

Module 2: Implementing DNS to Support Active Directory

Contents

Overview	1
Introduction to the Role of DNS in Active Directory	2
DNS and Active Directory	3
DNS Name Resolution in Active Directory	7
Active Directory Integrated Zones	16
Installing and Configuring DNS to Support Active Directory	17
Lab A: Installing and Configuring DNS to Support Active Directory	22
Best Practices	30
Review	31



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, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT 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.

Instructor Notes

Presentation:
45 Minutes

Lab:
30 Minutes

This module provides students with the knowledge and skills to implement a Domain Name System (DNS) infrastructure in preparation for installing Microsoft® Windows® Active Directory® directory service. Students will learn about the roles of DNS in an Active Directory network, and about DNS and Active Directory namespaces. This module explains the process of DNS name resolution in Active Directory, and describes how to configure Active Directory to manage DNS zones. Students will also learn how to install and configure DNS to support an Active Directory installation.

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

- Describe the role of DNS in an Active Directory network.
- Describe the similarities and differences between the DNS namespace and the Active Directory namespace.
- Describe how client computers locate domain controllers in Windows 2000.
- Install and configure DNS to support an installation of Active Directory.
- Apply best practices for setting up DNS to support an installation of Active Directory.

In the hands-on lab in this module, students will have the opportunity to install and configure DNS in preparation for installing Active Directory.

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 2154A_02.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the topics related to Active Directory and DNS domain names in chapter 1, “Active Directory Logical Structure” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read chapter 3, “Name Resolution in Active Directory” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read the white paper, *Active Directory Architecture*, on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- **Introduction to the Role of DNS in Active Directory**

In this topic, you will introduce the role of DNS in Active Directory. Describe how DNS is integrated with Active Directory. Discuss the primary functions that DNS provides in an Active Directory network.
- **DNS and Active Directory**

In this topic, you will introduce DNS and Active Directory namespaces, DNS host names, and Windows 2000 computer names. First, explain the relationship between the DNS namespace and the Active Directory namespace. Emphasize how DNS can be used to locate computers that perform specific roles in an Active Directory domain by integrating the DNS and Active Directory namespaces. Next, point out that computers and domains have a DNS name and an Active Directory name. Explain that the DNS host name for a computer is the same name as that used for the computer account that is stored in Active Directory.
- **DNS Name Resolution in Active Directory**

In this topic, you will introduce DNS name resolution in Active Directory. Discuss how DNS is used to locate a Windows 2000 domain controller. Explain that Windows 2000 uses DNS SRV (service) resource records to locate domain controllers, and describe the format of an SRV record. Identify the SRV records registered by domain controllers during startup, and present information on how computers use DNS to locate domain controllers.
- **Active Directory Integrated Zones**

In this topic, you will introduce Active Directory integrated zones. Describe how to configure Active Directory to manage DNS zones, and discuss the benefits of Active Directory integrated zones.
- **Installing and Configuring DNS to Support Active Directory**

In this topic, you will introduce installing and configuring DNS to support Active Directory. First, discuss the DNS requirements for Active Directory. Next, present information on how to install and configure the DNS Server service in preparation for installing Active Directory. Finally, explain how the Active Directory Installation wizard installs and configures DNS.
- **Lab A: Installing and Configuring DNS to Support Active Directory**

Prepare students for the lab in which they will implement a DNS infrastructure that will support an installation of Active Directory. Students will install the DNS Server service, create forward and reverse lookup zones, enable dynamic update, and test DNS by using the **nslookup** command. After students have completed the lab, ask them if they have any questions.
- **Best Practices**

Present best practices for implementing DNS to support Active Directory. Emphasize the reason for each best practice.

Customization Information

This section identifies the lab setup requirements for the 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 lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

There are no lab setup requirements that affect replication or customization.

Lab Results

Performing the lab in this module introduces the following configuration changes:

- DNS is installed on all student computers.
- The primary DNS suffix of the student computers is *computerdom.nwtraders.msft* (where *computer* is the student's assigned computer name).
- The Preferred DNS server on the student computers is set to each student's Internet Protocol (IP) address.
- A forward lookup zone is created on each student computer.
- A reverse lookup zone is created on each student computer.
- Both the forward and reverse lookup zones are configured with dynamic update.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how DNS provides the location service in an Active Directory network. You will also learn how to configure DNS prior to installing Active Directory.

- Introduction to the Role of DNS in Active Directory
- DNS and Active Directory
- DNS Name Resolution in Active Directory
- Active Directory Integrated Zones
- Installing and Configuring DNS to Support Active Directory
- Best Practices

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

The integration of the Domain Name System (DNS) and Active Directory® directory service is a key feature of Microsoft® Windows® 2000. DNS and Active Directory use an identical hierarchical naming structure so that domains and computers are represented both as Active Directory objects and as DNS domains and resource records. The result of this integration is that computers in a Windows 2000 network use DNS to locate computers that provide specific Active Directory–related services. For example, when a user logs on from a client computer or needs to search Active Directory for a printer or shared folder, the client computer queries a DNS server to locate a domain controller. Windows 2000 also supports the integration of DNS zones in Active Directory, so that DNS primary zones can be stored in Active Directory for enhanced security and for replication to other domain controllers.

Windows 2000 requires that a DNS infrastructure is in place or is installed when you install Active Directory. Before you create Windows 2000 domains, you should understand how DNS and Active Directory are integrated, how client computers use DNS to locate domain controllers, and how to install and configure DNS to prepare for an Active Directory installation.

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

- Describe the role of DNS in an Active Directory network.
- Describe the similarities and differences between the DNS namespace and the Active Directory namespace.
- Describe how client computers locate domain controllers in Windows 2000.
- Install and configure DNS to support an installation of Active Directory.
- Apply best practices for setting up DNS to support an installation of Active Directory.

Introduction to the Role of DNS in Active Directory

Topic Objective

To introduce how DNS is integrated with Active Directory.

Lead-in

DNS provides a number of important functions in a Windows 2000 network.

■ Name Resolution

- DNS translates computer names to IP addresses
- Computers use DNS to locate each other on the network

■ Naming Convention for Windows 2000 Domains

- Windows 2000 uses DNS naming standards for domain names
- DNS domains and Active Directory domains share a common hierarchical naming structure

■ Locating the Physical Components of Active Directory

- DNS identifies domain controllers by the services they provide
- Computers use DNS to locate domain controllers and global catalog servers

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

DNS provides the following primary functions in an Active Directory network:

- *Name resolution.* DNS provides name resolution by translating computer names to Internet Protocol (IP) addresses so that computers can locate each other. A computer on a Windows 2000 network sends a DNS query containing the name of the computer it wants to locate to a DNS server. The DNS server resolves the query by looking in its local database or by forwarding the query to another DNS server. DNS also performs reverse name resolution by translating IP addresses to computer names.
- *Naming convention for Windows 2000 domains.* Active Directory uses DNS naming conventions to name Windows 2000 domains. In a Windows 2000 network, the names of DNS domains and Active Directory domains share a common hierarchical naming structure. For example, asia.contoso.msft is a valid DNS domain name and could also be the name of a Windows 2000 domain.
- *Locating the physical components of Active Directory.* DNS identifies domain controllers by the specific services that they provide, such as authenticating a logon request or performing an Active Directory search. A client computer uses this service-specific information to query DNS to locate a domain controller that provides the service.

For example, to log on to the network or to search Active Directory for published printers or folders, a computer running Windows 2000 first must locate a domain controller or global catalog server to process the logon authentication or the query. The DNS database stores information about which computers perform these roles.

◆ DNS and Active Directory

Topic Objective

To introduce the topics related to the integration of DNS and Active Directory in Windows 2000.

Lead-in

DNS domains and Active Directory domains use identical domain names for different namespaces.

- DNS and Active Directory Namespaces
- DNS Host Names and Windows 2000 Computer Names

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

The integration of DNS and Active Directory is a central feature of Windows 2000 Server. DNS domains and Active Directory domains use identical domain names for different namespaces. Using identical domain names enables computers in a Windows 2000 network to use DNS to locate domain controllers and other computers that provide Active Directory–related services.

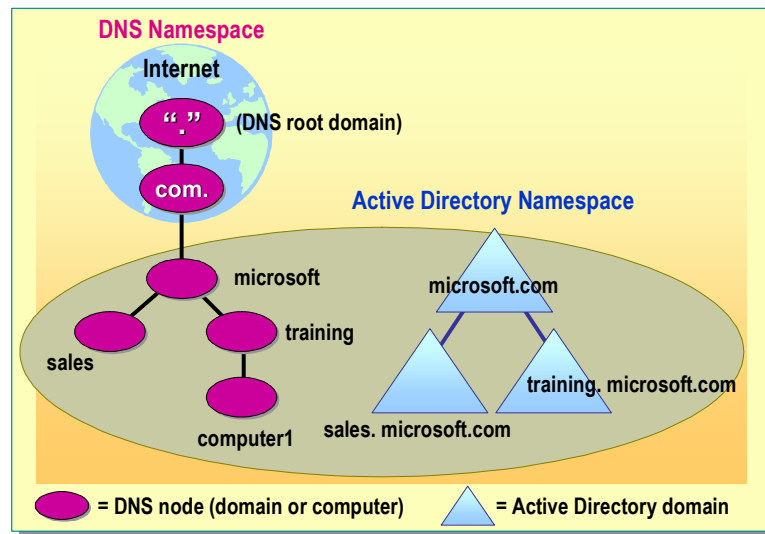
DNS and Active Directory Namespaces

Topic Objective

To illustrate the relationship between the DNS namespace and the Active Directory namespace.

Lead-in

In Windows 2000, DNS domains and Active Directory domains have the same hierarchical naming structures.



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

Key Points

In the Active Directory namespace, Active Directory objects represent the same domains and computers that exist as nodes in the DNS namespace.

The DNS and Active Directory namespaces use an identical naming structure so that domains and computers can be represented both as DNS nodes and Active Directory objects.

A *namespace* is a hierarchical naming structure in which the names in the namespace can be resolved to the objects that they represent. In Windows 2000, DNS domains and Active Directory domains have the same hierarchical naming structure, but they represent two different namespaces because they store different information about the same physical objects.

In the DNS namespace, zones store name information about one or more DNS domains. A *DNS zone* is a contiguous portion of the domain namespace for which a DNS server has authority to resolve DNS queries. A zone stores the resources records for the domains and computers in that zone. *Resource records* represent computers, and contain the information necessary for a DNS server to resolve DNS queries. Note that DNS zones can store information about computers that are joined to different Active Directory domains.

In the Active Directory namespace, Active Directory objects represent the same domains and computers that exist as nodes in the DNS namespace. Therefore, DNS domains and Active Directory domains share identical names.

In other words, the DNS and Active Directory namespaces use an identical naming structure so that domains and computers can be represented both as DNS nodes and Active Directory objects. For example, a Windows 2000 domain with a name training.microsoft.com also has a DNS domain name, which is training.microsoft.com. The advantage of integrating the DNS and Active Directory namespaces is that DNS can be used to locate computers that play specific roles in an Active Directory domain.

Active Directory and the Internet

The integration of DNS and Active Directory also enables the Active Directory domain structure to exist within the scope of the Internet namespace. This is possible because the global DNS namespace provides the hierarchical naming structure of the Internet. If your organization requires an Internet presence, then it must register the DNS name that will be used as the name of the root domain in the Active Directory domain structure.

When the root domain of your Active Directory domain structure has a DNS domain name that is registered, then resource records in the relevant top-level domains in the global Internet namespace point to DNS servers that are authoritative for your root domain. For example, name servers that are authoritative for the .com DNS database contain resource records for DNS name servers in the root domain of microsoft.com. These resource records enable external domains to use the Internet to find the microsoft.com domain. Similarly, the DNS name servers in your network can contain resource records for Internet name servers if you want to be able to locate other domains on the Internet.

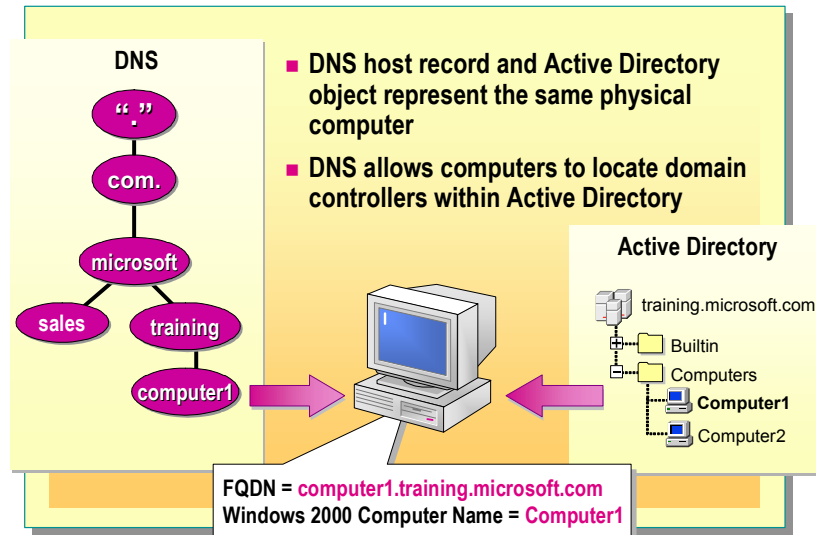
DNS Host Names and Windows 2000 Computer Names

Topic Objective

To describe how computers and domains have a DNS name and an Active Directory name.

Lead-in

Because DNS and Active Directory use identical domain names, the same DNS host name for a computer is used for the computer account that is stored in Active Directory.



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

Key Points

The DNS host name for a computer is the same name that is used for the computer account that is stored in Active Directory.

The Windows 2000 computer name is the relative distinguished name of the Active Directory object.

Because Windows 2000 integrates DNS and Active Directory, domains and computers are represented by resource records in the DNS namespace, and by Active Directory objects in the Active Directory namespace. Therefore, the DNS host name for a computer is the same name as that is used for the computer account that is stored in Active Directory. Note that the Windows 2000 computer name is the relative distinguished name of the Active Directory object. The DNS domain name, which is called the *primary DNS suffix*, is also the same as the name of the Active Directory domain to which the computer is joined.

In other words, a computer is represented in the DNS namespace and the Active Directory namespace by the same name. For example, a computer named Computer1 that is joined to the Active Directory domain named training.microsoft.com has the following fully qualified domain name (FQDN):

computer1.training.microsoft.com

The integration of DNS and Active Directory is essential because a client computer in a Windows 2000 network must be able to locate a domain controller to use the services provided by Active Directory. To locate a domain controller, a computer uses DNS to locate the IP address for a computer that provides the required service within Active Directory.

Note In Windows 2000, the FQDN for a computer is also called the *full computer name*.

◆ DNS Name Resolution in Active Directory

Topic Objective

To introduce the topics related to DNS name resolution in Active Directory.

Lead-in

Now that you understand the relationship between the DNS and Active Directory namespaces, let's discuss how DNS is used to locate a Windows 2000 domain controller.

- **SRV (Service) Resource Records**
- **SRV Record Format**
- **SRV Records Registered by Domain Controllers**
- **How Computers Use DNS to Locate Domain Controllers**

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

In addition to being identified by an FQDN in DNS and by a Windows 2000 full computer name, domain controllers are also identified by the specific services that they provide. Windows 2000 uses DNS to locate domain controllers by resolving a domain or computer name to an IP address. This is accomplished by SRV (service) resource records, which map a particular service to the domain controller that provides that service. The format of an SRV record contains this information, as well as Transmission Control Protocol/Internet Protocol (TCP/IP) specific information.

When a domain controller starts up, the Net Logon service running on the domain controller uses the DNS dynamic update feature to register with the DNS database the SRV records for all Active Directory–related services that the domain controller provides. Therefore, a computer running Windows 2000 can query a DNS server when it needs to contact a domain controller.

Note For more information about DNS name resolution in Active Directory, see chapter 3, “Name Resolution in Active Directory” in the Distributed Systems Guide in the Microsoft Windows 2000 Server Resource Kit.

SRV (Service) Resource Records

Topic Objective

To explain that Windows 2000 uses DNS SRV records to locate domain controllers.

Lead-in

In Windows 2000, SRV resource records are used to locate a computer that provides a specific service.

- **SRV Records Allow Computers to Locate Domain Controllers**
- **Information in SRV Records Maps DNS Computer Names to the Service**
- **Windows 2000 Uses SRV Records to Locate:**
 - A domain controller in a specific domain or forest
 - A domain controller in the same site as a client computer
 - A domain controller configured as a global catalog server
 - A computer configured as a Kerberos KDC server
- **DNS Servers Use the Information in the SRV Record and the A Resource Record to Locate Domain Controllers**

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

Key Points

SRV records allow client computers to locate servers that provide specific Active Directory services.

SRV records link the name of a service to the DNS computer name for the domain controller that offers that service.

For Active Directory to function properly, DNS servers must provide support for SRV (service) resource records. *SRV records* allow client computers to locate servers that provide specific services such as authenticating logon requests and searching for information in Active Directory. Windows 2000 uses SRV records to identify a computer as a domain controller. SRV records link the name of a service to the DNS computer name for the domain controller that offers that service.

SRV records also contain information that enables a DNS client to locate the following:

- A domain controller located in a specific Windows 2000 domain or forest.
- A domain controller located in the same site as a client computer.
- A domain controller that is configured as global catalog server.
- A computer that runs the Kerberos Key Distribution Center (KDC) service.

SRV Records and A Resource Records

When a domain controller starts up, it registers SRV records, which contain information about the services it provides, and an A resource record that contains its DNS computer name and its IP address. A DNS server then uses this combined information to resolve DNS queries and return the IP address of a domain controller so that the client computer can locate the domain controller.

Note In Windows 2000, domain controllers are also referred to Lightweight Directory Access Protocol (LDAP) servers because they run the LDAP service that responds to requests to search for or modify objects in Active Directory.

SRV Record Format

Topic Objective

To describe the format of an SRV record.

Lead-in

Let's look at the format of an SRV record, which contains the information necessary to locate domain controllers.

Field	Description
Service	Specifies the name for the service
Protocol	Indicates the transport protocol type
Name	Specifies the domain name referenced by the resource record
Ttl	Specifies the standard DNS resource record Time to Live value
Class	Specifies the standard DNS resource record class value
Priority	Specifies the priority of the host
Weight	Specifies the load balancing mechanism
Port	Shows the port of the service on this host
Target	Specifies the FQDN for the host supporting the service

<code>_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft.</code>
--

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

Key Point

An SRV record uses a format that consists of fields containing the information used to map a specific service to the computer that provides the service.

All SRV records use a standard format, which consists of fields that contain the information used to map a specific service to the computer that provides the service. SRV records use the following format:

_service._protocol.name ttl class SRV priority weight port target

The following table describes each field in an SRV record:

Field	Description
<i>_Service</i>	Specifies the name of the service, such as LDAP or Kerberos, provided by the server that registers this SRV record.
<i>_Protocol</i>	Specifies the transport protocol type, such as TCP or User Datagram Protocol (UDP).
<i>Name</i>	Specifies the domain name referenced by the resource record.
<i>Ttl</i>	Specifies the Time to Live (TTL) value (in seconds), which is a standard field in DNS resource.
<i>Class</i>	Specifies the standard DNS resource record class value, which is almost always "IN" for the Internet system.
<i>Priority</i>	Specifies the priority of the server. Clients attempt to contact the host with the lowest priority.
<i>Weight</i>	Denotes a load balancing mechanism that clients use when selecting a target host. When the priority field is the same for two or more records in the same domain, clients randomly choose SRV records with higher weights.
<i>Port</i>	Specifies the port where the server is "listening" for this service.
<i>Target</i>	Specifies the fully qualified domain name (FQDN), which is also called the full computer name, of the computer providing the service.

For example, the following SRV record:

_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft.

would be registered by a computer that:

- Provides the LDAP service
- Provides the LDAP service by using the TCP transport protocol
- Registers the SRV record in the contoso.msft DNS domain
- Has an FQDN of london.contoso.msft

SRV Records Registered by Domain Controllers

Topic Objective

To identify the SRV records registered by domain controllers during startup.

Lead-in

Now that you understand the information contained in an SRV record, let's look at the specific SRV records registered by domain controllers.

SRV Record	Lookup Criteria
<u>ldap._tcp.DnsDomainName.</u>	Allows a computer to find an LDAP server in the domain
<u>_ldap._tcp.SiteName._sites.dc._msdcs.DnsDomainName.</u>	Allows a computer to find a domain controller in the same site
<u>_gc._tcp.DnsForestName.</u>	Allows a computer to find a global catalog server
<u>_gc._tcp.SiteName._sites.DnsForestName.</u>	Allows a computer to find a global catalog server in the same site
<u>_kerberos._tcp.DnsDomainName.</u>	Allows a computer to locate a KDC server in the domain
<u>_kerberos._tcp.SiteName._sites.DnsDomainName.</u>	Allows a computer to locate a KDC server in the same site

■ Domain Controllers Running Windows 2000 Register Additional SRV Records in the **_msdcs** Subdomain in the Format of:
_Service._Protocol.DcType._msdcs.DnsDomainName

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

Delivery Tip

Use the DNS snap-in to show students SRV records and the **_msdcs** subdomain.

Explain that LDAP servers and global catalog servers are not always Windows 2000 domain controllers.

Tell students that *SiteName* is the relative distinguished name of the site object that is stored in Active Directory.

Refer students to the *Windows 2000 Server Resource Kit* for a complete list of SRV records registered by domain controllers.

Key Point

The service and name components of SRV records are examples of how the integration of DNS and Active Directory is implemented to map services to the specific domain controller that provides the service.

When a domain controller starts up, the Net Logon service running on the domain controller uses dynamic updates to register SRV resource records in the DNS database. These SRV records map the name of the service provided by the domain controller to the DNS computer name for that domain controller. The following table lists some of the SRV records registered by domain controllers and defines the lookup criteria that each record supports.

SRV Record	Lookup Criteria
<u>_ldap._tcp.DnsDomainName.</u>	Allows a computer to find an LDAP server in the domain named by <i>DnsDomainName</i> . All domain controllers register this record.
<u>_ldap._tcp.SiteName._sites.dc._msdcs.DnsDomainName.</u>	Allows a computer to find a domain controller in the domain named by <i>DnsDomainName</i> and in the site named by <i>SiteName</i> . Note that <i>SiteName</i> is the relative distinguished name of the site object that is stored in Active Directory. All domain controllers register this record.
<u>_gc._tcp.DnsForestName.</u>	Allows a computer to find a global catalog server in the forest named by <i>DnsForestName</i> . Note that <i>DnsForestName</i> is the domain name of the forest root domain. Only domain controllers configured as global catalog servers register this record.

(continued)

SRV Record	Lookup Criteria
<i>_gc._tcp.SiteName._sites.DnsForestName.</i>	Allows a computer to find a global catalog server in the forest named <i>DnsForestName</i> and in the site named by <i>SiteName</i> . Only domain controllers configured as global catalog servers register this record.
<i>_kerberos._tcp.DnsDomainName.</i>	Allows a computer to locate a KDC server for the domain named by <i>DnsDomainName</i> . All domain controllers running the Kerberos version 5 service register this record.
<i>_kerberos._tcp.SiteName._sites.DnsDomainName.</i>	Allows a computer to locate a KDC server for the domain named by <i>DnsDomainName</i> and in the site named by <i>SiteName</i> . All domain controllers running the Kerberos V5 service register this record.

Note In addition to Windows 2000 domain controllers, a network can contain computers that are configured as LDAP servers and global catalog servers that are not running Windows 2000. Therefore, any computer that provides appropriate services registers the SRV records listed in the previous table.

SRV Records Registered Only by Windows 2000 Domain Controllers

To enable a computer to locate domain controllers running Windows 2000, the Net Logon service registers SRV records that identify domain controllers that provide Windows 2000–specific services in the domain or forest. Therefore, in addition to the SRV records listed above, domain controllers running Windows 2000 also register SRV records in the following format:

_Service._Protocol.DcType._msdcs.DnsDomainName or DnsForestName

The *_msdcs* component in these SRV records denotes a subdomain in the DNS namespace that is specific to Microsoft, which allows computers to locate domain controllers that have functions in the domain or forest that are specific to Windows 2000.

The possible values for the *DcType* component, which is a prefix to the *_msdcs* subdomain, specify the following server roles types:

- **dc** for a domain controller
- **gc** for global catalog server

The presence of the `_msdcs` subdomain means that domain controllers running Windows 2000 also register the following SRV records:

`_ldap._tcp.dc._msdcs.DnsDomainName.`

`_ldap._tcp.SiteName._sites.dc._msdcs.DnsDomainName.`

`_ldap._tcp.gc._msdcs.DnsForestName.`

`_ldap._tcp.SiteName._sites.gc._msdcs.DnsForestName.`

`_kerberos._tcp.dc._msdcs.DnsDomainName.`

`_kerberos._tcp.SiteName._sites.dc._msdcs.DnsDomainName.`

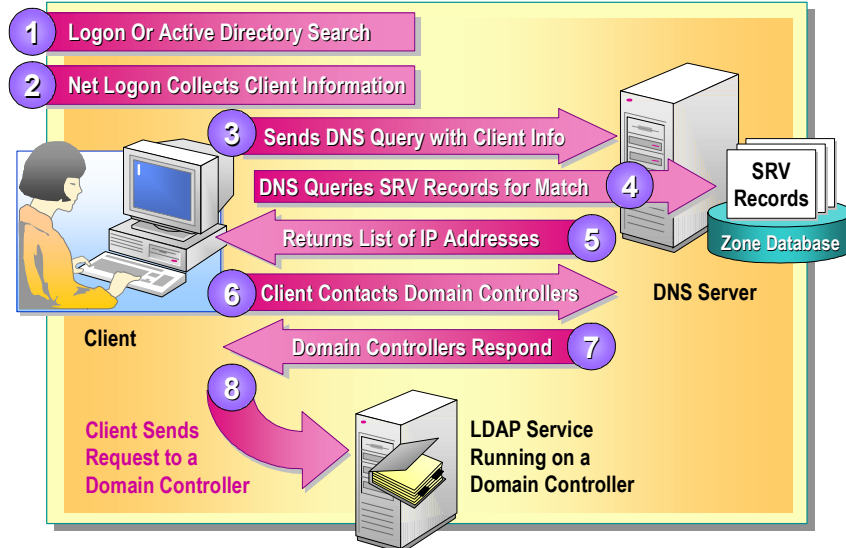
How Computers Use DNS to Locate Domain Controllers

Topic Objective

To illustrate how a computer locates a Windows 2000 domain controller.

Lead-in

Computers query DNS to locate Windows 2000 domain controllers.



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

To log on to a Windows 2000 domain or to search Active Directory, a client computer must contact a domain controller. All domain controllers register both *A resource records* and *SRV records*. The *A resource record* contains the FQDN and IP address for the domain controller. The *SRV record* contains the FQDN of the domain controller and the name of the service that the domain controller. Therefore, the client computer can query DNS to locate a domain controller.

The following describes the process of how a computer locates a domain controller:

1. A user logs on to the domain, initiates an Active Directory search, or performs other tasks that require a domain controller. The Net Logon service on the client (the computer that is locating the domain controller) starts the DsGetDcName application programming interface (API).
2. Net Logon collects information about the client and the specific service required; this information will be included in the DNS query. This information is specified by the following DsGetDcName parameters:
 - *ComputerName*. The name of the client computer.
 - *DomainName*. The name of the DNS domain that will be queried.
 - *SiteName*. The name of the site in which the domain controller should be located. If the site is not specified, the domain controller that will be located is in the site that is closest to the site in which the client computer is located.

The client also specifies that the domain controller should be an LDAP server in the domain named by *DomainName*, or a global catalog server or KDC server for the forest in which *DomainName* is located.

3. The Net Logon service sends a DNS query to a DNS server. This DNS query contains the information it collected from the client and specifies the service that is required.

4. The DNS server queries the DNS zone database for SRV records that match the service required by the client in the domain named by *DomainName*.
5. The DNS server returns a list of IP addresses of domain controllers that provide the service requested in the domain specified by the client.
6. The Net Logon service sends a datagram (an LDAP UDP message) to one or more of the located domain controllers to determine whether it is running and whether it supports the specified domain.
7. Each available domain controller responds to the datagram to indicate that it is currently operational, and then returns the information to DsGetDcName. The Net Logon service returns the information to the client from the domain controller that responds first.
8. The client computer chooses the first domain controller that responds and meets the criteria, and then sends the request to that domain controller.

The Net Logon service caches the domain controller information so that it is not necessary that the client computer repeat the discovery process for subsequent requests. Caching this information also encourages the consistent use of the same domain controller.

Active Directory Integrated Zones

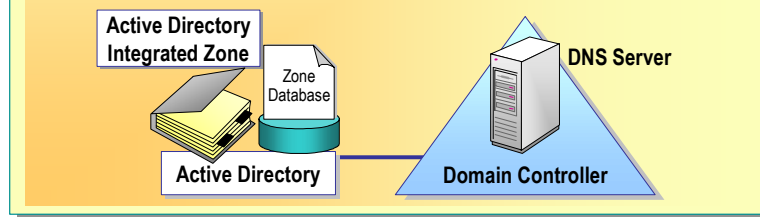
Topic Objective

To describe how to configure Active Directory to manage DNS zones.

Lead-in

When you implement DNS in Windows 2000, you have the option of using the services in Active Directory as the data storage and replication engine.

- **Store Primary Zones in Active Directory**
- **Replicate DNS Zone Information During Active Directory Replication**
- **Provide Additional Benefits:**
 - Eliminates a primary DNS server as a single point of failure
 - Enables secure dynamic updates
 - Performs standard zone transfers to other DNS servers



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

Tell students that the zone database files for Active Directory integrated zones are not stored in the `systemroot\System32\Dns` folder, where the standard zone database files are stored.

Key Points

Active Directory integrated zones can be created only on DNS servers that are configured to run the DNS dynamic update protocol.

Active Directory integrated zones are stored in Active Directory.

One of the benefits of integrating DNS and Active Directory is the capability to integrate DNS zones into the Active Directory database. *Active Directory integrated zones* are primary DNS zones that are stored as an object in the Active Directory database. A zone is a portion of the domain namespace that is defined by the resource records that are stored in a zone database file. A zone database file stores information that is used to resolve host names to IP addresses and IP addresses to host names. Therefore, when you configure Active Directory integrated zones, the zone database file is replicated during Active Directory replication rather than through DNS zone transfers.

An Active Directory integrated zone provides the following benefits:

- Eliminates a primary DNS server as a single point of failure. Because DNS replication is single-master, it relies on a primary DNS server to update all of the secondary servers. In contrast, Active Directory replication is multi-master, so an update can be made to any domain controller, and the change will be replicated to all other domain controllers. Therefore, if you integrate a DNS zone with Active Directory, Active Directory replication will always synchronize the DNS zone information.
- Enables secure dynamic updates. Because DNS zones are Active Directory objects in Active Directory integrated zones, you can set permissions on records within those zones to control which computers can update their records. Therefore, updates that use the dynamic update protocol can come from only authorized computers.
- Performs standard zone transfers to DNS servers that are not configured as domain controllers and performs standard zone transfers to DNS servers that are in other domains. You must use standard zone transfers to replicate the zones to DNS servers in other domains.

Important Active Directory must first be installed before you can configure Active Directory integrated zones.

◆ Installing and Configuring DNS to Support Active Directory

Topic Objective

To introduce the topics related to installing and configuring DNS to support an installation of Active Directory.

Lead-in

Implementing an Active Directory infrastructure requires that a DNS infrastructure be in place or installed during Active Directory installation.

- DNS Requirements for Active Directory
- Installing and Configuring DNS
- Installing DNS During the Active Directory Installation

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

Implementing an Active Directory infrastructure requires that a DNS infrastructure be in place or installed during Active Directory installation. To support Active Directory, your DNS implementation must support SRV records.

To implement DNS, you need to install DNS and configure the forward and reverse lookup zones. Because DNS domain names correspond to Active Directory domain names, you can configure your forward and reverse lookup zones so that they correspond to your Active Directory domains. However, DNS zones can also include data about computers in one or more Active Directory domains, so zones can also encompass more than one Active Directory domain.

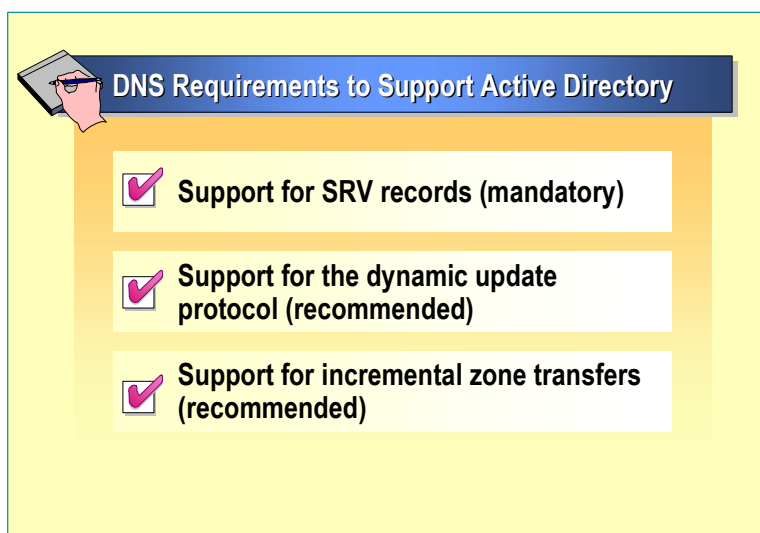
DNS Requirements for Active Directory

Topic Objective

To describe the DNS requirements necessary to support Active Directory.

Lead-in

To enable DNS function as the location service for Active Directory, you must implement a DNS server that supports SRV resource records.



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

Key Points

The DNS server you choose must support service location SRV resource records.

You cannot install Active Directory without having DNS on your network because Active Directory uses DNS as its location service. For DNS to function as a location service for Active Directory, you must have a DNS server that supports SRV resource records.

The version of DNS included with Windows 2000 provides the requirements necessary to support an installation of Active Directory. If you choose not to use Windows 2000 DNS, you need to determine if your DNS server provides the following support:

- *SRV records* (RFC 2052). SRV records are DNS records that map to the name of a server offering a particular service. If your existing DNS server does not support SRV records, you must switch to a DNS server that does, or delegate the domains used by Active Directory to a DNS server that supports SRV records.
- *Dynamic update protocol* (RFC 2136). The dynamic update protocol is optional but is highly recommended because it enables the servers and clients in your environment to add records to the DNS database automatically, which reduces administration costs. If you are using a DNS server that supports SRV resource records and does not support the dynamic update protocol, you must enter the SRV resource records manually. When you install Active Directory on a computer, a file containing the required SRV resource records is created as part of the installation process. This file is called Netlogon.dns and is located in the *systemroot\System32\Config* folder.
- *Incremental zone transfers* (RFC 1995). An incremental zone transfer is optional, and allows only new or modified resource records to be replicated between DNS servers, rather than to the entire zone database file.

Note To obtain a copy of RFC 2052, RFC 2136, or RFC 1995, see the Internet Engineering Task Force Web page at <http://www.ietf.org>.

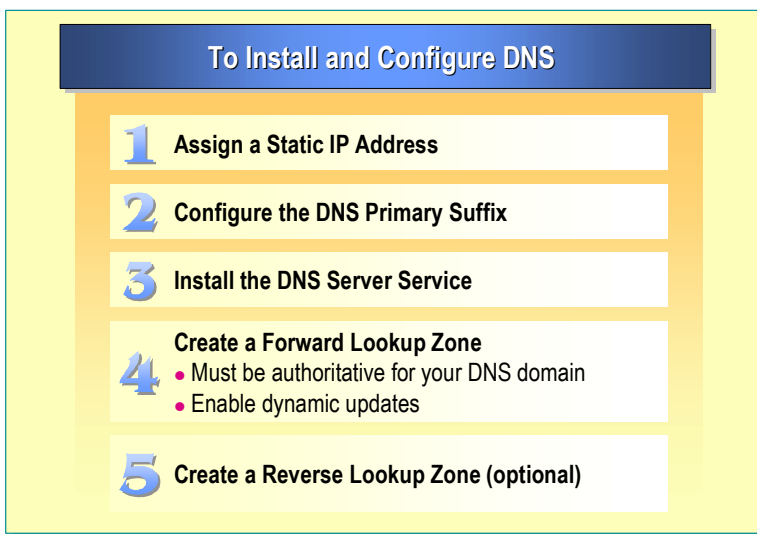
Installing and Configuring DNS

Topic Objective

To describe how to install and configure the DNS Server service in preparation for installing Active Directory.

Lead-in

It is recommended that you implement a DNS infrastructure before you install Active Directory.



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

To implement a DNS infrastructure before you install Active Directory, you must install and configure the DNS Server service on a computer running Windows 2000 Server.

► **To install and configure DNS:**

1. Assign a static IP address. You must configure the computer with a static IP address before you install the DNS Server service.
2. Configure the DNS primary suffix. If you are creating the first DNS server in your organization, the DNS primary suffix should be the same name that you will use for the forest root of your Active Directory forest.
3. Install the DNS Server service. Use the DNS Installation wizard to install the DNS Server service.
4. Create a standard primary forward lookup zone.
 - This zone must be authoritative for the name of the first Active Directory domain that you will create.
 - Configure the forward lookup zone to enable dynamic updates.
5. Create a standard primary reverse lookup zone (optional). A reverse lookup zone is not required during the Active Directory installation, but it is a best practice to create a reverse lookup zone so that IP addresses can be resolved to computer names. If you create a reverse lookup zone, you should also configure it to enable dynamic updates.

Verifying the DNS Server is Authoritative

After you have installed and configured the DNS server, use the following command to verify that this DNS server is authoritative for the DNS domain name that you will use to name your first Active Directory domain:

nslookup -type=ns *DnsDomainName*

The results of this command list the FQDN of the DNS servers that are authoritative for the DNS domain named by *DnsDomainName*.

Installing DNS During the Active Directory Installation

Topic Objective

To describe the process of creating a DNS server during the Active Directory installation.

Lead-in

If you do not have a DNS infrastructure in place when you create your first Active Directory domain, you can use the Active Directory Installation wizard to install and configure DNS during the Active Directory installation.

- **The Active Directory Installation Wizard Prompts You to Install and Configure a Local DNS Server if It Does Not Find an Existing DNS Infrastructure**

To Implement DNS, the Active Directory Wizard:

- 1** Installs the DNS Server Service
- 2** Creates a Forward Lookup Zone
- 3** Configures the Zone As Active Directory Integrated
- 4** Enables Secure Dynamic Updates for the Zone

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

If you do not have a DNS infrastructure in place at the time when you create the first domain, which is the forest root domain, in your Windows 2000 forest, the Active Directory Installation wizard can install and configure the DNS Server service on the computer on which you are installing Active Directory.

The following describes how the Active Directory Installation wizard installs and configures DNS:

1. If the Active Directory Installation wizard cannot find the DNS server that is authoritative for the name of the new Active Directory domain, or if the DNS server it finds does not support dynamic updates or is not configured to accept dynamic updates, the wizard asks you whether you want the wizard to automatically install and configure a local DNS server.
2. If you answer yes, the Active Directory Installation wizard performs the following tasks to install and configure DNS:
 - a. Installs the DNS Server service.
 - b. Creates a forward lookup zone with the same name as the Active Directory domain you are creating.
 - c. Configures the forward lookup zone as an Active Directory integrated zone.
 - d. Enables secure dynamic updates on the forward lookup zone.

Note that the Active Directory Installation wizard does not create a reverse lookup zone. If you want a reverse lookup zone, you will need to create one after you complete the Active Directory installation.

Lab A: Installing and Configuring DNS to Support Active Directory

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will implement a DNS infrastructure that will support an installation of Active Directory.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install the DNS Server service.
- Create forward and reverse lookup zones.
- Enable dynamic update.
- Test DNS by using the **nslookup** command.

Prerequisites

Before working on this lab, you must have familiarity with DNS concepts and operations.

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.

Lab Setup

To complete this lab, you need the following:

- A computer running Microsoft Windows 2000 Advanced Server that is configured as a standalone server.
- A static IP address and subnet mask.
- A DNS domain name, a name for the forward lookup zone, and a name for the reverse lookup zone. Refer to the table on the next page for this information.

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.

Forward and Reverse Lookup Zone Information

During this lab, you will be asked to enter a name for the primary DNS suffix and the forward lookup zone, and a network ID for the reverse lookup zone. Use the information from the following table to determine what to enter for these values based on the computer that you are using. Your instructor will provide the number to use in place of the *x* in the network ID value.

Computer Name	Network ID	DNS Domain Name	Forward Lookup Zone Name (DNS Primary Suffix)
Vancouver	192.168.x	vancouverdom	vancouverdom.nwtraders.msft
Denver	192.168.x	denverdom	denverdom.nwtraders.msft
Perth	192.168.x	perthdom	perthdom.nwtraders.msft
Brisbane	192.168.x	brisbanedom	brisbanedom.nwtraders.msft
Lisbon	192.168.x	lisbondom	lisbondom.nwtraders.msft
Bonn	192.168.x	bonndom	bonndom.nwtraders.msft
Lima	192.168.x	limadom	limadom.nwtraders.msft
Santiago	192.168.x	santiagodom	santiagodom.nwtraders.msft
Bangalore	192.168.x	bangaloredom	bangaloredom.nwtraders.msft
Singapore	192.168.x	singaporedom	singaporedom.nwtraders.msft
Casablanca	192.168.x	casablancadom	casablancadom.nwtraders.msft
Tunis	192.168.x	tunisdom	tunisdom.nwtraders.msft
Acapulco	192.168.x	acapulcodom	acapulcodom.nwtraders.msft
Miami	192.168.x	miamidom	miamidom.nwtraders.msft
Auckland	192.168.x	aucklanddom	aucklanddom.nwtraders.msft
Suva	192.168.x	suvadom	suvadom.nwtraders.msft
Stockholm	192.168.x	stockholmdom	stockholmdom.nwtraders.msft
Moscow	192.168.x	moscowdom	moscowdom.nwtraders.msft
Caracas	192.168.x	caracasdom	caracasdom.nwtraders.msft
Montevideo	192.168.x	montevideodom	montevideodom.nwtraders.msft
Manila	192.168.x	maniladom	maniladom.nwtraders.msft
Tokyo	192.168.x	tokyodom	tokyodom.nwtraders.msft
Khartoum	192.168.x	khartoumdom	khartoumdom.nwtraders.msft
Nairobi	192.168.x	nairobidom	nairobidom.nwtraders.msft

Estimated time to complete this lab: 30 minutes

Exercise 1

Installing the DNS Server Service

Scenario

You have determined that to successfully deploy Active Directory, you first need to deploy a DNS infrastructure to support Active Directory.

Goal

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

Tasks	Detailed Steps
1. Configure the DNS suffix for your computer. When prompted, restart the computer. Domain Suffix: <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name)	- Log on as Administrator with a password of password. - Open the Properties dialog box for My Computer. - In the System Properties dialog box, on the Network Identification tab, click Properties. - In the Identification Changes dialog box, click More. - In the DNS Suffix and NetBIOS Computer Name dialog box, in the Primary DNS suffix of this computer box, type <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), and then click OK. - Click OK to close the Identification Changes dialog box, and then click OK to close the Network Identification message box. - Click OK to close the System Properties dialog box, and then click Yes in the System Settings Change message box to restart your computer.
2. Start the Windows Components wizard, and install the Domain Name System (DNS) subcomponent of Networking Services. Copy the required files from the Windows 2000 Advanced Server compact disc.	- Log on as Administrator with a password of password. - In Control Panel, double-click Add/Remove Programs, and then click Add/Remove Windows Components. - On the Windows Components page, under Components, click Networking Services, and then click Details. - Under Networking Services, verify that all check boxes are cleared, select the Domain Name System (DNS) check box, and then click OK. - In the Windows Components wizard, click Next. - If prompted, insert the compact disc labeled Windows 2000 Advanced Server, and then click OK. - After the required files have been copied, click Finish, and then close all windows.

Exercise 2

Creating Forward and Reverse Lookup Zones

Scenario

After installing DNS, you must configure a forward lookup zone to resolve host names to IP addresses and a reverse lookup zone to resolve IP addresses to host names.

Goal

In this exercise, you will configure a forward lookup zone for your domain and a reverse lookup zone for your network ID.

Tasks	Detailed Steps
1. Add a standard primary forward lookup zone for <i>domain.nwtraders.msft</i> .	- Click Start, point to Programs, point to Administrative Tools, and then click DNS. - In the console tree, right-click <i>computer</i> (where <i>computer</i> is your computer name), 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, ensure 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 your assigned domain name) and then click Next. - On the Zone File page, ensure that Create a new file with this file name is selected, and then click Next.
2. Add a standard primary reverse lookup zone for your network ID.	- On the Reverse Lookup Zone page, ensure that Yes, create a reverse lookup zone is selected, and then click Next. - On the Zone Type page, click Standard primary, and then click Next. - On the Reverse Lookup Zone page, verify that Network ID is selected. For the network ID, type the first three octets of the IP address of your computer, and then click Next. (For example, for an IP address of 192.168.1.1, type 192.168.1) - On the Zone File page, ensure that Create a new file with this file name is selected, and then click Next. - On the Completing the Configure DNS Server Wizard page, click Finish. - Leave DNS open.

Tasks	Detailed Steps
3. Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use your computer for DNS.	a. Right-click My Network Places, and then click Properties. b. Right-click Local Area Connection, and then click Properties. c. Click Internet Protocol (TCP/IP), and then click Properties. d. In the Preferred DNS Server box, type your assigned IP address, and then click OK. e. Click OK to close the Local Area Connections Properties box, and then close the Network and Dial-up Connections window.

Exercise 3

Configuring DNS to Support Dynamic Update

Scenario

After installing DNS and creating forward and reverse lookup zones, you must now configure DNS to support dynamic updates before you deploy Active Directory.

Goal

In this exercise, you will configure the forward and reverse lookup zones to support dynamic update.

Tasks	Detailed Steps
1. Configure the forward lookup zone for <i>domain.nwtraders.msft</i> to support dynamic update.	- In the console tree of DNS, expand <i>computer</i> (where <i>computer</i> is your assigned computer name). - In the console tree, expand Forward Lookup Zone, and then click <i>domain.nwtraders.msft</i>. - Right-click <i>domain.nwtraders.msft</i>, and then click Properties. - In the <i>domain.nwtraders.msft</i> Properties box, in the Allow dynamic updates list, click Yes, and then click OK.
2. Configure the reverse lookup zone for your subnet to support dynamic update.	- In the console tree, expand Reverse Lookup Zone, and then click 192.168.y.x Subnet (where <i>y</i> is your assigned classroom number). - Right-click 192.168.y.x Subnet, and then click Properties. - In the 192.168.y.x Subnet Properties box, in the Allow dynamic updates list, click Yes, and then click OK. - Leave DNS open.
3. Use the ipconfig command to re-register your computer's DNS records.	- Open a command prompt. - At the command prompt, type ipconfig /registerdns and then press ENTER. - Close the command prompt.
4. Refresh DNS to display the pointer resource record in the reverse lookup zone.	- Switch to the DNS window. - On the Action menu, click Refresh.  Notice that a new pointer resource record appears in the 192.168.y.x Subnet reverse lookup zone. - Close all open windows.

Exercise 4

Using Nslookup to Test DNS

Scenario

After installing DNS, creating forward and reverse lookup zones, and configuring the zones to allow dynamic updates, you have decided to test DNS prior to installing Active Directory to ensure that it is functioning properly.

Goal

In this exercise, you will use the **nslookup** command to confirm that DNS is properly installed and configured.

Tasks	Detailed Steps
1. Confirm that DNS can resolve a host name to an IP address.	- Open a command prompt. - At the command prompt, type nslookup <i>computer.domain.nwtraders.msft</i> (where <i>computer</i> is your assigned computer name and <i>domain</i> is your assigned domain name), and then press ENTER.  <i>The DNS server responds with its name and IP address, followed by the name and IP address of the computer name provided on the command line.</i> - Leave the command prompt open.
2. Confirm that DNS can resolve an IP address to a host name.	- At the command prompt, type nslookup ip_address (where <i>ip_address</i> is your assigned IP address), and then press ENTER.  <i>The DNS server responds with its name and IP address, followed by the name and IP address for the IP address provided on the command line.</i> - Close all open windows, and then log off.

Best Practices

Topic Objective

To describe best practices for implementing DNS to support Active Directory.

Lead-in

Review this checklist before you implement DNS to support Active Directory.



Use Standard DNS Guidelines When Implementing DNS



Use at Least Two DNS Servers to Host Each Zone



Implement Active Directory Integrated Zones



Configure Client Computers to Use DNS Servers Located Nearby

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

Consider the following best practices for implementing DNS to support Active Directory:

- Use standard DNS guidelines and preferred practices when planning and implementing your DNS infrastructure.
- Make sure that at least two DNS servers host each zone. They can host either primary and secondary copies of the zone, or two directory-integrated copies of each zone. This provides fault tolerance in case one of your DNS servers is not available.
- Implement Active Directory integrated zones. Active Directory integrated zones ensure that the domain controllers for each of your Active Directory domains correspond in a direct one-to-one mapping to DNS servers. When you troubleshoot DNS and Active Directory replication problems, the same server computers are used in both topologies, which simplifies planning, deployment, and troubleshooting.

If you do not use Active Directory integrated zones, be sure to correctly configure your clients and understand that a standard primary zone becomes a single point of failure for dynamic updates and for zone replication.

- Configure client computers to use domain controllers located near the client computer as the preferred and alternate DNS servers. When you configure a list of preferred and alternate DNS servers for each client, you can specify servers corresponding to domain controllers located near each client computer.

Note For more information about planning your DNS infrastructure to support Active Directory, see Module 2, “Designing an Active Directory Naming Strategy” in Course 1561B, *Designing a Microsoft® Windows® 2000 Directory Services Infrastructure*.

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.

- Introduction to the Role of DNS in Active Directory
- DNS and Active Directory
- DNS Name Resolution in Active Directory
- Active Directory Integrated Zones
- Installing and Configuring DNS to Support Active Directory
- Best Practices

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

Give students time to read and answer the review questions on their own, and then discuss the answers as a group.

1. What functions does DNS provide in an Active Directory network?

Name resolution, a standard naming convention, and a location service.

2. What are the differences between the DNS namespace and the Active Directory namespace?

The DNS namespace consists of resource records, which are stored in zones. The Active Directory namespace consists of objects that are stored in domains.

3. What are SRV resource records used for in an Active Directory domain?

SRV resource records are used to locate servers that are offering a service that the client needs, for example, if the client is issuing a query against a global catalog server, an SRV resource record will contain the information the client needs to locate a server that is functioning as a global catalog server.

4. What are the main benefits provided by Active Directory integrated zones?

Fault tolerance, security, and more efficient replication of large zones.

5. What are the requirements that a DNS implementation needs to meet to support Active Directory?

Any DNS implementation must support the SRV resource record format. In addition, it is strongly recommended that it also support the dynamic update protocol and incremental zone transfers.