Internet Protocol (TCP/IP) component has chosen an address that the DHCP client has verified as not in use, the Internet Protocol (TCP/IP) component configures the interface with this address. With APIPA, users on single-subnet Small Office/Home Office (SOHO) networks can use TCP/IP without having to perform manual configuration or set up a DHCP server. APIPA does not configure a default gateway. Therefore, only local subnet traffic is possible.

□□□**User Configured** If you choose this option, the Internet Protocol (TCP/IP) component uses the configuration that you specify. This option is useful when a computer is used on more than one network, not all of the networks have a DHCP server, and an APIPA configuration is not wanted. For example, you might want to choose this option if you have a laptop computer that you use both at the office and at home. At the office, the laptop uses a TCP/IP configuration from a DHCP server. At home, where no DHCP server is present, the laptop automatically uses the alternate manual configuration. This option provides easy access to home network devices and the Internet and allows seamless operation on both networks, without requiring you to manually reconfigure the Internet Protocol (TCP/IP) component. If you specify an APIPA configuration or an alternate manual configuration, the Internet Protocol (TCP/IP) component continues to check for a DHCP server in the background every 5 minutes. If TCP/IP finds a DHCP server, it stops using the APIPA or alternate manual configuration and uses the IPv4 address configuration offered by the DHCP server.

Manual Configuration

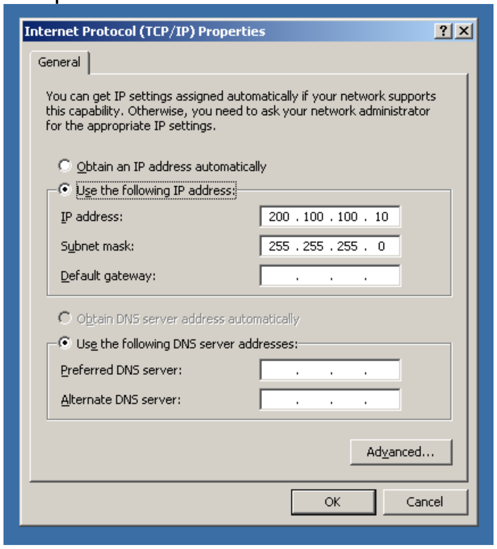
To configure the Internet Protocol (TCP/IP) component manually, also known as creating a static configuration, you must at a minimum assign the following:

□□□**IP address** An IP (IPv4) address is a logical 32-bit address that is used to identify the interface of an IPv4-based TCP/IP node. Each IPv4 address has two parts: the subnet prefix and the host ID. The subnet prefix identifies all hosts that are on the same physical network. The host ID identifies a host on the network. Each interface on an IPv4-based TCP/IP network requires a unique IPv4 address, such as 131.107.2.200.

□□□**Subnet mask** A subnet mask allows the Internet Protocol (TCP/IP) component to distinguish the
subnet prefix from the host ID. An example of a subnet mask is 255.255.255.0.

You must configure these parameters for each network adapter in the node that uses the Internet Protocol (TCP/IP) component. If you want to connect to nodes beyond the local subnet, you must also assign the IPv4 address of a default gateway, which is a router on the local subnet to which the node is attached. The Internet Protocol (TCP/IP) component sends packets that are destined for remote networks to the default gateway, if no other routes are configured on the local host. You can also manually configure the IPv4 addresses of primary and alternate DNS servers. The Internet Protocol (TCP/IP) component uses DNS servers to resolve names, such as www.example.com, to IPv4 or IPv6 addresses.

Figure 1-4 shows an example of a manual configuration for the Internet Protocol (TCP/IP) component.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 200 . 100 . 100 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Figure 1-4 An example of a manual configuration for the Internet Protocol (TCP/IP)

You can also manually configure the Internet Protocol (TCP/IP) using **netsh interface ip** commands at a command prompt.

Installing and Configuring the IPv6-based TCP/IP Component in Windows

Windows XP with Service Pack 1 (SP1) and Windows Server 2003 are the first versions of Windows to support IPv6 for production use. You install IPv6 as a component in Network Connections; the component is named Microsoft TCP/IP Version 6 in Windows Server 2003 and Microsoft IPv6 Developer Edition in Windows XP with SP1.

Note The Microsoft IPv6 Developer Edition component included in Windows XP with no service packs was intended for application developers only, not for use in production environments. Therefore, all of the Help topics for that version contain a disclaimer describing its limitations and supported uses. SP1 includes a version of IPv6 that is intended for production use. However, the Help topics were not updated for SP1. Therefore, you can disregard the disclaimer if you have installed SP1. Unlike the Internet Protocol (TCP/IP) component, the IPv6 component is not installed by default, and you can uninstall it. You can install the IPv6 component in the following ways:
□□□Using the Network Connections folder.

□□□Using the **netsh interface ipv6 install** command.
To install the IPv6 component in Windows Server 2003 using the Network Connections folder, do the following:
1. Click **Start**, point to **Control Panel**, and then double-click **Network Connections**.

2. Right -click any local area connection, and then click **Properties**.
3. Click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
5. In the **Select Network Protocol** dialog box, click **Microsoft TCP/IP Version 6**, and then click **OK**.
6. Click **Close** to save changes.

Unlike Internet Protocol (TCP/IP), the IPv6 component has no properties dialog box from which you can configure IPv6 addresses and settings. Configuration should be automatic for IPv6 hosts and manual for IPv6 routers.

Automatic Configuration

The Microsoft TCP/IP Version 6 component supports address auto configuration. All IPv6 nodes automatically create unique IPv6 addresses for use between neighboring nodes on a subnet. To reach remote locations, each IPv6 host upon startup sends a Router Solicitation message in an attempt to discover the local routers on the subnet. An IPv6 router on the subnet responds with a Router Advertisement message, which the IPv6 host uses to automatically configure IPv6 addresses, the default router, and other IPv6 settings.

Manual Configuration

You do not need to configure the typical IPv6 host manually. If a host does require manual configuration, use the **netsh interface ipv6** commands to add addresses or routes and configure other settings.

If you are configuring a computer running Windows XP with SP1 or Windows Server 2003 to be an IPv6 router, then you must use the **netsh interface ipv6** commands to manually configure the IPv6 component with address prefixes.

Chapter Glossary

address – An identifier that specifies the source or destination of IP packets and that is assigned at the IP layer to an interface or set of interfaces.

APIPA – See Automatic Private IP Addressing.

Automatic Private IP Addressing – A feature in Windows Server 2003 and Windows XP that automatically configures a unique IPv4 address from the range 169.254.0.1 through 169.254.255.254 and a subnet mask of 255.255.0.0. APIPA is used when the Internet Protocol (TCP/IP) component is configured for automatic addressing, no DHCP server is available, and the Automatic Private IP Address alternate configuration option is chosen.

host – A node that is typically the source and a destination of IP traffic. Hosts silently discard received packets that are not addressed to an IP address of the host.

interface – The representation of a physical or logical attachment of a node to a subnet. An example of a physical interface is a network adapter. An example of a logical interface is a tunnel interface that is used to send IPv6 packets across an IPv4 network.

IP – Features or attributes that apply to both IPv4 and IPv6. For example, an IP address is either an IPv4 address or an IPv6 address.

IPv4 – The Internet layer protocols of the TCP/IP protocol suite as defined in RFC 791. IPv4 is in widespread use today.

IPv6 – The Internet layer protocols of the TCP/IP protocol suite as defined in RFC 2460. IPv6 is gaining acceptance today.

LAN segment – A portion of a subnet that consists of a single medium that is bounded by bridges or Layer 2 switches.

neighbor – A node that is connected to the same subnet as another node.

network – Two or more subnets that are connected by routers. Another term for network is internetwork.

node – Any device, including routers and hosts, which runs an implementation of IP.

packet – The protocol data unit (PDU) that exists at the Internet layer and comprises an IP header and payload.

Request for Comments (RFC) - An official document that specifies the details for protocols included in the TCP/IP protocol suite. The Internet Engineering Task Force (IETF) creates and maintains RFCs for TCP/IP.

RFC – See Request for Comments (RFC).

router – A node that can be a source and destination for IP traffic and can also forward IP packets that are not addressed to an IP address of the router. On an IPv6 network, a router also typically advertises its presence and host configuration information.

subnet – One or more LAN segments that are bounded by routers and that use the same IP address prefix. Other terms for subnet are network segment and link.

TCP/IP – See Transmission Control Protocol/Internet Protocol (TCP/IP).
Transmission Control Protocol/Internet Protocol (TCP/IP) – A suite of networking protocols, including both IPv4 and IPv6, that are widely used on the Internet and that provide communication across interconnected networks of computers with diverse hardware architectures and various operating systems.

upper-layer protocol – A protocol above IP that uses IP as its transport. Examples of upper-layer protocols include Internet layer protocols such as the Internet Control Message Protocol (ICMP) and Transport layer protocols such as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

DHCP

Dynamic Host Configuration Protocol (DHCP) is an IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on your network. The Microsoft Windows Server 2003 family provides the DHCP service, which enables the server computer to perform as a DHCP server and configure DHCP-enabled client computers on your network as described in the current DHCP draft standard, RFC 2131. (Request for Comments (RFC)
An official document of the Internet Engineering Task Force (IETF) that specifies the details for protocols included in the TCP/IP family.

DHCP includes Multicast Address Dynamic Client Assignment Protocol (MADCAP) which is used to perform multicast address allocation. When registered clients are dynamically assigned IP addresses through MADCAP, they can participate efficiently in the data stream process, such as for real-time video or audio network transmissions.

Before installing a DHCP or MADCAP server

To install a DHCP server

Open **Windows Components Wizard**.
Under Components, scroll to and click **Networking Services**.
Click **Details**.

Under Subcomponents of Networking Services, click **Dynamic Host Configuration Protocol (DHCP),** and then click **OK.**

Click **Next**. If prompted, type the full path to the Windows Server 2003 distribution files, and then click **Next.**
Required files are copied to your hard disk.

Notes

> To open the Windows Components Wizard, click **Start**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
>
> DHCP servers must be configured with a static IP address.

Network Connections

Network Connections provides connectivity between your computer and the Internet, a network, or another computer. With Network Connections, you can configure settings to reach local or remote network resources or functions.

Network Connections combines Microsoft Windows NT version 4.0 Dial-Up Networking with features that were formerly located in the Network Control Panel, such as network protocol and service configuration. Each connection in the Network Connections folder contains a set of features that creates a link between your computer and another computer or network. By using Network Connections, performing a task, such as modifying a network protocol, is as easy as right-clicking a connection and then clicking **Properties**.

About Network Connections

Network Connections provides connectivity between your computer and the Internet, a network, or another computer. With Network Connections, you can gain access to network resources and functionality, whether you are physically located at the location of the network or in a remote location. Connections are created, configured, stored, and monitored from within the Network Connections folder.

Hardware requirements for network and dial-up connections

Depending on your configuration, you may need some or all of the following hardware:

- One or more network adapters with a Network Driver Interface Specification (NDIS) driver for LAN connectivity
- One or more compatible modems and an available COM port
- ISDN adapter (if you are using an ISDN line)
- DSL adapter
- X.25 adapter or PAD (if you are using X.25)
- Analog telephone line, ISDN line, X.25 line, or DSL line
- Smart card reader

- Wireless adapter

Using local area connections

Typically, computers running Windows are connected to a local area network (LAN). When you install Windows, your network adapter is detected, and a local area connection is created. It appears, like all other connection types, in the Network Connections folder. By default, a local area connection is always activated. A local area connection is the only type of connection that is automatically created and activated.

If you disable your local area connection, the connection is no longer automatically activated. Because your hardware profile remembers this, it accommodates your location-based needs as a mobile user. For example, if you travel to a remote sales office and use a separate hardware profile for that location that does not enable your local area connection, you do not waste time waiting for your network adapter to time out. The adapter does not even try to connect.

If your computer has more than one network adapter, a local area connection icon for each adapter is displayed in the Network Connections folder.

Examples of LAN connections include Ethernet, token ring, cable modems, DSL, FDDI, IP over ATM, IrDA (Infrared), wireless, and ATM-emulated LANs. Emulated LANs are based on virtual adapter drivers such as the LAN Emulation Protocol.

If changes are made to your network, you can modify the settings of an existing local area connection to reflect those changes. The **General** tab of the *Local Area Connection* **Status** dialog box allows you to view connection information such as connection status, duration, speed, signal strength, amounts of data transmitted and received, and any diagnostic tools available for a particular connection. The **Support** tab contains information on:

- The address type which indicates how the address was assigned. For example the TCP/IP address is assigned by DHCP.
- The IP address currently assigned for the session.
- The IP subnet mask for the IP address currently assigned for the session.
- The default gateway address of the IP device that allows access to other protocols.

The **Support** tab also has a **Details** button that displays detailed information about the properties of the network connection. This includes the addresses of dependent external devices.

If you install a new LAN adapter in your computer, the next time you start your computer, a new local area connection icon appears in the Network Connections folder. Plug and Play functionality finds the network adapter and creates a local area connection for it. If you are using a laptop computer, you can add a PC card while the computer is on. Plug and Play will identify the new card without you having to restart your laptop computer. The local area connection icon is immediately added to the folder. You cannot manually add local area connections to the Network Connections folder.

You can configure multiple LAN adapters through the **Advanced Settings** menu option. You can modify the order of adapters that are used by a connection, and the associated clients, services, and protocols for the adapter. You can modify the provider order in which this connection gains access to information on the network, such as networks and printers.

You configure the device a connection uses, and all of the associated clients, services, and protocols for the connection, through the **Properties** menu option. Clients define the access of the connection to computers and files on your network. Services provide features such as file and printer sharing. Protocols, such as TCP/IP, define the language your computer uses to communicate with other computers.

Depending on the status of your local area connection, the icon changes appearance in the Network Connections folder, or a separate icon appears in the taskbar. If a LAN adapter is not detected by your computer, a local area connection icon does not appear in the Network Connections folder.