

Module 3: Implementing Name Resolution by Using DNS

Contents

Overview	1
Multimedia: Basics of the Domain Name System (DNS)	2
Overview of the DNS Query Process	3
Installing the DNS Server Service	5
Configuring Name Resolution for Client Computers	7
Creating Zones	9
Configuring Zones	14
Lab A: Installing and Configuring the DNS Server Service	17
Configuring DNS for Internal Use	36
Integrating DNS and DHCP	37
Maintaining and Troubleshooting DNS Servers	43
Lab B: Maintaining and Troubleshooting a DNS Server	53
Review	64



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events 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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

This module provides students with the knowledge and skills necessary to install, configure, and troubleshoot the Domain Name System (DNS) in a Microsoft® Windows® 2000 network.

Labs:
90 Minutes

At the end of this module, students will be able to:

- Describe the DNS query process.
- Install the DNS Server service.
- Configure name resolution for client computers.
- Create zones.
- Configure zones.
- Configure DNS for internal use by configuring a root zone.
- Configure Dynamic Host Configuration Protocol (DHCP) for DNS integration.
- Maintain and troubleshoot DNS servers.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2153a_03.ppt
- Multimedia file PBSG_DNS.avi, *Basics of the Domain Name System (DNS)*

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- View the multimedia presentation, *Basics of the Domain Name System (DNS)*, under **Multimedia Presentations** on the Web page on the Trainer Materials compact disc.
- Complete the lab.
- Read the following RFCs under **Additional Reading** on the Web page on the Student Materials compact disc:
 - RFC 1034, *Domain Names-Concepts and Facilities*
 - RFC 1035, *Domain Names-Implementation and Specification*
 - RFC 1123, *Requirements for Internet Hosts-Application and Support*
 - RFC 1886, *DNS Extensions to Support IP Version 6*
 - RFC 1995, *Incremental Zone Transfer in DNS*
 - RFC 1996, *A Mechanism for Prompt DNS Notification of Zone Changes*
 - RFC 2136, *Dynamic Updates in the Domain Name System (DNS UPDATE)*
 - RFC 2181, *Clarifications to the DNS Specification*
 - RFC 2308, *Negative Caching of DNS Queries (DNS NCACHE)*
- Read the white paper, *Windows 2000 DNS*, under **Additional Reading** on the Web page on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Overview of the DNS Query Process

This topic expands on the DNS concepts that the multimedia presentation introduces. Describe the two types of queries that can be performed in DNS, and describe the lookup types that can be specified for DNS queries.

- Installing the DNS Server Service

This topic provides information about requirements and instructions for installing the Windows 2000 DNS Server service. Explain to students that they must configure a computer running Windows 2000 with a static Internet Protocol (IP) address prior to installing the DNS Server service. Explain the procedure for installing the DNS Server service. Emphasize that the Active Directory™ directory service relies on DNS for name resolution and for the location of Active Directory components in a network.

- Configuring Name Resolution for Client Computers

This topic provides information about how to configure clients to use a DNS server for name resolution. Explain to students that clients can be configured to use the DNS Server service by changing the Transmission Control Protocol/Internet Protocol (TCP/IP) settings on the client computer, and identify the different configuration options.

- Creating Zones

This topic provides information about how to create zones to divide the DNS namespace. Explain how to create a new zone, and describe the three types of zones that you can configure in DNS. Describe the purpose of the zone file, and then explain how to create forward and reverse lookup zones to enable clients to perform forward or reverse lookups.

- Configuring Zones

This topic provides information about the concepts and configuration options involved in configuring zones. Explain the procedures for configuring standard zones. Describe the zone transfer process, and then explain how to configure zone transfers. Describe the procedures for creating a subdomain to organize a zone and configuring an Active Directory integrated zone. Finally, explain how to migrate zones to the Windows 2000 DNS Server service.

- Configuring DNS for Internal Use

This topic provides information about how to configure DNS for internal use by configuring a root zone on a DNS server. Identify the circumstances in which it is necessary to configure a root zone, and describe the different configuration methods.

- Integrating DNS and DHCP

This topic provides information about how to integrate DNS and DHCP to enable DHCP servers and clients to update the DNS database with the names and IP addresses of client computers. Provide an overview of the dynamic update process by describing the dynamic update protocol and referring students to RFC 2136 for more information. Describe the dynamic update process for Windows 2000–based clients and for clients running previous versions of Windows. Emphasize that for clients running previous versions of Windows, the DHCP server must be configured to always update the DNS database on behalf of these clients.

Explain that to configure dynamic updates, you must configure the DNS and DHCP servers, and Windows 2000–based clients. Describe the options that are available for configuring the DNS server to allow dynamic updates. Do not discuss the **Only secure updates** option, as it is described in more detail in the next section. Demonstrate the procedures for configuring the DHCP Server for dynamic updates, and for configuring Windows 2000–based clients for dynamic updates.

Explain how to configure the DNS server to ensure that dynamic updates are secure. Emphasize that only Active Directory integrated zones can be configured for secure dynamic updates. Demonstrate the procedure for configuring secure dynamic updates.

- Maintaining and Troubleshooting DNS Servers

This topic provides information about how to maintain DNS and troubleshoot name resolution problems. Describe the utilities that are available for maintaining and troubleshooting DNS servers. Explain that a caching-only server can be configured to reduce traffic across a wide area network (WAN). Identify the different resource records that DNS servers can contain, and then explain how to maintain DNS zones by creating or modifying resource records. Describe the methods that are available for testing and monitoring the DNS Server service, and explain how to use the Nslookup utility to verify that resource records have been added or modified correctly. Finally, describe name resolution problems that may occur and explain how to resolve them.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Lab Setup

The lab in this module requires that you perform the procedure specified in the Classroom Setup Guide before performing the lab.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how to install, configure, and test the DNS Server service in Windows 2000.

- Overview of the DNS Query Process
- Installing the DNS Server Service
- Configuring Name Resolution for Client Computers
- Creating Zones
- Configuring Zones
- Configuring DNS for Internal Use
- Integrating DNS and DHCP
- Maintaining and Troubleshooting DNS Servers

*****ILLEGAL FOR NON-TRAINER USE*****

The Domain Name System (DNS) is an integral part of client/server communications in Internet Protocol (IP) networks. DNS is a distributed database that is used in IP networks to translate, or resolve, computer names into IP addresses. Microsoft® Windows® 2000 uses DNS as its primary method for name resolution.

Windows 2000–based clients use the DNS Server service for name resolution and to locate services, including domain controllers that provide user authentication.

At the end of this module, you will be able to:

- Describe the DNS query process.
- Install the DNS Server service.
- Configure name resolution for client computers.
- Create zones.
- Configure zones.
- Configure DNS for internal use by configuring a root zone.
- Configure Dynamic Host Configuration Protocol (DHCP) for DNS integration.
- Maintain and troubleshoot DNS servers.

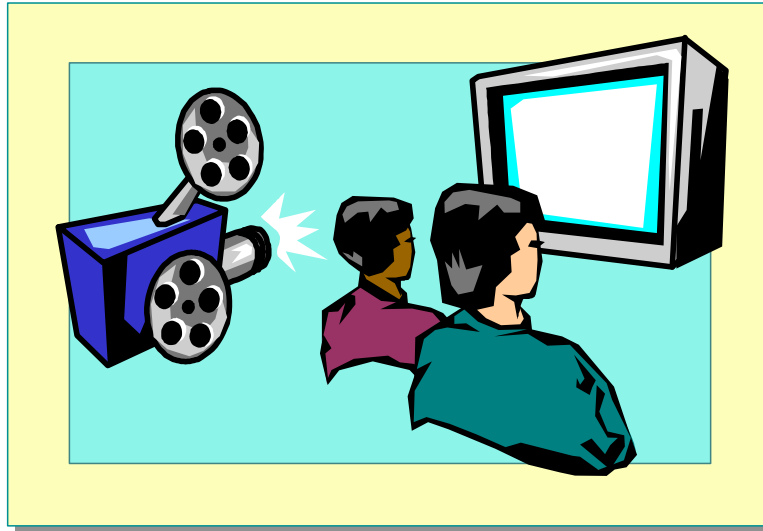
Multimedia: Basics of the Domain Name System (DNS)

Topic Objective

To introduce the multimedia presentation.

Lead-in

This multimedia presentation describes key components of DNS and how the name resolution process works. You must understand these concepts to effectively support a Windows 2000 network.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

When the multimedia presentation is finished, review the key points.

To run the Basics of the Domain Name System (DNS) multimedia presentation, open the Web page on the Trainer Materials compact disc, click **Multimedia Presentations**, and then click **Basics of the Domain Name System (DNS)**.

The estimated time to complete this multimedia presentation is eight minutes.

Inform students that a copy of the multimedia presentation is included on the Web page on the Student Materials compact disc.

Before you begin the process of installing and configuring the DNS Server service in Windows 2000, it is important to review some basic concepts of DNS.

Note The purpose of this presentation is to review basic DNS concepts prior to learning about the features in the Windows 2000 DNS Server service. To view the Basics of the Domain Name System (DNS) multimedia presentation, open the Web page on the Student Materials compact disc, click **Multimedia Presentations**, and then click **Basics of the Domain Name System (DNS)**.

Review the following key points after you view the multimedia presentation:

- DNS is a distributed database system that can serve as the foundation for name resolution in an IP network.
- The hierarchical structure of the domain namespace is such that the root domain is at the top of the domain structure and is represented by a period. Below the root domain, top-level domains can be represented by an organizational type, such as com or edu, or a geographic location, such as au for Australia. Second-level domains are registered to individuals or organizations and can have many subdomains.
- The fully qualified domain name (FQDN) describes the exact relation of a host to its domain. DNS uses the FQDN to resolve a host name to an IP address.
- The name-to-IP address data for computers that are located in a zone is stored in a zone file on a DNS server.
- A forward lookup query is a request to resolve a name to an IP address.
- When a client sends a forward lookup query to request an IP address from a domain for which the local DNS server does not have authority, the local DNS server sends a query to a DNS server that hosts the root zone.

Overview of the DNS Query Process

Topic Objective

To list the query types and lookup types, and their descriptions.

Lead-in

There are two types of queries that can be performed in DNS. Each query type can be associated with one of two lookup types.

Query Types	
Iterative Query	The DNS server returns the best answer that it can provide without help from other servers
Recursive Query	The DNS server returns a complete answer to the query, not a pointer to another DNS server
Lookup Types	
Forward Lookup	Requires name-to-address resolution
Reverse Lookup	Requires address-to-name resolution

*****ILLEGAL FOR NON-TRAINER USE*****

DNS uses a client/server model in which the DNS server contains information about a portion of the DNS namespace and provides this information to clients. A DNS client queries a DNS server for information about the DNS namespace. This server can, in turn, query other DNS servers to provide an answer to the query from the client.

When a DNS server receives a DNS request, it attempts to locate the requested information within its own database. If the request fails, further communication with other DNS servers is necessary.

Delivery Tip

Inform students that an iterative query is one in which the server returns the best answer that it can provide without help from other servers. If the server has the requested record, it is returned to the client; otherwise it returns pointers to servers that are more likely to have the answer.

A recursive query is one in which the server returns a complete answer to the query, not just a pointer to another server.

Query Types

There are two types of queries that can be performed in DNS:

- *Iterative.* A query made from a client to a DNS server in which the server returns the best answer that it can provide based on its cache or zone data. If the queried server does not have an exact match for the request, it provides a pointer to an authoritative server in a lower level of the domain namespace. The client then queries the authoritative server to which it was referred. The client continues this process until it locates a server that is authoritative for the requested name, or until an error occurs or time-out condition is met.
- *Recursive.* A query made from a client to a DNS server in which the server assumes the full workload and responsibility for providing a complete answer to the query. The server will then perform separate iterative queries to other servers (on behalf of the client) to assist in answering the recursive query.

Query Process

Delivery Tip

Use the white board to illustrate the query process that takes place when a client computer generates a request for the IP address of `www.microsoft.com`

Client computers typically send recursive queries to DNS servers. The DNS servers then use iterative queries to provide an answer to the client. For example, when a client computer issues a request to a DNS server to resolve the address `www.microsoft.com`, the following process takes place:

1. The client computer generates a request for the IP address of `www.microsoft.com` by sending a recursive query to the DNS server that it is configured to use.
2. The DNS server that received the recursive query is unable to locate an entry for `www.microsoft.com` in its database, so it sends an iterative query to a DNS server that is authoritative for the root domain.
3. The DNS server that is authoritative for the root domain is unable to locate an entry for `www.microsoft.com` in its database, so it sends a reply to the querying DNS server with the IP addresses of DNS servers that are authoritative for the `com` domain.
4. The DNS server that received the recursive query sends an iterative query to a server that is authoritative for the `com` domain.
5. The DNS server that is authoritative for the `com` domain is unable to locate an entry for `www.microsoft.com` in its database, so it sends a reply to the querying DNS server with the IP addresses of DNS servers that are authoritative for the `microsoft.com` domain.
6. The DNS server that received the recursive query sends an iterative query to a server that is authoritative for the `microsoft.com` domain.
7. The DNS server that is authoritative for the `microsoft.com` domain locates an entry for `www.microsoft.com` in its database and sends a reply to the querying DNS server with the IP address of `www.microsoft.com`.
8. The DNS server that received the recursive query sends a reply to the client computer with the IP address of `www.microsoft.com`.

Lookup Types

Delivery Tip

Describe the difference between forward lookup and reverse lookup.

The zone lookup type determines the tasks that a DNS server will perform. When you create a zone, you specify whether the zone will be used for resolving forward or reverse lookup queries by specifying the zone type. Iterative and recursive queries can be associated with either of the following lookup types:

- *Forward lookup.* A request to map a name to an IP address. This is the most common type of lookup, and is used to locate a server's IP address so that a connection can be made to it. This type of request requires name-to-address resolution.
- *Reverse lookup.* A request to map an IP address to a name. This is most commonly used when you know an IP address, but you want to know the domain name that is associated with the IP address. For example, if you monitor IP connections that are made to a server, you can use a reverse lookup to locate the domain name associated with the IP address of the connecting computer. This type of request requires address-to-name resolution.

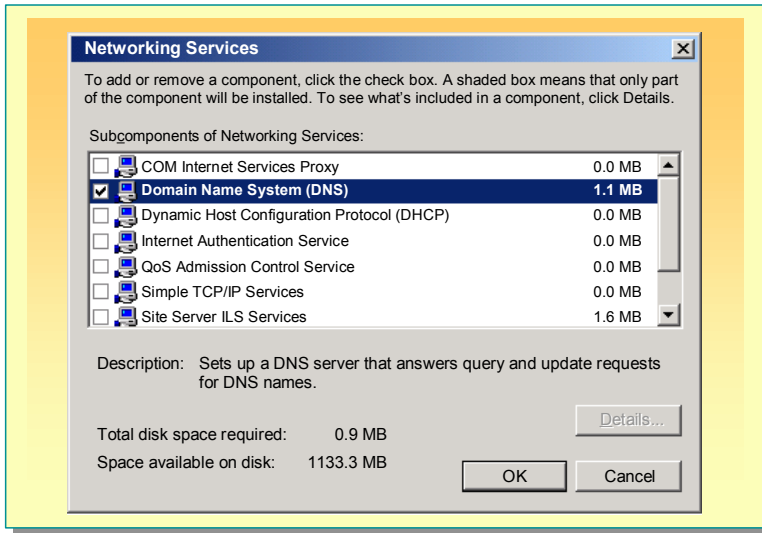
Installing the DNS Server Service

Topic Objective

To illustrate the **Networking Services** page in the Windows Components wizard.

Lead-in

Before you install the DNS Server service on a computer running Windows 2000, you must configure the computer with a static IP address.



*****ILLEGAL FOR NON-TRAINER USE*****

You create a DNS server by installing the DNS Server service on a computer running Windows 2000 Server.

Computers running Windows 2000 are configured to receive Transmission Control Protocol/Internet Protocol (TCP/IP) configuration information from a DHCP server by default. You must configure TCP/IP with a static IP address before you install the DNS Server service.

Configuring TCP/IP

To configure TCP/IP, you must assign a static IP address in the **Internet Protocol (TCP/IP) Properties** dialog box on the computer on which you are installing the DNS Server service.

Microsoft also recommends that you configure the domain name on the computer on which you are installing the DNS Server service.

To configure the domain name:

1. Open the **Properties** dialog box for the network connection that you are configuring.
2. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced**.
4. On the **DNS** tab of the **Advanced TCP/IP Settings** dialog box, verify that the DNS address in the **DNS server addresses, in order of use** box is correct.
5. Type the domain name in the **DNS suffix for this connection** box, and then click **OK**.

Delivery Tip

Explain how to configure TCP/IP and the domain name on the computer on which you are installing the DNS server service.

DNS Server Service Installation Process

Delivery Tip

Describe the procedure for installing the DNS Server service.

To install the DNS Server service:

1. In Control Panel, click **Add/Remove Programs**, and then click **Add/Remove Windows Components**.
2. On the **Windows Components** page of the Windows Components wizard, click **Networking Services**, and then click **Details**.
3. Select the **Domain Name System (DNS)** check box, and then click **OK**.
4. Click **Next**, and then click **Finish** to complete the Windows Components wizard.

Note The Active Directory™ directory service relies on DNS for name resolution and for the location of Active Directory components in a network. You must configure the DNS infrastructure prior to installing Active Directory or let Active Directory automatically configure the DNS server.

Configuring Name Resolution for Client Computers

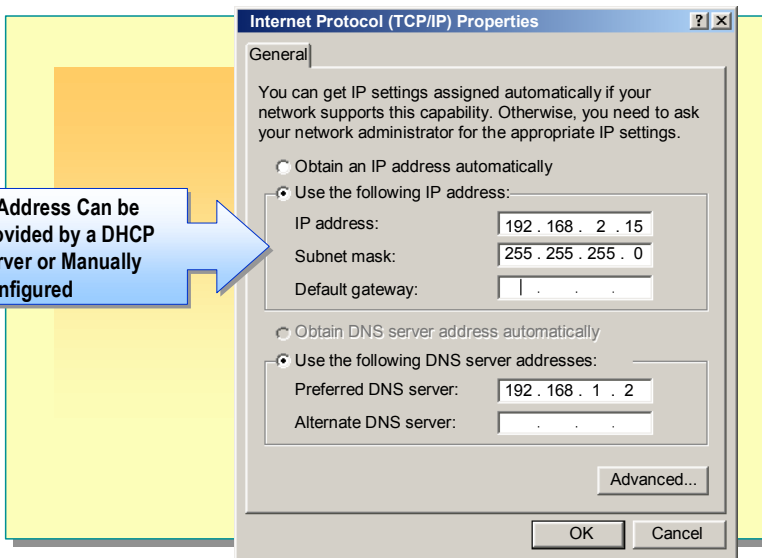
Topic Objective

To illustrate the TCP/IP settings for configuring a DNS client.

Lead-in

You configure clients to use the DNS Server service by changing the TCP/IP settings on the client computer.

IP Address Can be Provided by a DHCP Server or Manually Configured



*****ILLEGAL FOR NON-TRAINER USE*****

A DNS client uses a DNS server to resolve queries and locate resources on IP networks. In Windows 2000, configuring a computer as a DNS client involves only one configuration parameter: the IP address of the DNS server.

Note The networking component that performs DNS lookups is sometimes referred to as a *resolver*.

Delivery Tip

Describe the procedure for configuring a client to use a DNS server for name resolution.

Configuring Client Computers

To configure a client to use a DNS server for name resolution, open the **Properties** dialog box for the connection, and then open the **Internet Protocol (TCP/IP) Properties** dialog box:

- If you want DNS server addresses to be provided by a DHCP server, click **Obtain DNS server address automatically**.
- If you want to manually configure an IP address for a DNS server, click **Use the following DNS server addresses**. Type the IP address of the primary server in the **Preferred DNS server** box. If you are configuring a second DNS server, type the IP address of the additional DNS server in the **Alternate DNS server** box.

Note Windows 2000 uses the second (or alternate) DNS server only when it cannot contact the primary DNS server.

Configuring the Hosts file

A *Hosts file* is a text file that contains static mappings of host names to IP addresses. Before DNS became the Internet standard for name resolution services, computer names were mapped to IP addresses by using Hosts files. Windows 2000 can use a local Hosts file for name resolution, which provides a faster response to DNS queries because the Hosts file is queried before any DNS servers.

You must update the Hosts file manually, because the mappings in the Hosts file are not dynamic. In Windows 2000, you can use any text editor to edit the Hosts file, which is located in the `\systemroot\system32\drivers\etc` folder.

◆ Creating Zones

Topic Objective

To list the topics that are related to creating zones.

Lead-in

You can divide the DNS namespace into zones, which store name information about one or more DNS domains. Use the New Zone wizard to create a zone.

- Identifying Zone Types
- Examining the Zone File
- Creating Lookup Zones

*****ILLEGAL FOR NON-TRAINER USE*****

A *zone* is a contiguous portion of the domain namespace for which a DNS server has authority to resolve DNS queries. You can divide the DNS namespace into zones, which store name information about one or more DNS domains or portions of a DNS domain. For each DNS domain name included in a zone, the zone becomes the authoritative source for information about that domain.

Before you create zones, you must understand the following concepts:

Key Points

A DNS server can host multiple zones and different types of zones.

The zone file contains the resource records that are used for name resolution.

Use the New Zone wizard to create a zone.

- *Zone types.* DNS servers can host different types of zones. To limit the number of DNS servers on your network, you can configure a single DNS server to support, or host, multiple zones. You can also configure multiple servers to host one or more zones to provide fault tolerance and distribute the name resolution and administrative workloads.
- *Zone file.* The resource records that are stored in a zone file define a zone. The zone file stores information that is used to resolve host names to IP addresses and IP addresses to host names. If you use Active Directory-integrated zones, you can also store zone information in Active Directory, not only in zone files on a DNS server.

Important To create zones and administer a DNS server that is not running on a domain controller, you must be a member of the Administrators group on that computer. To configure a DNS server that is running on a domain controller, you must be a member of the DNSAdmins, Domain Admins, or Enterprise Admins groups.

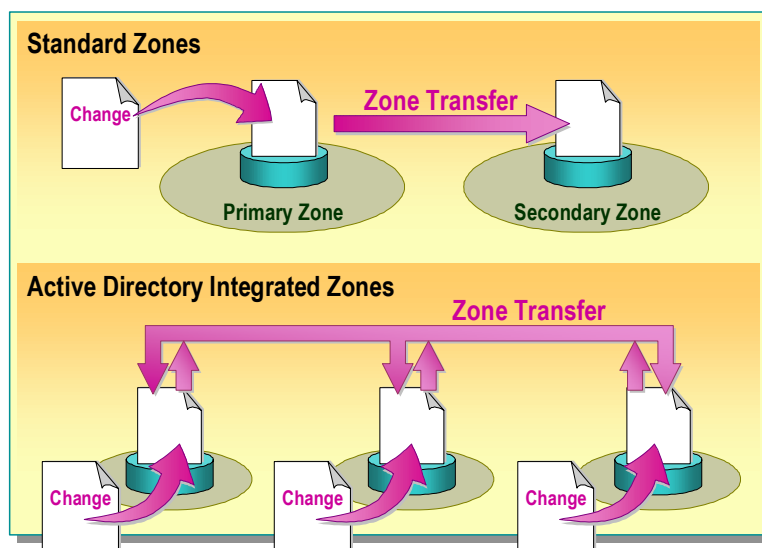
Identifying Zone Types

Topic Objective

To illustrate the difference between Standard zones and Active Directory integrated zones.

Lead-in

You can configure three types of zones in DNS: Standard primary, Standard secondary, and Active Directory integrated zones.



*****ILLEGAL FOR NON-TRAINER USE*****

The following table describes the three types of zones that you can configure, and the zone files associated with them.

Zone type	Description
Standard primary	Contains a read/write version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in that file. You must create a standard primary zone each time you create a new zone.
Standard secondary	Contains a read-only version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in the primary zone file and replicated to the secondary zone file. Create a standard secondary zone to create a copy of an existing zone and its zone file. This allows the name resolution workload to be distributed among multiple DNS servers.
Active Directory integrated	Stores the zone information in Active Directory, rather than a text file. Updates to the zone occur automatically during Active Directory replication. Create an Active Directory integrated zone to simplify planning and configuration of a DNS namespace. You do not need to configure DNS servers to specify how and when updates occur because Active Directory maintains zone information.

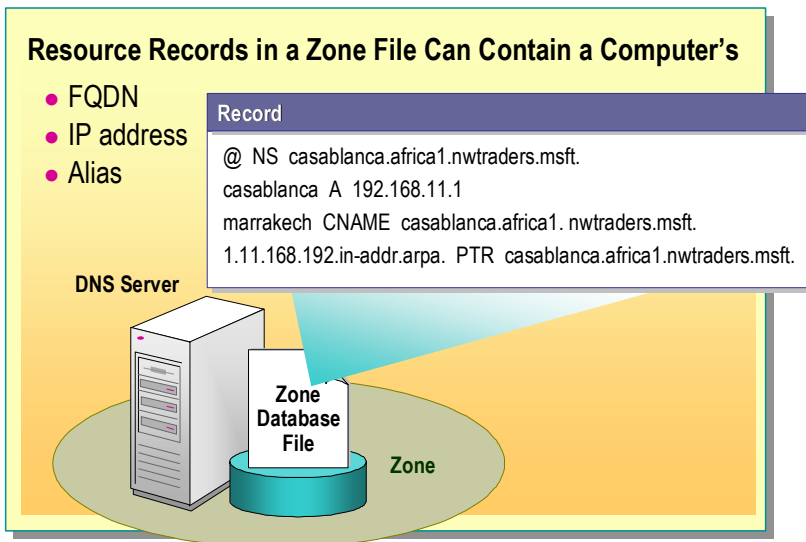
Examining the Zone File

Topic Objective

To highlight some of the attributes that are included in a resource record, which is contained in a zone file.

Lead-in

DNS servers use zone files to locate the information that they need to perform name resolution.



*****ILLEGAL FOR NON-TRAINER USE*****

Zone files contain the necessary information that a DNS server references to perform two different tasks: resolving host names to IP addresses or resolving IP addresses to host names. This information is stored as resource records that populate the zone file.

A zone file contains the name resolution data for a zone, including resource records that contain information for answering DNS queries. *Resource records* are database entries that contain various attributes, such as the host name or the FQDN of a computer, an IP address, or an alias.

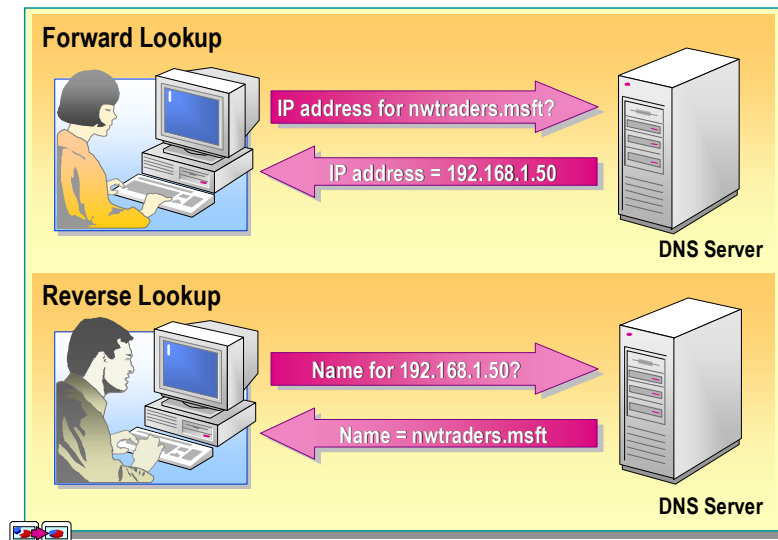
Creating Lookup Zones

Topic Objective

To illustrate the forward and reverse lookup processes.

Lead-in

You can enable clients to perform forward or reverse lookups by creating a forward or a reverse lookup zone.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

In most DNS lookups, clients typically perform a forward lookup, which is a request to map a computer name to an IP address. DNS also provides a reverse lookup process, which enables clients to request a computer name based on the computer's IP address.

Creating a Forward Lookup Zone

To create a forward lookup zone, click **Forward lookup** on the **Select the Zone Lookup Type** page of the New Zone wizard. The wizard guides you through the process of naming the zone and the zone file. The wizard automatically creates the zone, the zone file, and the necessary resource records for the DNS server on which you create the zone.

Creating a Reverse Lookup Zone

To create a reverse lookup zone, click **Reverse lookup** on the **Select the Zone Lookup Type** page of the New Zone wizard. The wizard guides you through the process of specifying the network identification or zone name, and verifying the name of the zone file based on the network identification information. The wizard automatically creates the zone, the zone file, and the necessary resource records for the DNS server on which you create the zone.

The in-addr.arpa domain is a special top-level DNS domain that is reserved for reverse mapping of IP addresses to DNS host names. To create the reverse namespace, you form subdomains within the in-addr.arpa domain by using the reverse ordering of the numbers in the dotted-decimal notation of IP addresses.

Delivery Tip

Explain that the New Zone wizard automatically adds the in-addr.arpa suffix to the reverse lookup zone name.

To comply with RFC standards, the reverse lookup zone name requires the in-addr.arpa domain suffix. When you create a reverse lookup zone, the in-addr.arpa suffix is automatically appended to the end of the network identification. For example, if the network uses the class B network identifier of 172.16.0.0, the reverse lookup zone name becomes 16.172.in-addr.arpa.

Note For more information about the in-addr.arpa domain suffix, see RFC 2317 under **Additional Reading** on the Web page on the Student Materials compact disc.

◆ Configuring Zones

Topic Objective

To introduce the concepts and configuration options that are involved in configuring a zone.

Lead-in

Zone information is stored in a zone file, and you can configure a zone in several ways.

- **Configuring Standard Zones**
- **Zone Transfer Process**
- **Configuring Zone Transfers**
- **Creating a Subdomain**
- **Configuring Active Directory Integrated Zones**
- **Migrating Zones to the Windows 2000 DNS Server service**

*****ILLEGAL FOR NON-TRAINER USE*****

A zone is defined by the information that is stored in the zone file on the DNS server. DNS servers reference this information to perform name resolution.

You must configure a zone to enable the authoritative DNS server to provide name resolution for DNS clients and other DNS servers. When you configure a zone, you determine the type of zone file that is stored on a DNS server, in addition to how the zone file is updated.

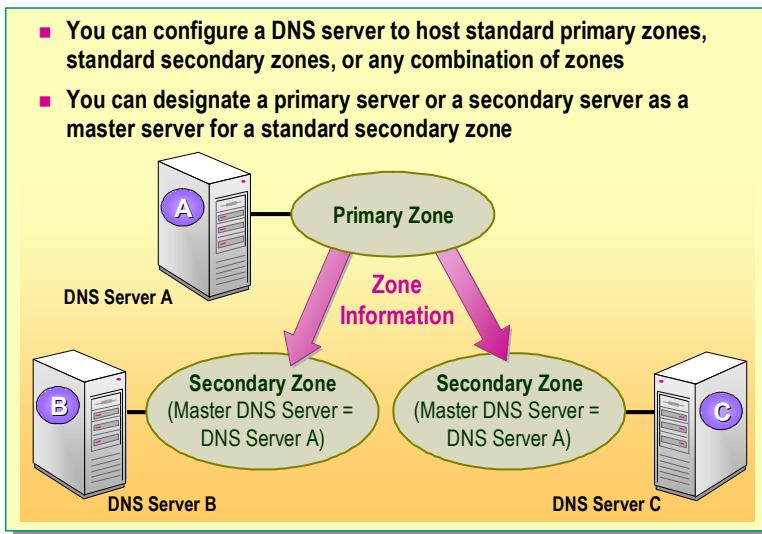
Configuring Standard Zones

Topic Objective

To illustrate primary and secondary zones, and the concept that both types of zones can be designated as master servers.

Lead-in

You can configure standard zones as primary or secondary. A standard primary zone contains the master copy of a zone file, whereas a standard secondary zone is a replica of an existing zone file.



*****ILLEGAL FOR NON-TRAINER USE*****

For each zone, the server that maintains the standard primary zone files is called the *primary server*, and the servers that host the standard secondary zone files are called *secondary servers*. A DNS server can host the standard primary zone file (as the primary server) for one zone and the standard secondary zone file (as the secondary server) for another zone.

You can configure a single DNS server or multiple DNS servers to host:

- One or more standard primary zones.
- One or more standard secondary zones.
- Any combination of standard primary and standard secondary zones.

Key Point

You must create a standard primary zone before creating a standard secondary zone.

Note You must create a standard primary zone before you can create a standard secondary zone.

Key Points

The server that contains the standard secondary zone receives updated zone files from a master server.

The master server is configured to notify secondary servers of modifications to the zone file.

Specifying a Master DNS Server for a Secondary Zone

When you add a standard secondary zone, you must designate a DNS server from which to obtain the zone information. The designated server is referred to as a *master DNS server*. A master DNS server transfers zone information to the secondary DNS server. You can designate a primary server or another secondary server as a master DNS server for a standard secondary zone.

Specifying a Master DNS Server

To specify a master DNS server, on the **Master Servers** page of the New Zone wizard, type the IP address of the master server in the **IP address** box, and then click **Add**.

Specifying Multiple Master DNS Servers

To specify more than one master DNS server, use the same procedure to add additional master DNS server IP addresses to the list. You can sort the list into the order in which you want the master DNS servers to be contacted. To sort the list, click an IP address, and then click **Up** or **Down**.

Lab A: Installing and Configuring the DNS Server Service

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will install the DNS Server service, configure a DNS client, and create standard primary zones.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install the DNS Server service.
- Delegate authority for a domain.
- Create forward and reverse lookup zones.
- Enable dynamic updates.

Prerequisite

Before working on this lab, you must be familiar with DNS concepts and operations.

Lab Setup

To complete this lab, you need the following:

- A computer running Microsoft Windows 2000 Advanced Server that is configured as a domain controller.
- A static IP address and subnet mask.
- A lab partner. One partner will create the primary zone; the other will create a secondary zone and designate his or her partner's computer as the master DNS server.
- An FQDN. Refer to the Student Computer IP Addresses and FQDNs section of the lab for this information.
- The IP address of the instructor computer. This is 192.168.z.200, where *z* is the assigned classroom number.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Student Computer IP Addresses and FQDNs

The following table provides the IP address and FQDN of each student computer in the fictitious domain nwtraders.msft.

Find the student number that the instructor has assigned to you, and make a note of the IP address (where *x* is the assigned classroom number) and FQDN for your student number.

Student number	IP address	FQDN
1	192.168.x.1	vancouver.namerica1.nwtraders.msft
2	192.168.x.2	denver.namerica1.nwtraders.msft
3	192.168.x.3	perth.spacific1.nwtraders.msft
4	192.168.x.4	brisbane.spacific1.nwtraders.msft
5	192.168.x.5	lisbon.europe1.nwtraders.msft
6	192.168.x.6	bonn.europe1.nwtraders.msft
7	192.168.x.7	lima.samerica1.nwtraders.msft
8	192.168.x.8	santiago.samerica1.nwtraders.msft
9	192.168.x.9	bangalore.asia1.nwtraders.msft
10	192.168.x.10	singapore.asia1.nwtraders.msft
11	192.168.x.11	casablanca.africa1.nwtraders.msft
12	192.168.x.12	tunis.africa1.nwtraders.msft
13	192.168.x.13	acapulco.namerica2.nwtraders.msft
14	192.168.x.14	miami.namerica2.nwtraders.msft
15	192.168.x.15	auckland.spacific2.nwtraders.msft
16	192.168.x.16	suva.spacific2.nwtraders.msft
17	192.168.x.17	stockholm.europe2.nwtraders.msft
18	192.168.x.18	moscow.europe2.nwtraders.msft
19	192.168.x.19	caracas.samerica2.nwtraders.msft
20	192.168.x.20	montevideo.samerica2.nwtraders.msft
21	192.168.x.21	manila.asia2.nwtraders.msft
22	192.168.x.22	tokyo.asia2.nwtraders.msft
23	192.168.x.23	khartoum.africa2.nwtraders.msft
24	192.168.x.24	nairobi.africa2.nwtraders.msft

Scenario

Your company, Northwind Traders, is migrating to Windows 2000, and part of that migration involves configuring DNS domains for use across the organization. Your company domain name is nwtraders.msft, and the different geographic regions in your company have been assigned subdomains.

Estimated time to complete this lab: 45 minutes

Exercise 1

Installing the DNS Server Service

Scenario

Your organization currently has DNS servers installed to manage the zones for your domain, nwtraders.msft. You are responsible for installing and configuring the DNS servers for your subdomain, and these servers will host your regional subdomain.

Goal

In this exercise, you will configure the domain name of your computer and install the DNS Server service.

Tasks	Detailed Steps
1. Install the DNS Server service.	- Log on as administrator@<i>domain</i>.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - In Control Panel, double-click Add/Remove Programs, and then click Add/Remove Windows Components.
 Important: In the following detailed step, click the text Networking Services rather than the check box to avoid selecting all options under Networking Services .	
1. (continued)	- In the Windows Components wizard, on the Windows Components page, under Components, click Networking Services, and then click Details. - In the Networking Services dialog box, select the Domain Name System (DNS) check box, and then click OK. - In the Windows Components wizard, click Next. - If the Files Needed dialog box appears, type \\London\Setup\Winsrc and then click OK. - When the configuration process is complete, click Finish, and then close all open windows.

Exercise 2

Delegating Authority for a Domain

Scenario

You are going to create a new subdomain for your region, and this subdomain will be hosted on your server. So that the DNS hierarchy will be able to locate your domain, you must now delegate authority from the parent domain, *nwtraders.msft*, to your domain.

Goal

In this exercise, you will delegate authority from the instructor DNS server to the student DNS server that will host the primary zone for the new subdomain.

Tasks	Detailed Steps
 Perform the following procedure on the computer of the partner with the lower student number.	
1. Add the instructor's DNS server to your DNS console.	- Click Start, point to Programs, point to Administrative Tools, right-click DNS, and then click Run as. - In the Run As Other User dialog box, type eadmin@nwtraders.msft in the User name box, type password in the Password box, delete the contents of the Domain box, and then click OK. - In the console tree, right-click DNS, and then click Connect To Computer. - In the Select Target Computer dialog box, click The following computer, type London in the text box, and then click OK.
2. Delegate authority for <i>domain.nwtraders.msft</i> to your DNS server.	- In the console tree, expand London, expand Forward Lookup Zones, and then expand nwtraders.msft. - In the console tree, right-click nwtraders.msft, and then click New Delegation. - On the Welcome to the New Delegation Wizard page, click Next. - On the Delegated Domain Name page, in the Delegated domain box, type <i>domain</i> (where <i>domain</i> is the name of your domain), and then click Next. - On the Name Servers page, click Add. - In the New Resource Record dialog box, in the Server name box, type the FQDN of your computer, click Resolve, and then click OK. - On the Name Servers page, click Add. - In the New Resource Record dialog box, in the Server name box, type the FQDN of your partner's computer, click Resolve, and then click OK. - On the Name Servers page, click Next. - On the Completing the New Delegation Wizard page, click Finish.

Exercise 3

Creating Forward and Reverse Lookup Zones

Scenario

Now that you have delegated authority for your subdomain to your server, you must create the lookup zones to host the DNS records for your subdomain.

Goal

In this exercise, you will create forward and reverse lookup zones.

Tasks	Detailed Steps
 Perform the following procedure on the computer of the partner with the lower student number.	
1. Add a standard primary forward lookup zone for <i>domain.nwtraders.msft</i>	- In the console tree, click <i>server</i> (where <i>server</i> is your computer name), right-click <i>server</i>, and then click Configure the server. - On the Welcome to the Configure DNS Server Wizard page, click Next. - On the Forward Lookup Zone page, ensure that Yes, create a forward lookup zone is selected, and then click Next. - On the Zone Type page, verify that Standard primary is selected, and then click Next. - On the Zone Name page, in the Name box, type <i>domain.nwtraders.msft</i> (where <i>domain</i> is the name of your domain), and then click Next. - On the Zone File page, verify that Create a new file with this file name is selected, and then click Next.
2. Add a standard secondary reverse lookup zone for your subnet.	- On the Reverse Lookup Zone page, verify that Yes, create a reverse lookup zone is selected, and then click Next. - On the Zone Type page, click Standard secondary, and then click Next. - On the Reverse Lookup Zone page, in the Network ID box, type the first three octets of the IP address of your Classroom connection, and then click Next. (For example, if your Classroom adapter has an IP address of 192.168.1.1, type 192.168.1) - On the Master DNS Servers page, in the IP address box, type the IP address of the instructor computer, click Add, and then click Next. - On the Completing the Configure DNS Server Wizard page, click Finish.
 Perform the following procedure on the computer of the partner with the higher student number.	

(continued)

Tasks	Detailed Steps
3. Add a standard secondary forward lookup zone for <i>domain.nwtraders.msft</i> and a standard secondary reverse lookup zone for your subnet.	a. Open DNS from the Administrative Tools menu. b. Right-click <i>server</i> (where <i>server</i> is your computer name), and then click Configure the server. c. On the Welcome to the Configure DNS Server Wizard page, click Next. d. On the Forward Lookup Zone page, verify that Yes, create a forward lookup zone is selected, and then click Next. e. On the Zone Type page, click Standard secondary, and then click Next. f. On the Zone Name page, type <i>domain.nwtraders.msft</i> (where <i>domain</i> is the name of your domain), and then click Next. g. On the Master DNS Servers page, in the IP address box, type the IP address of your partner's Classroom connection, click Add, and then click Next. h. On the Reverse Lookup Zone page, verify that Yes, create a reverse lookup zone is selected, and then click Next. i. On the Zone Type page, click Standard secondary, and then click Next. j. On the Reverse Lookup Zone page, in the Network ID box, type the first three octets of the IP address of your Classroom connection, and then click Next. (For example, for an IP address of 192.168.1.1, type 192.168.1) k. On the Master DNS Servers page, in the IP address box, type the IP address of the instructor's computer, click Add, and then click Next. l. On the Completing the Configure DNS Server Wizard page, click Finish. m. Close DNS.

Exercise 4

Enabling Dynamic Update

Scenario

You want DHCP and client computers to update DNS records automatically to decrease the administrator's workload.

Goal

In this exercise, you will enable dynamic update on the DNS server.

Tasks	Detailed Steps
 Perform the following procedure on the computer of the partner with the lower student number.	
1. Enable dynamic update on the forward lookup zone for <i>domain.nwtraders.msft</i> .	- In the console tree, expand <i>server</i> (where <i>server</i> is your computer name), expand Forward Lookup Zones, and then click <i>domain.nwtraders.msft</i> (where <i>domain</i> is the name of your domain). - Right-click <i>domain.nwtraders.msft</i> (where <i>domain</i> is the name of your domain), and then click Properties. - In the <i>domain.nwtraders.msft Properties</i> box, in the Allow dynamic updates box, click Yes, and then click OK. - Close DNS.
 Perform the following procedure on the computer with the higher student number.	
2. Configure the secondary zone <i>domain.nwtraders.msft</i> to allow zone transfers.	- Open DNS from the Administrative Tools menu. - In the console tree, expand <i>server</i>, expand Forward Lookup Zones, and then click <i>domain.nwtraders.msft</i>. - Right-click <i>domain.nwtraders.msft</i>, and then click Properties. - On the Zone Transfers tab, click Allow zone transfers, and then click OK. - Close DNS.
 Perform the following procedure on both student computers.	

(continued)

Tasks	Detailed Steps
3. Configure the TCP/IP properties for both adapters so that your computer is a client of the DNS Server service on your computer.	a. Right-click My Network Places, and then click Properties. b. Open the Properties dialog box for the Classroom connection. c. Click Internet Protocol (TCP/IP), and then click Properties. d. In the Internet Protocol (TCP/IP) Properties dialog box, verify that Use the following DNS server addresses is selected, type the IP address of your Classroom connection in the Preferred DNS server box, and then click OK. e. Click OK to close the Classroom Properties dialog box. f. Repeat steps b through e to change the DNS server address for the PartnerNet connection. g. Close all open windows, and then log off.

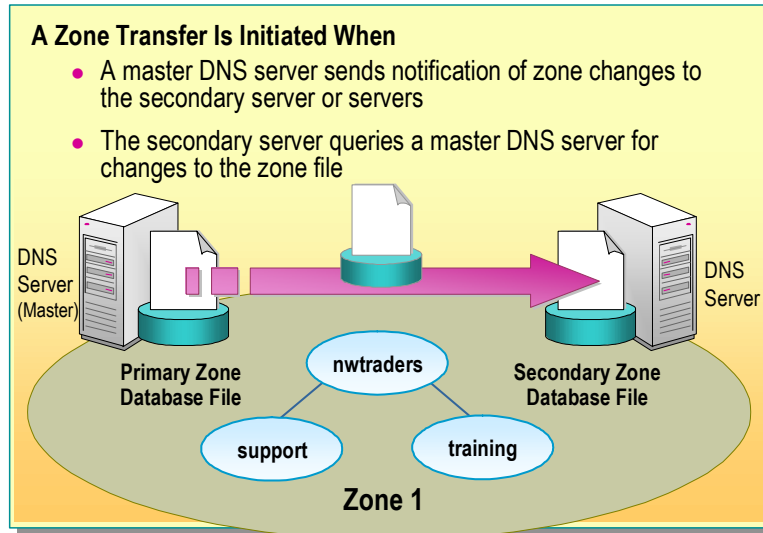
Zone Transfer Process

Topic Objective

To illustrate the zone transfer process.

Lead-in

Zone transfer is the process by which DNS servers interact to maintain and synchronize zone files.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

To provide fault tolerance, store zone data on more than one DNS server.

The zone transfer process ensures that zone data is up-to-date on all of the DNS servers that are configured to host the zone.

To provide availability and fault tolerance when resolving name queries, zone data should be available from more than one DNS server on a network. For example, if a single DNS server is used and that server is not responding, name queries will fail. When more than one server is configured to host a zone, zone transfers are required to replicate and synchronize zone data among all of the servers that are configured to host the zone.

Zone Transfer

Zone transfer is the process of replicating a zone file to another DNS server. Zone transfers occur when names and IP address mappings change within your domain. When this happens, the changes to the zone are copied from a master server to its secondary servers.

Incremental Zone Transfer

In Windows 2000, zone information is updated by *incremental zone transfer (IXFR)*, which only replicates changes to the zone file, instead of replicating the entire zone file. DNS servers that do not support IXFR request the entire contents of a zone file when they initiate a zone transfer.

Note For more information about IXFR, see RFC 1995 under **Additional Reading** on the Web page on the Student Materials compact disc.

The zone transfer process begins when one of the following occurs:

- A master server sends a notification of a change in the zone to one or more secondary servers. When the secondary server receives the notification, it queries the master server for the changes.
- Each secondary server periodically queries a master server for changes to the zone file, even if the secondary servers have not been notified of a change. This occurs when the DNS Server service on the secondary server starts, or when the refresh interval on the secondary server expires.

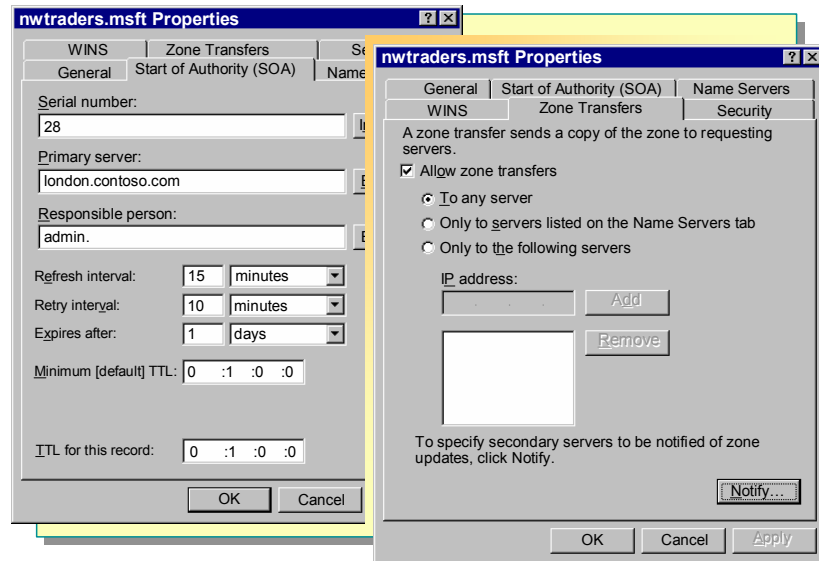
Configuring Zone Transfers

Topic Objective

To illustrate the user interface for configuring zone transfers.

Lead-in

You can modify the SOA resource record to configure how often zone transfers occur. You can also modify zone properties to enable zone transfers and specify the servers to be notified when a zone file is updated.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

It is not necessary to explain each of the zone transfer properties in detail.

Explain them briefly, and suggest that the students review this information in depth outside class.

You can control how often and when a zone transfer occurs by modifying the SOA (Start of Authority) resource record. The SOA record specifies the domains for which the zone is authoritative, and the parameters for how zone transfers occur. It also contains administrative information about the zone.

Modifying the SOA Resource Record

To modify the SOA resource record, change any of the following settings on the **Start of Authority (SOA)** tab in the **Properties** dialog box for the zone:

- **Serial number.** Tracks updates to the zone file. Each time the zone database is modified, the serial number is incremented. When a secondary server queries its primary server for updates, it uses the serial number to determine whether changes have been made to a zone. If the number has changed, a zone transfer occurs to update the records on the secondary server.
- **Primary Server.** Specifies the FQDN of the primary server.
- **Responsible Person.** Specifies the Simple Mail Transfer Protocol (SMTP) e-mail address of the person who is responsible for the server. This value should contain the e-mail address of someone who is available and who will check e-mail regularly. If zone transfers are not working properly, users can use the nslookup utility to locate the e-mail address of the responsible person and e-mail a description of the problem.

Note Replace the @ symbol, which appears in the nslookup response, with a period when typing the e-mail address of the responsible person.

- **Refresh interval.** Controls how often a secondary server queries its master server for new data. If DNS data is constantly changing, decrease this value to ensure that DNS data is updated in a timely manner. However, decreasing this value can increase the volume of network traffic.
- **Retry interval.** Controls how often a secondary server will attempt to update its zone file. If a secondary server cannot contact its master server, the retry interval determines how long the secondary server waits before attempting to contact its master server again.
- **Expires after.** Controls the length of time that a secondary server uses its current zone data to answer queries if it cannot contact its master server because of problems on the network. At the end of the expiration interval, if the secondary server cannot contact its master server, it stops performing name resolution for that zone. Increase this value if your secondary servers are unable to contact a master server for an extended period of time.
- **Minimum TTL.** Specifies the Time to Live (TTL) interval, or the minimum amount of time that a server can cache information for a zone. Increase this value if your network names do not change frequently.
- **TTL for this record.** Specifies the TTL of the SOA resource record.

Configuring Zone Transfer Security

You can specify the servers that are authorized to receive zone transfers for the zone by configuring one of the following options on the **Zone Transfers** tab of the **Properties** dialog box for the zone:

- **To any server.** Enables zone information to replicate to any server.
- **Only to servers listed on the Name Servers tab.** Enables zone information to replicate only to the servers that are listed on the **Name Servers** tab of the **Properties** dialog box for the zone. The **Name Servers** tab contains a list of servers that are in the same domain as the zone.
- **Only to the following servers.** Specifies whether you want to allow zone transfers only to the servers that you list under **IP address** on the **Zone Transfers** tab of the **Properties** dialog box for the zone.

Configuring Notification

You can also configure a master DNS server to include a list of one or more secondary servers that should be notified when a zone file is updated. If a secondary server receives notification from its master DNS server that changes have been made to the zone file, it initiates a zone transfer to update its records. It is recommended that on the **Name Servers** tab, you configure master DNS servers to allow zone transfers to only designated DNS servers.

Delivery Tip

Describe the notification process.

DNS Notify allows you to configure a master server to notify one or more secondary servers whenever changes to the zone occur. The secondary server then sends a request to its master DNS server for the updated information. Whenever a change is made to the primary zone, DNS updates the serial number of the zone file. When this happens, a master DNS server notifies any secondary servers that are included in its notify list, and the secondary servers that receive the notification then retrieve the updated information.

Note For more information about DNS Notify, see RFC 1996 under **Additional Reading** on the Web page on the Student Materials compact disc.

Delivery Tip

Explain how to configure the notify list.

To configure the notify list, open the **Properties** dialog box for the zone, click the **Zone Transfers** tab, and then click the **Notify** button. Then, specify the secondary server or servers that the master server will automatically notify of updates to the zone.

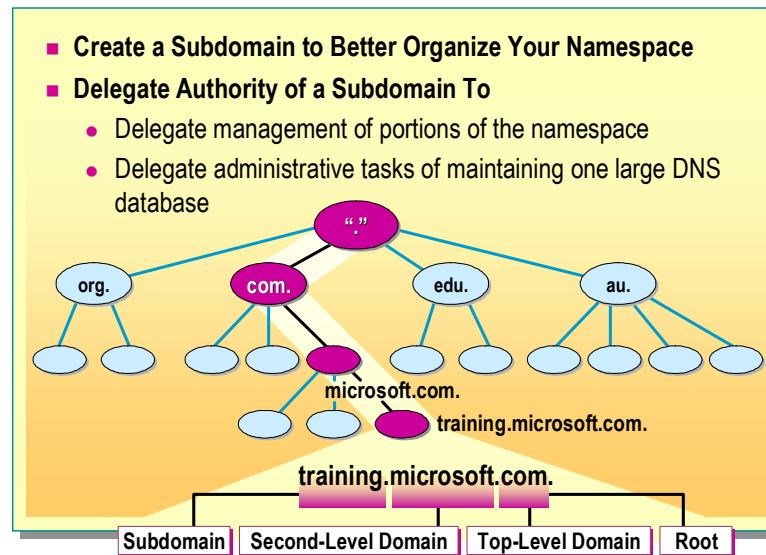
Creating a Subdomain

Topic Objective

To illustrate the different levels of the domain namespace.

Lead-in

A subdomain (child domain) is a DNS domain that is located directly beneath another domain (parent domain) in the namespace tree.



*****ILLEGAL FOR NON-TRAINER USE*****

A subdomain, also called a child domain, is a DNS domain that is located directly beneath another domain in the DNS hierarchical structure. The domain located immediately above the subdomain in the DNS hierarchical structure is called the parent domain. For example, training.microsoft.com is a subdomain of the microsoft.com domain.

Creating a Subdomain in an Existing Zone

You can create subdomains to better organize a zone and provide structure to your namespace. Dividing your namespace to include subdomains can be compared to creating folders and subfolders on a hard disk. Subdomains are generally based on departmental or geographic divisions within an organization.

Delivery Tip

Explain how to create a subdomain.

To create a subdomain, open DNS, and then expand the **Forward Lookup Zones** or **Reverse Lookup Zones** folder. Click the name of the zone in which you want to create a subdomain, right-click the zone name, and then click **New Domain**. Type the name of the subdomain in the **New Domain** dialog box, and then click **OK**.

Creating a Subdomain in a New Zone

You can delegate authority of a subdomain to a DNS server that you want to manage that portion of your DNS namespace. Delegation of authority allows you to:

- Delegate the management of a DNS domain to a number of departments (subdomains) within an organization.
- Delegate the administrative tasks of maintaining one large DNS database. You can assign different administrators to manage the DNS servers in the subdomain.

Delivery Tip

Explain the procedure for delegating authority of a subdomain.

To delegate authority of a subdomain, open the DNS console, and then expand **Forward Lookup Zones** or **Reverse Lookup Zones**. Click the name of the domain for which you want to delegate authority. Right-click the domain name, point to **New**, and then click **Delegation**.

The Add New Delegation wizard guides you through the process of specifying the name of the domain to which you are delegating authority. The wizard also guides you through the process of adding the name and IP address of the server or servers that will host the delegated domain.

Configuring Active Directory Integrated Zones

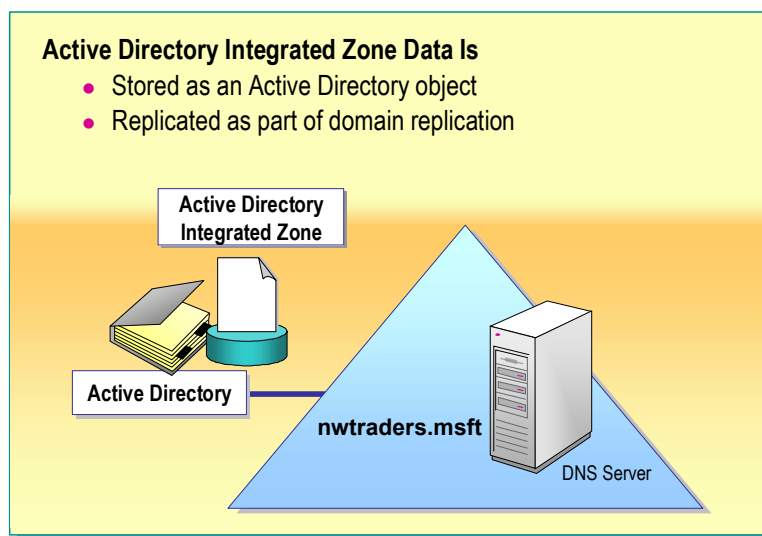
Topic Objective

To illustrate the concept of an Active Directory integrated zone.

Lead-in

You can integrate DNS zones into Active Directory to provide fault tolerance and increased security.

If you place the same Active Directory integrated zone on more than one DNS server, any of those DNS servers can act as primary servers for the zone.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

The zone files for Active Directory integrated zones are not stored in the `systemroot\System32\Dns` folder, where the standard zone files are stored. They are stored as objects in Active Directory.

In Active Directory integrated zones, zone data is stored as an Active Directory object and is replicated as part of domain replication. Active Directory integrated zones provide the following advantages:

- *No single point of failure.* With Active Directory integrated zones, changes made by using the dynamic update protocol can be made to any server that hosts the Active Directory integrated zone, rather than to a single server.
- *Fault tolerance.* All Active Directory integrated zones are primary zones. Therefore, each domain controller that hosts an Active Directory integrated zone maintains the zone information. Only domain controllers that reside in the Active Directory domain in which the zone data is stored can host the zone.
- *Single replication topology.* Zone transfers occur automatically as part of Active Directory replication, eliminating the need to configure replication for DNS and Active Directory separately.
- *Secure dynamic updates.* With Active Directory integrated zones, you can set permissions on zones and records within those zones. Also, updates that use the dynamic update protocol can only come from authorized computers.

Note You can only create Active Directory integrated zones on servers that are configured as domain controllers and that have the DNS Server service installed on them.

Creating Active Directory Integrated Zones

To create an Active Directory integrated zone, use the same procedure that you would use to create a standard zone, but click **Active Directory integrated** on the **Zone Type** page of the New Zone wizard.

Converting Existing Zones

Delivery Tip

Describe the process of converting an existing zone to an Active Directory integrated zone.

Before you convert an existing zone to an Active Directory integrated zone, it is important to be aware of the following information:

- The server that is running the DNS Server service must be configured as a domain controller.
- Active Directory integrated zones are stored in Active Directory. When you store a zone in Active Directory, the zone file is copied into Active Directory and deleted on the primary server for the zone.

You can convert a standard primary zone to an Active Directory integrated zone. To do this, open the **Properties** dialog box for the zone that you want to convert. Click the **General** tab, and then click **Change**. In the **Change Zone Type** dialog box, click **Active Directory integrated**, and then click **OK**.

Note The **Active Directory integrated** option is not available in the **Change Zone Type** dialog box until you implement Active Directory.

Migrating Zones to the Windows 2000 DNS Server Service

Topic Objective

To list the server files that are necessary for the Windows 2000 DNS Server service.

Lead-in

When copying zone files from a DNS server running BIND to a Windows 2000-based DNS server, use the file naming convention for the Windows 2000 DNS Server service.

Files in the Windows 2000 DNS Server Service Include:	
Domain_name.dns	The Forward Lookup File That Is Used to Translate Host Names to IP Addresses
z.y.x.w.in-addr.arpa.dns	The Reverse Lookup File That Is Used to Translate IP Addresses to Host Names
Cache.dns	Contains the Required Host Information for Resolving Names Outside Authoritative Domains
Boot	Controls How the DNS Server Service Starts

*****ILLEGAL FOR NON-TRAINER USE*****

The DNS Server service installation process creates the *systemroot\System32\Dns* folder. This folder contains the DNS database files described in the following table.

File type	Description
<i>Domain_name.dns</i>	The forward lookup file that is used to translate host names to IP addresses.
<i>z.y.x.w.in-addr.arpa.dns</i>	The reverse lookup file that is used to translate IP addresses to host names.
<i>Cache.dns</i>	The cache file that contains the required host information for resolving names outside authoritative domains. The default file contains records for all of the servers that host the root zone on the Internet.
<i>Boot</i>	The boot file that controls how the DNS Server service starts. In Windows 2000, the Boot file is optional because the boot settings are stored in the registry.

Migrating From a BIND-Based DNS Server

When migrating from a DNS server running Berkeley Internet Name Domain (BIND) to a Windows 2000–based DNS server, you need to rename any BIND-created zone or boot files and copy them to the folder that is used by the Windows 2000 DNS Server service.

If you continue to use a BIND boot file to provide the initial configuration settings that are used when the DNS Server service starts, you must change the boot method that the DNS Server service uses.

Renaming Zone Files

BIND zone files on UNIX-based DNS servers use a different naming convention from the naming convention that the Windows 2000 DNS Server service uses. Therefore, you must copy and rename zone files on UNIX-based DNS servers that use BIND to the computer running Windows 2000 Server.

The following table compares the file names on a UNIX-based DNS server that uses BIND with the file names that the Windows 2000 Server service uses.

File type	UNIX file name	Windows 2000 file name
Boot file	named.boot	Boot
Forward lookup zone file	db. <i>domain_name</i>	<i>Domain_name</i> .dns
Reverse lookup zone file	db.w.x.y	y.x.w.in-addr.arpa.dns

Note The Boot file is a part of the BIND-specific implementation of DNS. If you are migrating from a DNS server running BIND, copying the Boot file allows easy migration of your existing configuration.

For more information about BIND, see the Internet Software Consortium (ISC) Web site at <http://www.isc.org>

Configuring DNS for Internal Use

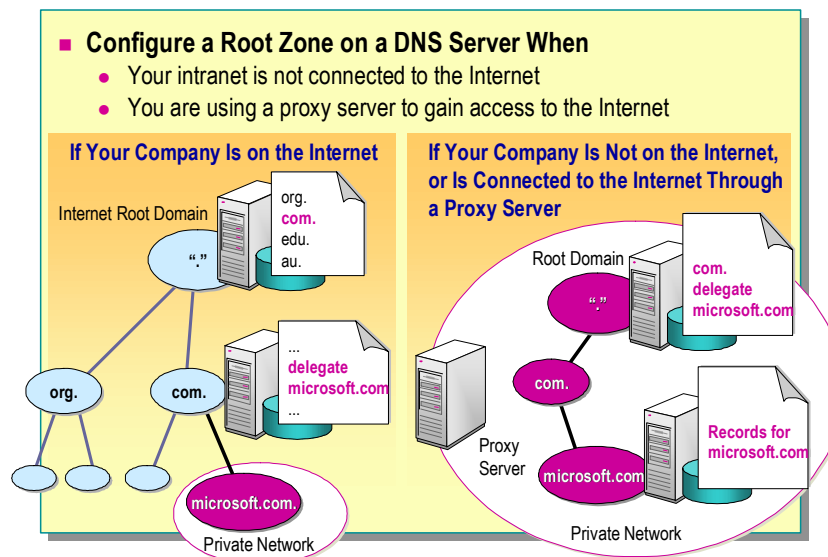
Topic Objective

To highlight the key points of configuring DNS for internal use.

Lead-in

Root zones on computers that are running the DNS Server service are authoritative for the root of the domain namespace.

Typically, a root zone is external to an organization. Therefore, you should consider whether it is necessary to configure a root zone on your intranet.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

It is necessary to create a root server only if you are configuring DNS in an intranet, or if you are using a proxy server to gain access to the Internet.

DNS is the hierarchical structure that defines the Internet's namespace. The Internet's root domain contains information about various attributes of the top-level DNS servers (for example, the servers in the com domain). The top-level DNS servers contain information about the second-level DNS servers (for example, the servers in the microsoft.com domain).

To resolve a host name on the Internet, a DNS server begins its search in its own database. If unsuccessful, it then starts at the root, and continues searching through the top-level and second-level servers, until it can resolve the host name.

There are two instances in which you would configure a root zone on a DNS server on your intranet to enable name resolution to start at your internal root domain rather than at the Internet's root domain. It is necessary for you to configure a root zone if:

- Your intranet is not connected to the Internet.
- Your organization is connected to the Internet through a proxy server.

To configure a root zone on a DNS server, use the New Zone wizard to create a root zone that is represented by a period (.).

Important To allow your DNS server to perform name lookups on the Internet, ensure that you have not configured a root zone on the server, and that the **Root Hints** tab in the **Properties** dialog box of the server contains a list of servers that are authoritative for the root zone of the Internet.

◆ Integrating DNS and DHCP

Topic Objective

To list the topics that are related to DNS and DHCP integration.

Lead-in

You can integrate DNS and DHCP to enable DHCP servers and clients to update the DNS server database.

- Overview of Dynamic Updates
- Configuring Dynamic Updates
- Securing Dynamic Updates

*****ILLEGAL FOR NON-TRAINER USE*****

By default, Windows 2000–based clients can update DNS with their name-to-IP address mapping information whenever a DHCP server assigns an IP address to them. However, computers running previous versions of Windows, such as Microsoft Windows NT® and Windows 98, do not have this capability. To resolve this problem, you can configure a DHCP server to update the DNS server database with the name-to-IP address mapping information of client computers. The DHCP server uses the dynamic update protocol to update the DNS server.

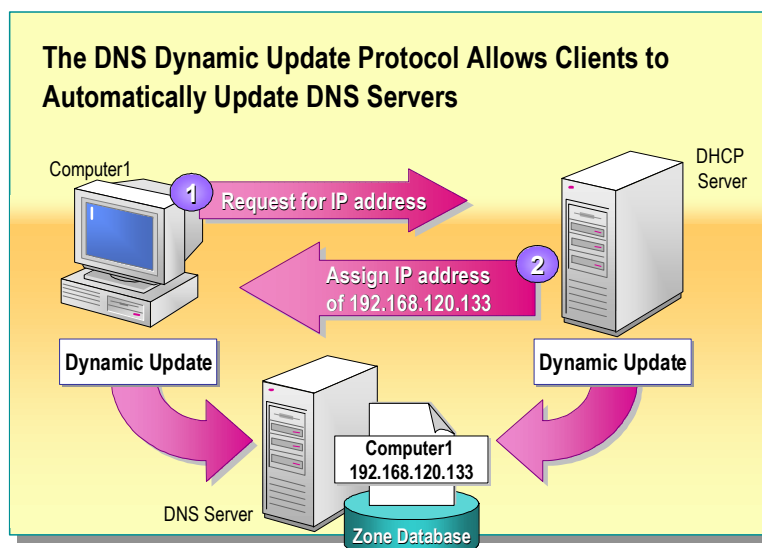
Overview of Dynamic Updates

Topic Objective

To illustrate the dynamic update process.

Lead-in

Dynamic updates can be used in conjunction with DHCP to dynamically update resource records when a computer's DHCP address is released and renewed.



*****ILLEGAL FOR NON-TRAINER USE*****

You can configure DHCP servers to automatically assign IP addresses to client computers. When a client receives a new IP address from a DHCP server, the name-to-IP address mapping information that is stored on a DNS server must be updated. In Windows 2000, DHCP servers and clients can register with and dynamically update name-to-IP address mapping information on DNS servers that are configured to support dynamic updates.

Important Static DNS servers are incapable of interacting dynamically with DHCP when client configurations change. Therefore, Microsoft recommends that you upgrade all DNS servers to Windows 2000 to enable them to support dynamic updates.

Dynamic Update Protocol

Delivery Tip

Describe the dynamic update protocol, and refer students to RFC 2136 or the *Windows 2000 DNS* white paper for more information.

The dynamic update protocol enables client computers to automatically update their resource records on a DNS server without administrator intervention. Windows 2000-based computers that are configured with a static IP address are, by default, also configured to perform dynamic updates on the DNS server. In this case the client will update both the forward and reverse lookup entries.

Note For more information about the DNS dynamic update protocol, see RFC 2136 or the white paper *Windows 2000 DNS* under **Additional Reading** on the Web page on the Student Materials compact disc.

Dynamic Update Process

Delivery Tip

Describe the dynamic update process for Windows 2000–based clients.

When a DHCP server assigns an IP address to a Windows 2000–based DHCP client, the following process occurs:

1. The client initiates a DHCP request message to the DHCP server, requesting an IP address. This message includes the FQDN.
2. The DHCP server returns a DHCP acknowledgment message to the client, granting an IP address lease.
3. The client sends a DNS update request to the DNS server for its own forward lookup record, the A resource record.

Note As an alternative to this step, you can configure the DHCP client and the DHCP server to enable the DHCP server to send updates on behalf of the client.

4. The DHCP server sends updates for the DHCP client's reverse lookup record, the PTR (pointer) resource record. The DHCP server uses the FQDN that it obtained in the first step to perform this operation.

Dynamic Updates for Clients Running Previous Versions of Windows

Delivery Tips

Describe the dynamic update process for clients running previous versions of Windows.

Emphasize that the DHCP server must be configured to always update the DNS database on behalf of these clients.

Client computers running previous versions of Windows do not support dynamic updates and are unable to interact dynamically with the DNS server. You must configure the DHCP server to always update A and PTR records for these clients, in which case the following process occurs:

1. The client initiates a DHCP request message to the server, requesting an IP address. Unlike DHCP request messages from Windows 2000–based DHCP clients, the request does not include an FQDN.
2. The server returns a DHCP acknowledgment message to the client, granting an IP address lease.
3. The DHCP server sends updates to the DNS server for the client's A and PTR resource records.

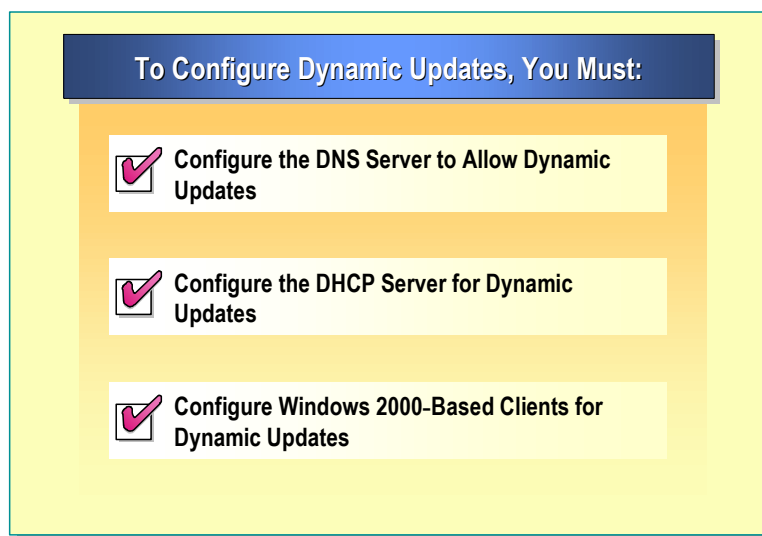
Configuring Dynamic Updates

Topic Objective

To list the topics that are related to configuring dynamic updates.

Lead-in

To configure dynamic updates, you must configure the DNS server, DHCP server, and Windows 2000–based clients.



*****ILLEGAL FOR NON-TRAINER USE*****

To enable dynamic updates, you must configure the DNS server to allow dynamic updates, and configure the DHCP server and the client computers to update the DNS database.

Configuring the DNS Server to Allow Dynamic Updates

To configure a DNS server to allow dynamic updates, open the **Properties** dialog box for the zone on the DNS server that you want to configure. On the **General** tab, click **Yes** in the **Allow dynamic updates** list box. The following table describes the available options for dynamic updates.

Option	Description
No	Disables dynamic updates for the zone.
Yes	Enables dynamic updates for the zone.
Only secure updates	Enables secure dynamic updates from authorized client computers to an Active Directory integrated zone.

Delivery Tip

Describe the options that are available for configuring a DNS server to allow dynamic updates.

The **Only secure updates** option is described in more detail in the next section.

Configuring the DHCP Server for Dynamic Updates

To configure the DHCP server to update the DNS database:

1. In DHCP, open the **Properties** dialog box for the server that you are configuring, and then click the **DNS** tab.
2. Select the **Automatically update DHCP client information in DNS** check box, and then click one of the following options to specify how you want the DHCP server to interact with the DNS server:
 - **Update DNS only if DHCP client requests.** Specifies that the DHCP server update the DNS database based on the client settings. By default, Windows 2000–based clients register their A resource records and request that the DHCP server update its PTR resource record. This option is the default setting for the DHCP server.

Delivery Tip

Demonstrate the procedure for configuring the DHCP Server for dynamic updates.

- **Always update DNS.** Specifies that the DHCP server update the client's A and PTR resource records in the DNS database, regardless of the client settings.

Note If you do not want the DHCP server to register and update client information in the DNS database, clear the **Automatically update DHCP client information in DNS** check box.

3. To specify how the DHCP server functions when a client's lease expires, perform one of the following steps:
 - Verify that the **Discard forward (name-to-address) lookups when the lease expires** check box is selected if you want the DHCP server to send updates to the DNS database to discard the client's A resource record when the lease expires. This is the default setting for the DHCP server.
 - Clear the **Discard forward (name-to-address) lookups when the lease expires** check box to prevent the DHCP server from sending updates to the DNS database to discard the client's A resource record when the lease expires.
4. To enable the DHCP server to update the DNS database with the A and PTR resource records of clients that are running previous versions of Windows, select the **Enable updates for DNS clients that do not support dynamic update** check box.
5. When you have finished configuring the DHCP server, click **OK**.

Configuring Windows 2000–Based Clients for Dynamic Updates

Delivery Tip

Demonstrate the procedure for configuring Windows 2000–based clients for dynamic updates.

To configure Windows 2000–based clients to update their A resource records in the DNS database:

1. In Networking and Dial-up Connections, right-click the connection that you want to configure, and then click **Properties**.
2. In the **Properties** dialog box for the connection, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced**.
4. In the **Advanced TCP/IP Settings** dialog box, on the **DNS** tab, select the appropriate check boxes:
 - **Register this connection's address in DNS.** Enables the client to register resource records in DNS by using the full computer name and the IP address of the network connection.
 - **Use this connection's DNS suffix in DNS registration.** Enables the client to register resource records in DNS by using the first label of the computer name in addition to the DNS suffix for the connection. Use this option only if the DNS suffix differs from the domain name.
5. Click **OK** three times.

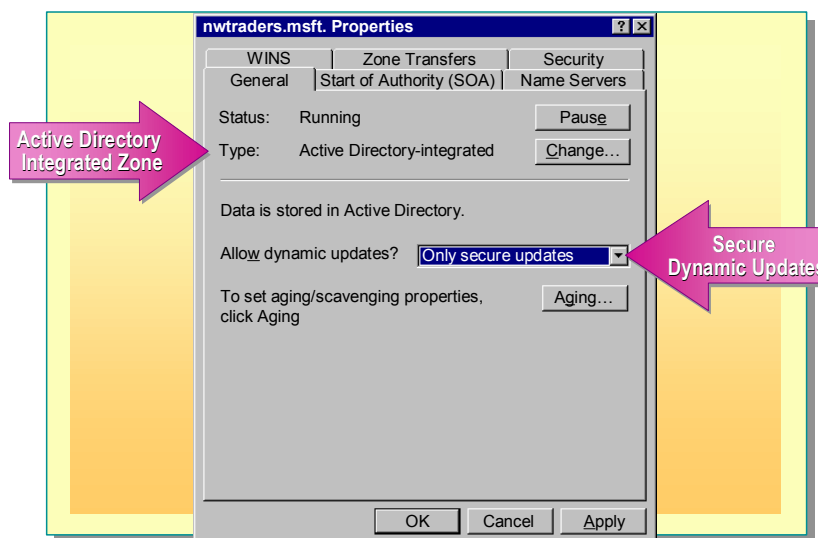
Securing Dynamic Updates

Topic Objective

To illustrate the user interface for securing dynamic updates.

Lead-in

You can configure the DNS server to ensure that dynamic updates are secure.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Only Active Directory integrated zones can be configured for secure dynamic updates.

You can configure the DNS server to perform secure dynamic updates for Active Directory integrated zones. With secure dynamic updates, the authoritative DNS server only accepts new registrations from computers that have a computer account in Active Directory, and only accepts updates from the computer that originally registered the record.

Benefits of Secure Dynamic Updates

Secure dynamic updates provide the following benefits:

- Protection of zones and resource records against modification by unauthorized computers.
- The ability to specify the computers and groups that are authorized to modify zones and resource records.

Delivery Tip

Demonstrate the procedure for configuring secure dynamic updates.

Configuring Secure Dynamic Updates

To configure secure dynamic updates on the DNS server:

1. In DNS, open the **Properties** dialog box for the Active Directory integrated zone on the DNS server that you want to configure.
2. On the **General** tab, click **Only secure updates** in the **Allow dynamic updates** list, and then click **OK**. This option appears in the list only if the zone type is Active Directory integrated.

Note For more information about secure dynamic updates, see RFC 2137 under **Additional Reading** on the Web page on the Student Materials compact disc.

◆ Maintaining and Troubleshooting DNS Servers

Topic Objective

To list the topics that are related to maintaining and troubleshooting DNS servers.

Lead-in

The DNS Server service includes several utilities that you can use to test DNS configuration, ensure that zone transfers are working properly, and identify errors.

- Reducing Network Traffic by Using Caching-Only Servers
- Maintaining DNS Zones
- Monitoring DNS Servers
- Verifying Resource Records by Using Nslookup
- Troubleshooting Name Resolution Problems

*****ILLEGAL FOR NON-TRAINER USE*****

DNS servers are critical to a network; therefore, you must maintain and troubleshoot them to ensure that they are functioning properly and to optimize network performance. For example, you can improve DNS performance by configuring a caching-only server to reduce the amount of DNS-related network traffic, and maintaining resource records to ensure that the name resolution data on a DNS server is current.

Windows 2000 provides several utilities for monitoring and troubleshooting DNS servers. These utilities include:

- The DNS in Microsoft Management Console (MMC), which you can use to test DNS servers and monitor their ability to process and resolve queries.
- Command-line utilities, such as Nslookup, which you can use to verify resource records and troubleshoot DNS problems.
- Logging features, such as the DNS server log, which you can view by using Event Viewer.

Reducing Network Traffic by Using Caching-Only Servers

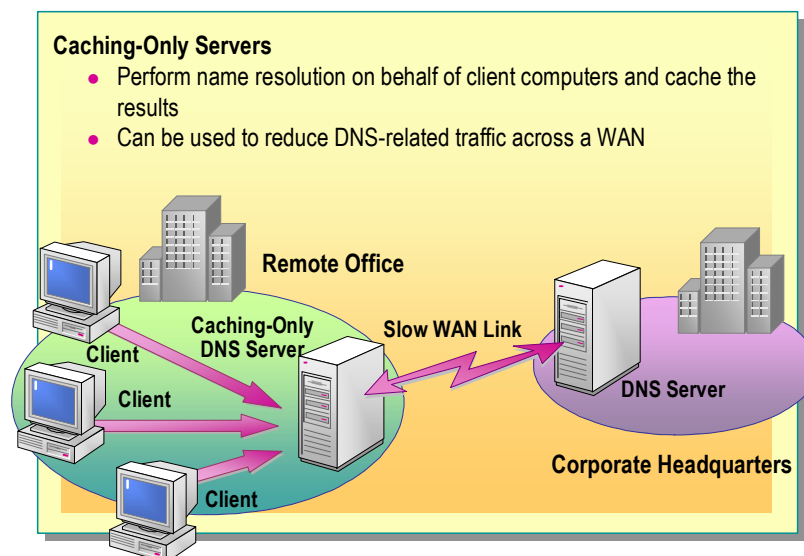
Topic Objective

To illustrate the concept of a caching-only server.

Lead-in

Caching-only servers are servers that only perform queries, cache the answers, and return the results.

Caching-only servers are not authoritative for any domains and contain only information that they have cached while resolving queries.



*****ILLEGAL FOR NON-TRAINER USE*****

Caching-only servers perform name resolution on behalf of clients and then cache, or store, the results. They are not configured to be authoritative for a zone, so they do not store standard primary or standard secondary zones. The cache is populated with the most frequently requested names. These names and their associated IP addresses are available from the cache for answering subsequent client queries.

Delivery Tip

Use the following example to explain how a caching-only server can be used to help reduce traffic across a WAN.

Remote offices often have a limited amount of available bandwidth for connecting to the Internet or corporate headquarters across a WAN. A caching-only server can be used to reduce the traffic that the name resolution or zone transfer process generates.

When a remote office has a limited amount of available bandwidth for connecting to a corporate office, a caching-only server should be configured at the remote office to send recursive queries to a DNS server at the corporate office. A recursive query is one in which the DNS server assumes the full workload and responsibility for providing a complete answer to the query. The DNS server at the corporate office is better equipped to handle recursive queries because it has a greater amount of available bandwidth for connecting to the Internet or an intranet.

Caching-only servers help to reduce traffic across a wide area network (WAN) in the following ways:

- A caching-only server attempts to locate information in its cache to resolve client requests. If the required information is not in its cache, the caching-only server performs a query across the WAN to locate the necessary information and update its cache. The greater the amount of information that is stored in its cache, the less likely it is that the caching-only server will need to perform a query, thus reducing traffic across the WAN.
- A caching-only server neither maintains zone files, as does a primary DNS server, nor does it store a copy of a zone file, as does a secondary DNS server. Therefore, caching-only servers do not generate zone transfer traffic.

Configuring a Caching-Only Server

To configure a caching-only server, install the DNS Server service on a computer running Windows 2000 Server, and do not configure any forward or reverse lookup zones.

Configuring Forwarders

You should configure a caching-only server to perform recursive rather than iterative queries by configuring it to use forwarders. A *forwarder* is a DNS server that other DNS servers designate to forward queries for resolving external domain names. This reduces the amount of traffic across the WAN for performing name resolution.

To forward queries to another server:

1. Open DNS from the **Administrative Tools** menu.
2. Right-click the server on which you want to configure forwarding, and then click **Properties**.
3. On the **Forwarders** tab, select the **Enable Forwarders** check box.
4. Type the IP address of the server to which you want to forward, click **Add**, and then click **OK**.

Note You can also configure forwarders on a server that hosts zones. In this case, the DNS server responds to all queries that it can resolve from its zone files and forwards all other queries.

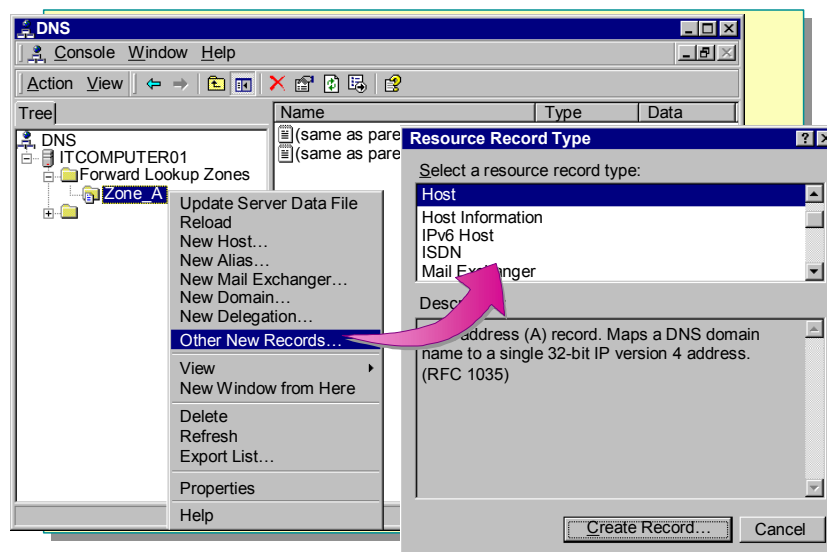
Maintaining DNS Zones

Topic Objective

To illustrate the user interface for creating resource records.

Lead-in

Resource records are stored in a DNS zone and provide the information that DNS servers use to perform name resolution.



*****ILLEGAL FOR NON-TRAINER USE*****

Resource records contain data that is used to configure a DNS server or to provide the information that DNS servers use when resolving queries from hosts and other servers. There are various resource record types that are defined for a zone. Each type of resource record contains different types of data.

DNS servers can contain the following types of resource records:

Record Type	Purpose
A (address)	Contains name-to-IP address mapping information. You must manually add A records to a DNS database if you have clients that do not register their names in the DNS database by using the DNS dynamic update protocol, such as clients running Windows NT version 4.0. An A record is also referred to as a host record.
NS (name server)	Defines the servers that are authoritative for a certain zone or contain the zone file for that domain.
CNAME (canonical name)	Allows you to provide additional names to a server that already has a name in an A record. For example, if the server called webserver1.nwtraders.msft hosts the Web site for nwtraders.msft, this server should have the common name www.nwtraders.msft. To do this, create a CNAME record that maps the name www to webserver1. An A record is also referred to as alias record.
MX (mail exchanger)	Specifies the server to which e-mail applications can deliver mail. For example, if you have a mail server running on a computer named mail1.nwtraders.msft and you want all mail for <i>user_name@nwtraders.msft</i> to be delivered to this mail server, you need to add an MX record to the zone for nwtraders.msft that points to the mail server for that domain.

(continued)

Record Type	Purpose
SOA (start of authority)	Indicates the starting point or original point of authority for information stored in a zone. The SOA resource record is the first resource record created when you add a new zone. It also contains several parameters used by other computers that use DNS to determine how long they will use information for the zone and how often updates are required.
PTR (pointer)	Used in a reverse lookup zone created within the in-addr.arpa domain to designate a reverse mapping of a host IP address to a host DNS domain name.
SRV (service)	Registered by services so that clients can locate a service by using DNS. For example, a Windows 2000 domain controller has many network services that perform functions such as verifying user logon and checking group membership. Domain controllers register these services by creating the appropriate SRV record in the DNS database. A client computer can then find a domain controller by looking up the necessary information in the DNS database. You are not normally required to add SRV resource records, because the service creates them automatically and adds them to the DNS database by using the dynamic update protocol.

Creating Resource Records

To create a new resource record, open DNS. Right-click the name of the zone to which you want to add the new resource record, and then click the type of record that you want to create, or click **Other New Records** for a complete list of resource records.

Removing a DNS Server From the Network

You must update your DNS configuration when removing a DNS server from your network. To remove a DNS server from the network, make the following changes in any zone for which the DNS server is authoritative:

- Remove the A resource record for the server.
- Delete the server name from the NS resource records.
- If the server is the primary server for a standard zone, revise the owner field of the SOA resource record for the zone to point to the new primary DNS server for the zone.

Note This step is not necessary for Active Directory integrated zones.

- Verify that all records (NS or A resource records) that are used for delegation to the zone are revised and no longer point to the removed server.

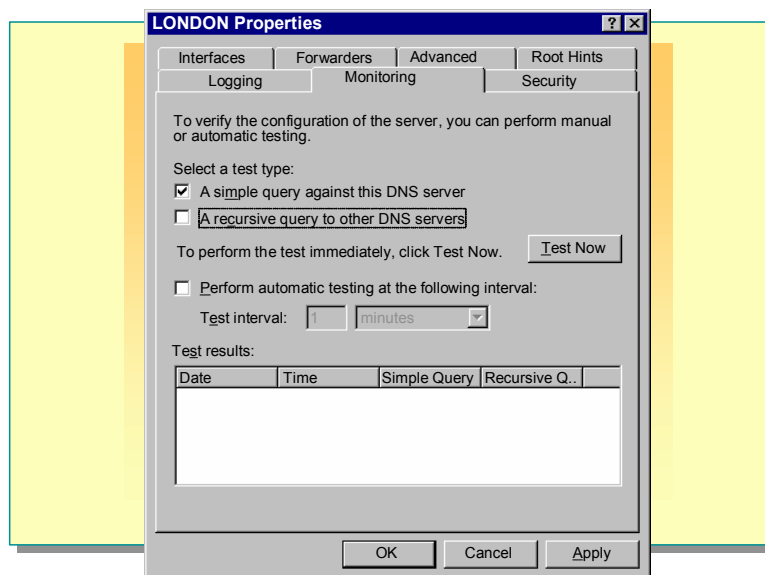
Monitoring DNS Servers

Topic Objective

To highlight the different methods for testing the DNS Server service.

Lead-in

You can use the DNS administrative tool to test the DNS Server service.



*****ILLEGAL FOR NON-TRAINER USE*****

After you install DNS, test the configuration before activating it on your network to prevent problems with name resolution. The Windows 2000 DNS Server service provides the capability to test and monitor DNS by using the DNS administrative tool.

Testing the DNS Server Service

You can configure the DNS Server service to perform queries immediately or on a scheduled basis to ensure that the service is operating correctly. In DNS, open the **Properties** dialog box for the server that you want to monitor, and then click the **Monitoring** tab. You can test a DNS server by performing two types of queries:

- *Simple query.* This type of query performs a local test by using the DNS client to query a DNS server.
- *Recursive query.* This type of query tests a DNS server by forwarding a recursive query to another DNS server.

Under **Tests Performed**, select the **Simple query** check box, the **Recursive query** check box, or both, and then click **Test Now**. The test results appear under **Test results**.

To perform tests on a scheduled basis, select the **Perform automatic testing at the following interval** check box, and then select an interval.

Tip You may receive incorrect results if you verify the operation of a DNS server immediately after adding or removing zones. If this occurs, either right-click the DNS server in the console tree, and then click **Refresh**, or close and then reopen DNS.

Monitoring the DNS Server Service By Using Event Viewer

You can use Event Viewer to view the DNS server event log. This information is particularly useful when you need detailed information about server performance.

Enabling DNS Server Debug Logging Options

For advanced troubleshooting purposes, you can configure a DNS server to record detailed information about all operations. To enable logging, on the **Logging** tab of the **Properties** dialog box of the DNS server, select the appropriate check boxes for the events that you want to record. By default, the DNS server records logging information in the file `\systemroot\system32\dns\dns.log`.

Important Enable logging for troubleshooting purposes only. Logging can be resource intensive, which can affect overall server performance and consume disk space.

Verifying Resource Records by Using Nslookup

Topic Objective

To illustrate the data that the **nslookup** command returns.

Lead-in

Use the Nslookup utility to verify that resource records have been added or updated correctly in a zone.

Use Nslookup to Verify That the Information Contained in Resource Records Is Correct

```

C:\>nslookup
Default Server:      london.nwtraders.msft
Address:             192.168.1.200

> bonn
Server:              london.nwtraders.msft
Address:             192.168.1.200

Name:                bonn.nwtraders.msft
Address:             192.168.1.1

> 192.168.1.2
Server:              london.nwtraders.msft
Address:             192.168.1.200

Name:                denver.nwtraders.msft
Address:             192.168.1.2

> exit
C:\>

```

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Run Nslookup in both non-interactive mode and interactive mode. Also, show how to view Nslookup Help by typing a question mark (?) while in interactive mode.

After you add resource records, you can use Nslookup to verify that the resource records are correct. Nslookup has two modes:

- *Interactive.* Use interactive mode when you require more than one piece of data. To run interactive mode, at the command prompt, type **nslookup**. To exit interactive mode, type **exit**.
- *Non-Interactive.* Use non-interactive mode when you require a single piece of data, or to include an Nslookup command in a command or batch file. Type the Nslookup syntax at the command prompt, and the data is returned.

The following table describes the Nslookup syntax:

nslookup [-option ...] [computer_to_find | - [server]]

Syntax	Description
-option...	Specify one or more Nslookup commands. For a list of available commands, type a question mark (?).
computer_to_find	If you specify the IP address of a computer, Nslookup returns the host name. If you specify the host name of a computer, Nslookup returns the IP address. If the computer that you want to find is a host name and does not have a trailing period, the default DNS domain name is appended to the name. To find a computer outside the current DNS domain, append a period to the name.
-server	Specify the server to use as the DNS server. If you omit the server, the currently configured default DNS server is used.

Note For Nslookup to work properly, a PTR resource record must exist for the server on which you perform a lookup. At startup, Nslookup performs a reverse lookup on the IP address of the server that is running the DNS Server service and reports an error if it cannot resolve the address to a name.

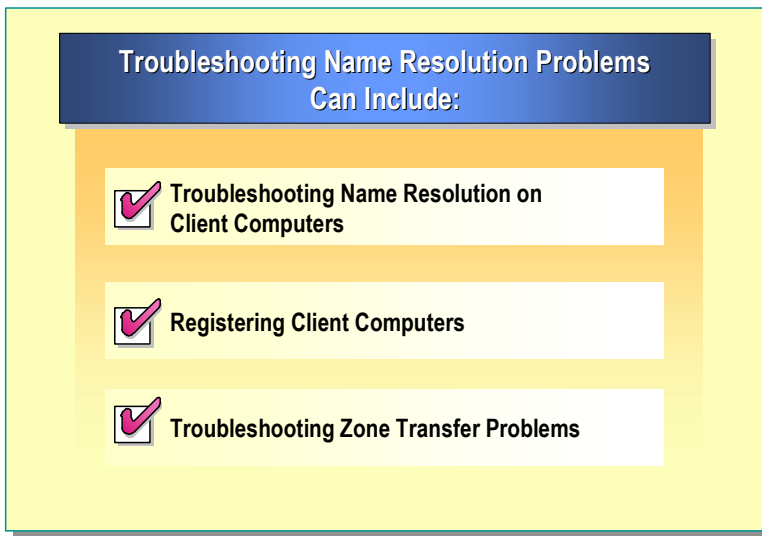
Troubleshooting Name Resolution Problems

Topic Objective

To list common name resolution problems and their solutions.

Lead-in

Windows 2000 includes several utilities that you can use to troubleshoot name resolution problems.



*****ILLEGAL FOR NON-TRAINER USE*****

Name resolution problems can occur if a client computer is resolving names incorrectly, or if the client computer name is not registered with the DNS servers on your network. Other name resolution problems can occur when the zone transfer process is not working properly.

Troubleshooting Name Resolution on Client Computers

Delivery Tip

Explain how to use the Ipconfig utility to flush and reset the cache on a client computer.

DNS clients cache query responses from DNS servers and use this information to answer future queries locally. When a query cannot be resolved locally, the client queries DNS servers to resolve a name. If you determine that the client computer is resolving names incorrectly, you can use the Ipconfig utility to flush and reset the cache on the client computer. At a command prompt, type **ipconfig /flushdns** to flush the cache.

Registering Client Computers

Delivery Tip

Explain how to use the Ipconfig utility to force a client to renew its registration.

Client computers use the dynamic update protocol to register their names with DNS servers. If a client's name records are missing from the servers, use the Ipconfig utility to refresh all DHCP leases and register any related DNS names. At a command prompt, type **ipconfig /registerdns** to force the client to renew its registration.

Troubleshooting Zone Transfer Problems

A secondary server queries its primary server for updates to a zone file, and uses the serial number in the SOA resource record to determine whether changes have been made to the zone. If the serial number has changed, a zone transfer occurs to update the records on the secondary server.

When a secondary server is not receiving updates from its master server, you can use the Nslookup utility to compare the serial numbers in each server's SOA resource record.

Delivery Tip

Explain how to use the Nslookup utility to compare the serial numbers in SOA resource records.

To compare serial numbers by using the Nslookup utility:

1. At a command prompt, type **nslookup**
2. Type the name of the primary server.
3. Type **set type=SOA**
4. Type *domain name* (where *domain name* is the name of the domain in which the primary server resides).
5. Record the serial number that appears on the SOA record.
6. Type the name of the secondary server.
7. Repeat steps 3–5, and then type **exit**

You can increase the serial number on the primary server to initiate a zone transfer and force an update to occur between a primary and a secondary server.

Delivery Tip

Explain how to change the serial number on a primary server to force a zone transfer.

To force a zone transfer:

1. On the server that hosts the primary zone file, open DNS from the **Administrative Tools** menu.
2. Open the **Properties** dialog box for the zone, and then click the **Start of Authority** tab.
3. Click **Increment** to increase the serial number, and then click **OK**.

Tip For more information about advanced DNS troubleshooting, see Windows 2000 Help and the Windows 2000 Server Resource Kit.

Lab B: Maintaining and Troubleshooting a DNS Server

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will monitor the DNS Server service, troubleshoot the DNS Server service by using the Nslookup utility, and enable event logging.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Monitor the DNS Server service.
- Troubleshoot the DNS Server service by using Nslookup.
- Enable event DNS logging.

Prerequisite

Before working on this lab, you must be familiar with DNS concepts and operations.

Lab Setup

To complete this lab, you need the following:

- A computer running Microsoft Windows 2000 Advanced Server that is configured as a domain controller.
- A static IP address and subnet mask.
- A lab partner. One partner will create the primary zone; the other will create a secondary zone and designate his or her partner's computer as the master DNS server.
- An FQDN. Refer to the Student Computer IP Addresses and FQDNs section of the lab for this information.

Scenario

Your company has configured DNS servers for your domain, and you are responsible for making sure that these servers are functioning correctly. Also, you are responsible for maintaining the DNS servers in your domain, so you must be able to determine when a server is not functioning correctly, and correct the problem quickly.

Estimated time to complete this lab: 45 minutes

Exercise 1

Monitoring the DNS Server Service

Scenario

You have just installed a DNS server, and you want to test it to ensure that it is functioning correctly.

Goal

In this exercise, you will test the DNS Server service to determine that it is functioning correctly.

Tasks	Detailed Steps
 Perform the following procedure on both computers.	
1. In DNS, perform simple query and recursive query tests.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - Open DNS from the Administrative Tools menu. - In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Properties. - In the <i>server Properties</i> dialog box, on the Monitoring tab, under Select a test type, select the check boxes for both query types, and then click Test Now. - Verify that PASS appears in both columns, click OK to close the <i>server Properties</i> dialog box, and then minimize DNS.
2. Disable all network adapters and clear the DNS cache. Perform the simple and recursive query tests again.	- Right-click My Network Places, and then click Properties. - In Network and Dial-up Connections, right-click Classroom, and then click Disable.
 Important: If your partner has already disabled the PartnerNet network connection on his or her computer, your PartnerNet network interface appears as disconnected.	
2. (continued)	- Right-click PartnerNet, and then click Disable. - Restore DNS. - In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Clear cache. - Right-click <i>server</i>, and then click Properties. - On the Monitoring tab, under Select a test type, verify that the check boxes for each query type are selected, and then click Test Now.
 Note: You may have to wait up to one minute for the results of the query tests to appear. This is because of the time-out values for DNS queries.	

(continued)

Tasks	Detailed Steps
 The Simple Query column lists PASS, and the Recursive Query column lists FAIL. If the recursive query fails but the simple query passes, as in this test, what is the most likely cause of the failure? A. The DNS server is unable to contact any of the servers listed in Root Hints. B. The DNS server SOA record has an incorrect entry on the Name Servers tab. C. The IP address of this computer is incorrect. D. There are no forward lookup zones configured. A. The DNS server is unable to contact any of the servers listed in Root Hints.	
3. Enable the network adapters and try the recursive and simple queries again.	a. Click OK to close the <i>server</i> Properties dialog box. b. Minimize DNS. c. Right-click Classroom, and then click Enable. d. Right-click PartnerNet, and then click Enable.
 Important: If your partner has not enabled the PartnerNet network connection yet, you may receive a message stating that the connection failed. You can ignore this message.	
3. <i>(continued)</i>	e. Close Network and Dial-up Connections. f. Restore DNS. g. Right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Clear cache. h. In the console tree, right-click <i>server</i>, and then click Properties. i. On the Monitoring tab, under Select a test type, verify that the check boxes for each query type are selected, and then click Test Now.  <i>PASS should appear the Simple Query and Recursive Query columns of the Test results box, indicating that the test was successful.</i> j. Click OK to close the <i>server</i> Properties dialog box, and then close DNS.

Exercise 2

Examining Resource Records by Using Nslookup

Scenario

You have received reports of DNS servers not resolving names correctly in all locations. You suspect that this may be a result of zone transfers not working correctly, or that it may be due to invalid resource records.

Goal

In this exercise, you will use Nslookup to verify resource records on your server and your partner's server. You will also use Nslookup to determine whether a zone transfer has taken place.

Tasks	Detailed Steps
1. Using Nslookup, examine the A (host), NS (name server) and SOA (start of authority) records for your domain.	a. At a command prompt, type nslookup and then press ENTER.
 Note: If you receive a message “Can’t find server name for address 192.168.1.200: Timed out,” ignore this message for this lab (note that the address may be 192.168.z.200, where <i>z</i> is the number for your classroom). This message appears because Nslookup attempts to use reverse lookup to determine the validity of the address. If there is no reverse lookup zone for this subnet, which in this case would be 1.168.192.in-addr.arpa, the reverse lookup query will fail, and this message will appear. This message does not imply that Nslookup will not work.	
1. (continued)	b. To set the default server to your server, type server server.domain.nwtraders.msft (where <i>server</i> is the name of your computer and <i>domain</i> is the name of your domain), and then press ENTER. c. Type ls -t a domain.nwtraders.msft and then press ENTER.  <i>Nslookup displays a list of the A records for the domain domain.nwtraders.msft. Using the ls -t command within nslookup is a quick way of viewing resource records in a domain. Next you are going to look at the NS and SOA records for the domain domain.nwtraders.msft.</i> d. Type set type=NS and then press ENTER. e. Type domain.nwtraders.msft and then press ENTER. f. Type set type=SOA and then press ENTER. g. Type domain.nwtraders.msft and then press ENTER.

(continued)

Tasks	Detailed Steps
	The serial number for both servers' SOA records should be the same. If the serial numbers are not the same after you wait a short time, what can you do to determine why zone transfer has not occurred? Select all that apply. A. Examine the System Log in Event Viewer B. Examine the DNS Server log in Event Viewer C. Examine all A (host) records in DNS D. Ping both servers E. Examine Zone Transfers and SOA tabs for your domain in DNS A, B, and E. Examine the event logs for more information, and then examine the settings in DNS for more information.
3. (continued)	d. Close the command prompt window.

Exercise 3

Examining the DNS Server Event Logs

Scenario

You are monitoring your DNS server to determine when changes that cause zone transfers occur, and when changes are written to the hard disk for ongoing performance management. You also want to monitor the DNS server to determine whether any errors are occurring.

Goal

In this exercise, you will examine the contents of the DNS Server event logs and DNS trace logs to determine the possible causes of an error.

Tasks	Detailed Steps
1. Open Computer Management and examine the DNS Server event log.	a. Open Computer Management from the Administrative Tools menu. b. In the console tree, expand Event Viewer , and then click DNS Server . c. In the details pane, double-click the first event log entry.
 What was the last version of the zone that was written to the zone file? Answers will vary. Notice that it is normal for the serial number for the zone file to be quite high (for example, 500), because the number will be incremented every time there is a change to the zone database file. 	
1. <i>(continued)</i>	d. Click OK to close the Event Properties dialog box. e. Close Computer Management.
2. Configure the DNS Server service to log updates to the zone database file.	a. Open DNS from the Administrative Tools menu. b. In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Properties . c. On the Logging tab, select the Update check box, and then click OK .
 Important: Perform the following procedure only on the computer with the lower student number.	

(continued)

Tasks	Detailed Steps
3. Increment the serial number for your domain's primary zone database file, and then update the Server Data files. Stop the DNS Server service.	- In the console tree, expand <i>server</i>, and then expand Forward Lookup Zones. - Right-click <i>domain.nwtraders.msft</i> (where <i>domain</i> is the name of your domain), and then click Properties. - On the Start of Authority (SOA) tab, click Increment, and then click OK. - Right-click <i>server</i>, and then click Update Server Data Files. - Right-click <i>server</i>, point to All Tasks, and then click Stop.
4. Examine the contents of the log file <code>c:\winnt\system32\dns\dns.log</code> .	- Click Start, and then click Run. - In the Open box, type <code>c:\winnt\system32\dns\dns.log</code> and then click OK.
 What information can you find in the log? Details about when the DNS database was updated, and when the database was written to a file on the hard disk.	
4. <i>(continued)</i>	- Close the dns-Notepad window. - Right-click <i>server</i>, (where <i>server</i> is the name of your computer), point to All Tasks, and then click Start.
 Perform the following procedure on both computers.	
5. Close all open windows.	Close all open windows.

Exercise 4

Removing the DNS Server Service

Scenario

You are now going to remove the DNS Server service, because you are going to decommission this server and configure another server as the DNS server for your domain.

Goal

In this exercise, you will remove the DNS Server service and configure its TCP/IP properties.

Tasks	Detailed Steps
 Perform the following procedure on both computers.	
1. Configure the server to use the instructor computer as the DNS server.	- Right-click My Network Places, and then click Properties. - Open the Properties dialog box for the Classroom connection. - Click Internet Protocol (TCP/IP), and then click Properties. - In the Preferred DNS server box, type 192.168.z.200 (where <i>z</i> is the number of your classroom), and then click OK. - Click OK to close the Classroom Properties dialog box. - Open the Properties dialog box for the PartnerNet connection. - Click Internet Protocol (TCP/IP), and then click Properties. - In the Preferred DNS server box, type 192.168.z.200 and then click OK. - Click OK to close the PartnerNet Properties dialog box, and then close Network and Dial-up Connections.
 Perform the following procedure only on the computer with the lower student number.	
2. Remove the delegation of authority for your domain at the nwtraders.msft domain.	- Click Start, point to Programs, point to Administrative Tools, right-click DNS, and then click Run as. - In the Run As Other User dialog box, type eadmin@nwtraders.msft in the User name box, type password in the Password box, delete the contents of the Domain box, and then click OK. - In the console tree, expand London, expand Forward Lookup Zones, and then expand nwtraders.msft. - In the console tree, right-click domain.nwtraders.msft, (where <i>domain</i> is the name of your domain), and then click Delete. - Click OK to close the DNS message box. - Close DNS.
 Perform the following procedures on both computers.	

(continued)

Tasks	Detailed Steps
3. Remove the DNS Server service.	a. In Control Panel, double-click Add/Remove Programs, and then click Add/Remove Windows Components. b. In the Windows Components wizard, on the Windows Components page, under Components, click Networking Services, and then click Details. c. Clear the Domain Name System (DNS) check box, and then click OK. d. Click Next. e. When the configuration process is complete, click Finish. f. Close all open windows.
4. Refresh the DNS entries for your computer by running <code>ipconfig /registerdns</code> , and then log off.	a. At a command prompt, type <code>ipconfig /registerdns</code> and then press ENTER. b. Type <code>net stop netlogon</code> and then press ENTER. c. Type <code>net start netlogon</code> and then press ENTER. d. Close the command prompt window, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Overview of the DNS Query Process
- Installing the DNS Server Service
- Configuring Name Resolution for Client Computers
- Creating Zones
- Configuring Zones
- Configuring DNS for Internal Use
- Integrating DNS and DHCP
- Maintaining and Troubleshooting DNS Servers

*****ILLEGAL FOR NON-TRAINER USE*****

1. Describe the difference between an iterative query and a recursive query.

An iterative query is one in which the DNS server returns the best answer that it can provide without querying other DNS servers. A recursive query is one in which the DNS server returns a complete answer to the query.

2. What must you do before installing the DNS Server service?

You must configure the computer with a static IP address. You should also configure a DNS domain name before you install the DNS Server service.

3. How do you configure name resolution on a client computer?

You configure clients to use the DNS Server service by modifying the TCP/IP settings on the client computer.

4. What is a zone?

A zone is a contiguous portion of the domain namespace for which a DNS server has authority to resolve DNS queries.

5. What is the difference between a standard primary zone and a standard secondary zone?

A standard primary zone contains the master copy of a zone file, whereas a standard secondary zone is a replica of an existing zone file.

6. When is it necessary to create a root zone?

It is necessary to create a root zone only if you are configuring DNS in an intranet, or if you are using a proxy server to gain access to the Internet.

7. How can a caching-only server be used to help reduce traffic across a WAN?

Remote offices often have a limited amount of available bandwidth for connecting to the Internet or corporate headquarters across a WAN. A caching-only server can be used to reduce the traffic that the name resolution or zone transfer process generates.

