5 Configuring a DNS Infrastructure

Exam Objectives in this Chapter:

- Configure a DNS server.
- Configure DNS zone options.
- Configure DNS forwarding.
- Manage DNS zone settings.
- Manage DNS server options.

Why This Chapter Matters

The Domain Name System (DNS) is too vital an element in a network infrastructure to be merely deployed and forgotten on a single server. For medium-sized and large organizations, DNS must be distributed throughout the network and kept up to date. Network administrators are tasked with the responsibility of maintaining this infrastructure, a job which requires understanding the nuances of features such as zone transfers, delegations, stub zones, round robin, and netmask ordering. Because of its importance, this chapter is one of the most heavily tested sections on the 70-291 exam.

This chapter introduces you to the main configuration options available for DNS servers and zones, many of which are available in the server properties and zone properties dialog boxes. In addition, this chapter teaches you how and why to implement delegations and stub zones in your Windows Server 2003 networks.

Lessons in this Chapter:

Before You Begin

To complete this chapter, you must have

- Networked two computers, named Computer1 and Computer2, each running Windows Server 2003. Computer1 should be assigned a static address of 192.168.0.1/24, and Computer2 should be configured to obtain an address automatically. Computer2 should have an alternate configuration address of 192.168.0.2/24. Both Computer1 and Computer2 should have a configured primary DNS suffix of domain1.local.
- A phone line and dial-up Internet service provider (ISP) account. (If you choose to substitute a dedicated Internet connection for this requirement, you should rename this Internet connection "MyISP." You might also need to make other minor adjustments to the lesson exercises.)
- Installed the Network Monitor Tools subcomponent of the Management And Monitoring Tools Windows component on Computer1. A Network Monitor capture file named Name Resolution 1 should be saved to the My Captures folder in My Documents on Computer1. This capture, created before DNS is deployed on the network, shows the traffic exchanged on the network after the Ping computer2 command is executed on Computer1.
- Installed the Domain Name System (DNS) subcomponent of the Networking Services. Once installed, the DNS server should host a primary forward lookup zone named domain1.local and a primary reverse lookup zone corresponding to the 192.168.0.0/24 address space. Both zones are configured to accept secure and nonsecure updates. A host (A) resource record for both Computer1 and Computer2 should exist in the domain1.local zone.
- Installed Windows Support Tools on Computer1.
- Created a dial-up connection to the Internet named MyISP on Computer1 that you have shared through Internet Connection Sharing (ICS). Computer2 should receive a fresh Internet Protocol (IP) configuration from Computer1 after ICS is enabled. (If you are using a dedicated Internet connection instead of a dial-up account, you should apply this requirement to the dedicated connection.)
- Selected the Use This Connection's DNS Suffix In DNS Registration option on the DNS tab in the Advanced TCP/IP Settings dialog box for the Local Area Connection on Computer2.

Lesson 1: Configuring DNS Server Properties

After you have installed a DNS server, you might need to modify its default settings to suit your network needs. In this lesson, you learn the various settings that you can configure through the server properties dialog box in the DNS console. The settings you configure in this properties dialog box do not apply to a particular zone but to the server in general.

After this lesson, you will be able to

- Configure a DNS server to listen for queries on selected network adapters
- Configure a DNS server to forward all or select DNS queries to an upstream DNS server
- Determine when it is necessary to modify root hints

Estimated lesson time: 45 minutes

Exploring DNS Server Properties Tabs

The DNS server properties dialog box allows you to configure settings that apply to the DNS server and all its hosted zones. You can access this dialog box in the DNS console tree by right-clicking the DNS server you want to configure and then selecting Properties, as shown in Figure 5-1.

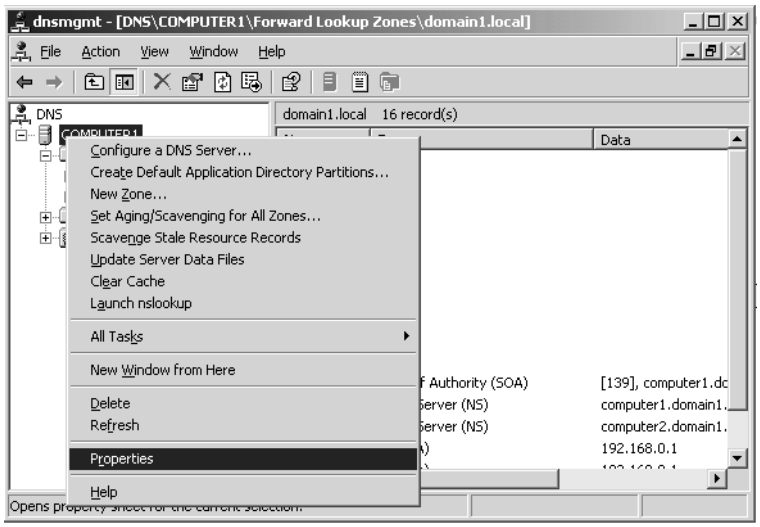


Figure 5-1 Accessing the DNS server properties dialog box

The DNS server properties dialog box contains eight tabs, which are introduced next.

Interfaces Tab

The Interfaces tab allows you to specify which of the local computer's IP addresses the DNS server should listen to for DNS requests. For example, if your server is multihomed and has one IP address for the local network and another IP address connected to the Internet, you can prevent the DNS server from servicing DNS queries from outside the local network. To perform this task, specify that the DNS server listen only on the computer's internal IP address, as shown in Figure 5-2.

By default, the setting on this tab specifies that the DNS server listens on all IP addresses associated with the local computer.

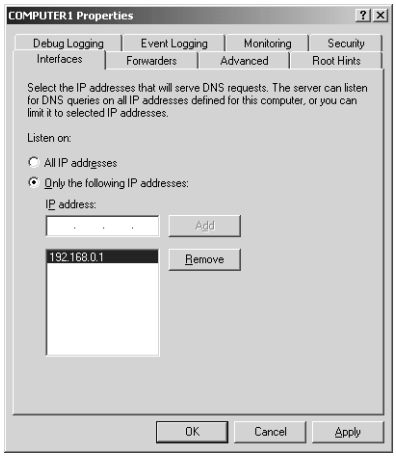


Figure 5-2 Interfaces tab

Exam Tip For simulation questions, be sure to review the procedure for configuring DNS listening by adding or removing interfaces from the DNS server. To spot such questions, look for requirements stating that a DNS server should listen or respond to queries only from certain networks (such as the private network).

Forwarders Tab

The Forwarders tab allows you to forward DNS queries received by the local DNS server to upstream DNS servers, called *forwarders*. Using this tab, you can specify the IP addresses of the upstream forwarders, and you can specify the domain names of queries that should be forwarded. For example, in Figure 5-3, all queries received for the domain lucernepublishing.com will be forwarded to the DNS server 207.46.132.23. When, after

receiving and forwarding a query from an internal client, the local forwarding server receives a query response back from 207.46.132.23, the local forwarding server then passes this query response back to the original querying client. The process of forwarding selected queries in this way is known as *conditional forwarding*.

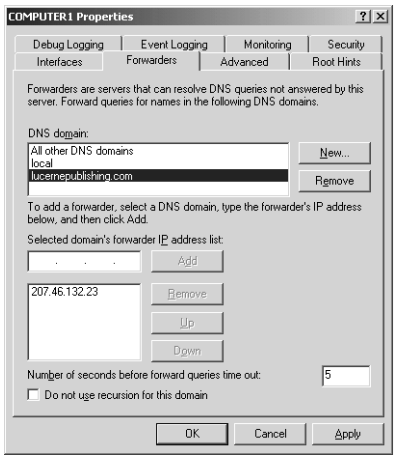


Figure 5-3 Forwarders tab

In all cases, a DNS server configured for forwarding uses forwarders only after it has determined that it cannot resolve a query using its authoritative data (primary or secondary zone data) or cached data.

Tip To specify how long the forwarding server should wait for a response from a forwarder before timing out, on the Forwarders tab, enter a value in the Number Of Seconds Before Forward Queries Time Out text box. The default setting is 5.

When to Use Forwarders In some cases, network administrators might not want DNS servers to communicate directly with external servers. For example, if your organization is connected to the Internet by means of a slow wide area link, you can optimize name resolution performance by channeling all DNS queries through one forwarder, as shown in Figure 5-4. Through this method, the server cache of the DNS forwarder has the maximum potential to grow and reduce the need for external queries.

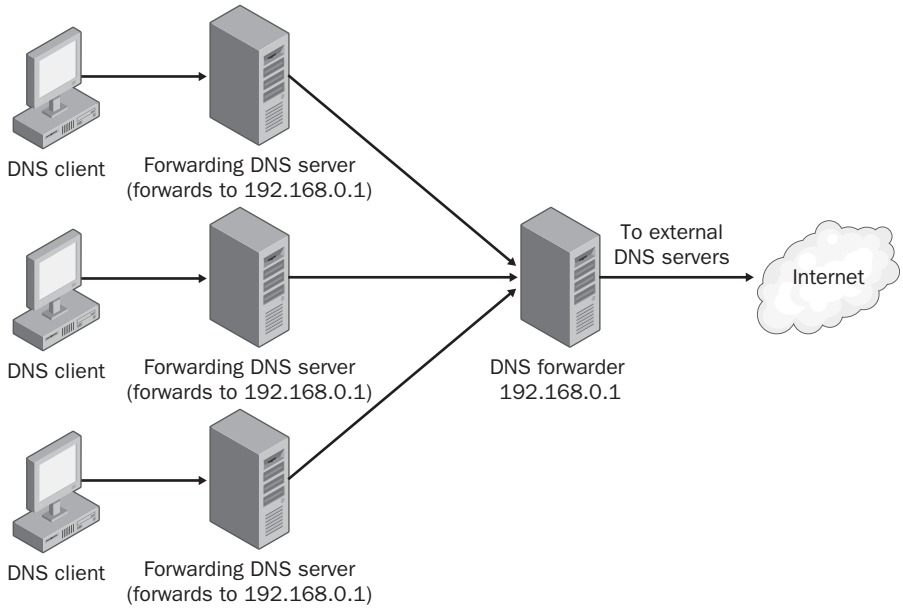


Figure 5-4 Using forwarding to consolidate caching

Another common use of forwarding is to allow DNS clients and servers inside a firewall to resolve external names securely. When an internal DNS server or client communicates with external DNS servers by making iterative queries, normally the ports used for DNS communication with all external servers must be left open to the outside world through the firewall. However, by configuring a DNS server inside a firewall to forward external queries to a single DNS forwarder outside your firewall, and by then opening ports only to this one forwarder, you can resolve names without exposing your network to outside servers. Figure 5-5 illustrates this arrangement.

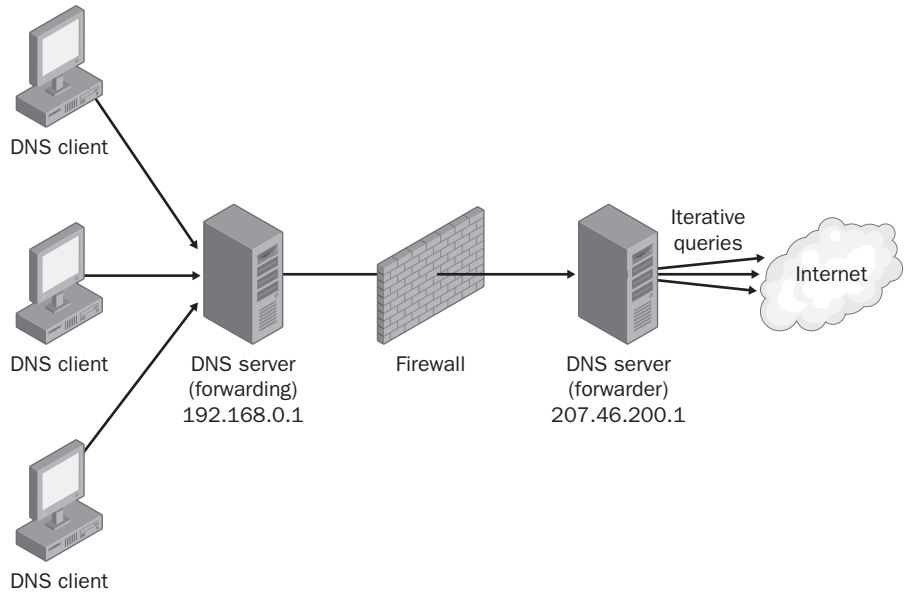


Figure 5-5 Secure iteration with forwarders

Exam Tip If your forwarders go down, you should remove them and force your DNS servers to perform recursion against the root servers. Alternatively, if you configure forwarders and remove the root hints, you are essentially forcing your DNS servers to use the forwarders for all unresolved queries.

When to Use Conditional Forwarding The term *conditional forwarding* describes a DNS server configuration in which queries for specific domains are forwarded to specific DNS servers.

One of the many scenarios in which conditional forwarding is useful is when two separate networks merge. For example, suppose the Contoso and Fabrikam companies have separate networks with Active Directory directory service domains. After the two companies merge, a 128-kilobits per second (Kbps) leased line is used to connect the private networks. For clients in each company to resolve queries for names in the opposite network, conditional forwarding is configured on the DNS servers in both domains. Queries to resolve names in the opposite domain will be forwarded to the DNS server in that domain. All Internet queries are forwarded to the next DNS server upstream beyond the firewall. This scenario is depicted in Figure 5-6.

Note that conditional forwarding is not the only way to provide name resolution in this type of merger scenario. Secondary zones and stub zones can also be configured for this reason and provide basically the same name resolution service. However, conditional

forwarding eliminates zone transfer traffic, provides zone data that is up to date, and allows for simple configuration and maintenance.

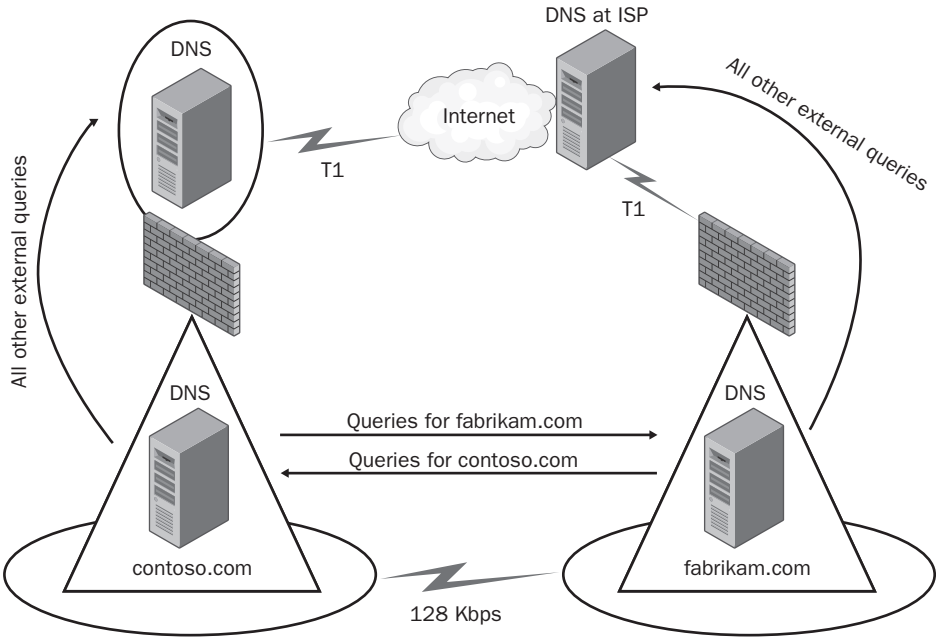


Figure 5-6 A conditional forwarding scenario

Exam Tip Conditional forwarding is a topic you should expect to encounter more than once on the 70-291 exam. Understand its purpose and the benefits it offers. For simulation questions, be sure to review how to configure conditional forwarding by using the Forwarders tab of the DNS server properties sheet. Finally, to spot these simulation questions, look for requirements stating that name resolution requests for a specific domain (such as contoso.com) *must be resolved by a server in that domain* or that *no zone transfer traffic should occur* over a wide area network (WAN) link.

Disabling Recursion The Forwarders tab allows you to disable recursion on any queries, specified by domain, that have been configured to be forwarded to an upstream server. When recursion is not disabled (the default), the local DNS server attempts to resolve a fully qualified domain name (FQDN) after a forwarder has failed to do so. This condition is preferable if you want to optimize settings for fault tolerance: If the upstream forwarder is down, name resolution can fall back to the local DNS server.

However, when under this default setting the forwarder receives the forwarded query and still fails to resolve it, the subsequent fallback recursion that occurs at the local DNS server is usually redundant and delays an inevitable query failure message

response. Disabling recursion on queries for which forwarding has been configured thus optimizes the speed of negative query responses at the expense of fault tolerance.

When forwarders are configured this way, in combination with disabling recursion, the local DNS server is known as a *slave server* because, in these cases, it is completely dependent on the forwarder for queries that it cannot resolve locally.

Note Do not confuse the use of the term *slave server* with the term *slave zone*, which is used in some implementations of DNS. In some non-Microsoft DNS servers, such as Berkeley Internet Name Domain (BIND), primary zones are called *master zones* and secondary zones are called *slave zones*.

Advanced Tab

The Advanced tab, shown in Figure 5-7, allows you to enable, disable, and configure certain DNS server options and features such as recursion, round robin, automatic scavenging, and netmask ordering. To learn more about the features configurable on this tab, see Lesson 3, "Configuring Advanced DNS Server Properties," in this chapter.

Note Whereas the Forwarders tab allows you to disable recursion on selected queries for domains used with forwarders, the Advanced tab allows you to disable recursion for all queries received by the local DNS server.

Note If you disable recursion on a DNS server using the Advanced tab, you cannot use forwarders on the same server, and the Forwarders tab becomes inactive.

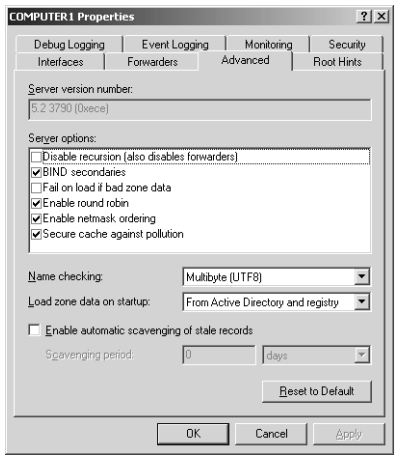


Figure 5-7 Advanced tab

Root Hints Tab

The Root Hints tab contains a copy of the information found in the WINDOWS \System32\Dns\Cache.dns file. For DNS servers answering queries for Internet names, this information does not need to be modified. However, when you are configuring a root DNS server (named ".") for a private network, you should delete the entire Cache.dns file. (When your DNS server is hosting a root server, the Root Hints tab is unavailable.)

In addition, if you are configuring a DNS server within a large private namespace, you can use this tab to delete the Internet root servers and specify the root servers in your network instead.

Exam Tip You need to understand root hints and root servers for the 70-291 exam, both for multiple choice and simulation questions. In addition to the information presented above, you also need to know that adding a zone named "." to a DNS server will turn that DNS server into a root server. And, when that happens, the DNS server will never forward queries or perform recursion for external names. In general, configuring a root server in this way prevents clients from accessing the Internet. However, users can still browse the Web if a Web proxy server such as an Internet Security and Acceleration (ISA) Server is deployed on the network *and* browsers have been configured to point to the proxy.

Figure 5-8 shows the Root Hints tab.

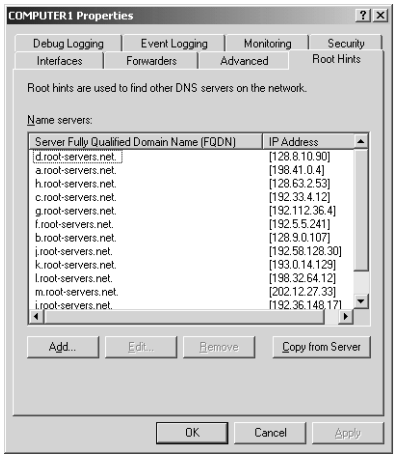


Figure 5-8 Root Hints tab

Note Every few years the list of root servers on the Internet is slightly modified. Because the Cache.dns file already contains so many possible root servers to contact, it is not necessary to modify the root hints file as soon as these changes occur. However, if you do learn of the availability of new root servers, you can choose to modify your root hints accordingly. As of this writing, the last update to the root servers list was made on January 29, 2004. You can download the latest version of the named cache file from InterNIC at *ftp://rs.internic.net/domain/named.cache*.

Debug Logging Tab

The Debug Logging tab allows you to troubleshoot the DNS server by logging the packets it sends and receives. Because logging all packets is resource-intensive, this tab allows you to restrict which packets to log, as specified by transport protocol, source IP address, packet direction, packet type, and packet contents. For more information on this feature, see Lesson 1 of Chapter 6, "Monitoring and Troubleshooting DNS."

Figure 5-9 shows the Debug Logging tab.

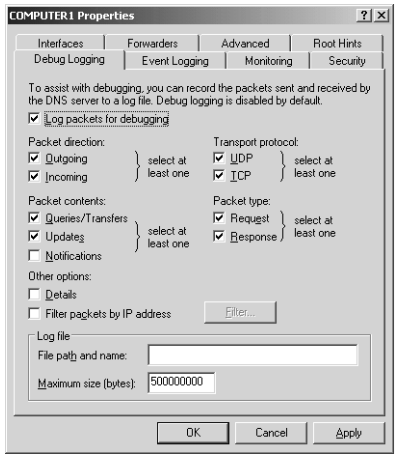


Figure 5-9 Debug Logging tab

Event Logging Tab

You can access the DNS Events log through the Event Viewer node in the DNS console.

The Event Logging tab, shown in Figure 5-10, allows you to restrict the events written to the DNS Events log file to only errors or to only errors and warnings. It also allows you to disable DNS logging. For more powerful features related to the filtering of DNS events, use the Filtering tab of the DNS Events Properties dialog box. You can open this dialog box by selecting Event Viewer in the left pane of the DNS console, right-clicking DNS Events in the right pane, and selecting Properties.

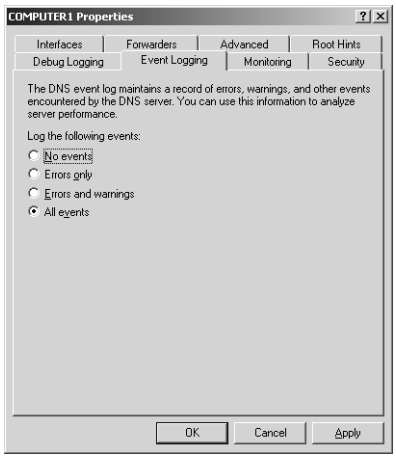


Figure 5-10 Event Logging tab

Monitoring Tab

The Monitoring tab allows you to test basic DNS functionality with two simple tests. The first test is a simple query against the local DNS server. To perform the first test successfully, the server must be able to answer forward and reverse queries targeted at itself.

The second test is a recursive query to the root DNS servers. To perform this second test successfully, the DNS server computer must be able to connect to the root servers specified on the Root Hints tab.

The Monitoring tab, shown in Figure 5-11, also allows you to schedule these tests to be conducted at regular intervals. The results of the tests, whether performed manually or automatically, are shown in the Test Results area of the tab.

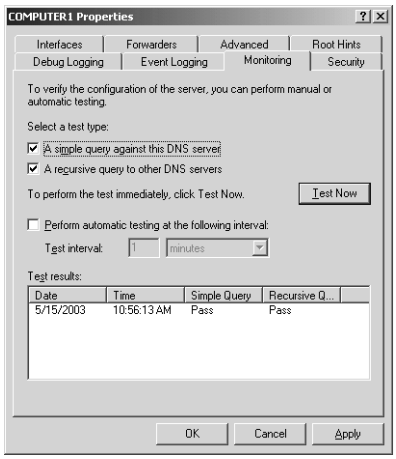


Figure 5-11 Monitoring tab

Security Tab

The Security tab is available only when the DNS server is also a domain controller. This tab allows you to control which users are granted permissions to view, configure, and modify the DNS server and its zones. By clicking the Advanced button, you can further refine settings related to DNS server permissions.

Figure 5-12 shows the Security tab.

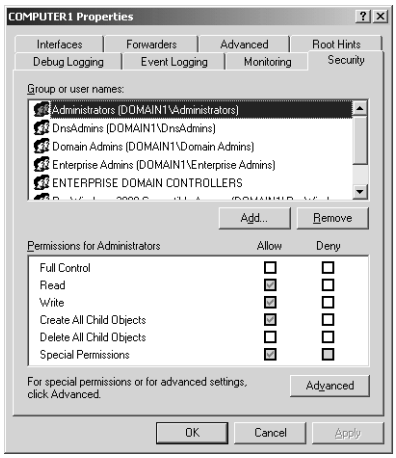


Figure 5-12 Security tab

Practice 1: Comparing NetBIOS and DNS Name Resolution Traffic

In this practice, you perform a capture of name resolution traffic and compare the result to a similar capture that was performed in Lesson 1 of Chapter 4, "Configuring DNS Servers and Clients."

Exercise 1: Capturing Name Resolution Traffic

In this exercise, you perform a Network Monitor capture of name resolution traffic from Computer2 and then compare this capture to one already saved on Computer1.

1. Log on to Computer2 as Administrator.
2. Install Network Monitor on Computer2, as explained in Lesson 1 of Chapter 3, "Monitoring and Troubleshooting TCP/IP Connections."
3. On Computer2, open Network Monitor.
4. If a message box appears requesting that you specify a network on which to capture data, click OK.

   The Select A Network window opens.

5. Select the adapter associated with your internal local area network (LAN), and then click OK.
6. Click the Start Capture button to begin a network trace.
7. Open a command prompt.

   The next two steps force Computer2 to contact Computer1 during the name resolution process.

8. At the prompt, type **nbtstat –R**, and then press ENTER. This step clears the cache of any NetBIOS name mappings.
9. At the prompt, type **ipconfig /flushdns**, and then press ENTER. This step clears the cache of host (DNS) name mappings.
10. At the command prompt, type **ping computer1**, and then press ENTER.

    The ping is successful. Notice how in this output, domain1.local has been appended to "computer1" in the original query.

11. After the Ping output has completed, switch back to Network Monitor, and click Stop And View Capture. The Frame Viewer window opens in Network Monitor, displaying the frames just captured.
12. From the File menu, select Save As to open the Save As dialog box.
13. In the File Name text box, type **Name Resolution 2**.
14. On Computer2, save the file to the My Captures folder.
15. Compare the traffic in the Name Resolution 2 file to the traffic in the Name Resolution 1 file saved in the My Captures folder on Computer1. Then answer the following questions in the spaces provided.

    What is the essential difference between the two captures?

    _____

    _____

    What accounts for the difference in name resolution methods?

    _____

    _____

16. Close all open windows on Computer1 and Computer2. If prompted to save any open files, click No.
17. Log off Computer1 and Computer2.

Practice 2: Verifying SRV Resource Records for Active Directory in DNS

After you first install Active Directory, you must verify that the installation has created the proper service location (SRV) resource records in DNS. In this practice, you install an Active Directory domain by promoting Computer1 to the status of domain controller. You then examine the DNS console to verify that the SRV resource records required for the new domain1.local Active Directory domain have been created. Finally, you join Computer2 to the new domain.

Exercise 1: Installing Active Directory

In this exercise, you install Active Directory and promote Computer1 to the status of domain controller in a new domain.

1. Log on to Computer1 as Administrator.
2. Verify that Computer1 is disconnected from the Internet.
3. Click Start and then select Manage Your Server.

   The Manage Your Server page appears.
4. On the Manage Your Server page, click the Add Or Remove A Role option.

   The Preliminary Steps page of the Configure Your Server Wizard appears.
5. Read the text on the page, and then click Next.

   The Server Role page appears.
6. In the Server Role list, select Domain Controller (Active Directory), and then click Next.

   The Summary Of Selections page appears.
7. Read the text on the page, and then click Next.

   The Welcome page of the Active Directory Installation Wizard appears.
8. Click Next.

   The Operating System Compatibility page appears.
9. Read all of the text on this page, and then answer the following question in the space provided.

   What is the restriction that applies to clients running Microsoft Windows 95 and Microsoft Windows NT 4 SP3 or earlier?

   _____

   _____
10. Click Next.

    The Domain Controller Type page appears.

11. Click Next to accept the default selection, Domain Controller For A New Domain.

    The Create New Domain page appears.

12. Click Next to accept the default selection, Domain In A New Forest.

    The New Domain Name page appears.

13. In the Full DNS Name For New Domain text box, type **domain1.local**, and click Next.

    The NetBIOS Domain Name page appears.

14. Click Next to accept the default selection of DOMAIN1 in the Domain NetBIOS Name text box.

    The Database And Log Folders page appears.

15. Click Next to accept the default selections in the Database Folder text box and the Log Folder text box.

    The Shared System Volume page appears.

16. Click Next to accept the default selection in the Folder Location text box.

    The DNS Registration Diagnostics page appears.

17. Read the diagnostic results and then click Next.

    The Permissions page appears.

18. Click Next to accept the default selection, Permissions Compatible Only With Windows 2000 Or Windows Server 2003 Operating Systems.

    The Directory Services Restore Mode Administrator Password page appears.

19. In the Restore Mode Password text box and the Confirm Password text box, type a strong password.

    This setting specifies that the password you have just entered must be used whenever you log on as Administrator in Directory Services Restore mode.

20. Click Next.

    The Summary page appears.

21. Read the text on the page, and then click Next.

    The Active Directory Installation Wizard window appears while Active Directory is being installed. When installation is complete, the Completing The Active Directory Installation Wizard page appears.

22. Click Finish.

    The Active Directory Installation Wizard dialog box appears, indicating that Windows must be restarted before the changes will take effect.

23. Click Restart Now.

Exercise 2: Verifying SRV Resource Records in DNS

In this exercise, you verify that new SRV resource records have been added to the domain1.local zone.

1. From Computer1, log on to Domain1 as Administrator. Use the same password that you originally assigned to the Computer1 Administrator account.
2. If you see the final page in the Configure Your Server Wizard, indicating that the server is now a domain controller, click Finish.
3. Open the DNS console. Expand the COMPUTER1, Forward Lookup Zones, and the Domain1.local nodes.

   Six subdomains are now listed under Domain1.local. They have been created by the installation of Active Directory.
4. In the DNS console tree, browse to locate an SRV resource record named _ldap._tcp.dc._msdcs.domain1.local. To perform this task, read each label in the name of the resource record from right to left, starting with the Domain1.local node. For example, after you have opened the _msdcs.domain1.local node, open the dc node, and finally select the _tcp node. You see the _ldap Service Location (SRV) resource record in the details pane when the _tcp node is selected, as shown in Figure 5-13.

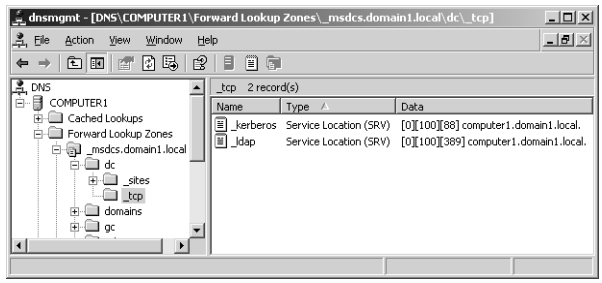


Figure 5-13 SRV resource records for a domain controller

   This resource record is used to locate domain controllers for the domain1.local domain. It is the most important record to check after you have installed Active Directory.
5. In the DNS console tree, browse to locate an SRV resource record named _ldap._tcp.gc._msdcs.domain1.local.

   This resource record is used to locate Active Directory global catalogs for the domain1.local domain. The records have been created successfully.
6. Log off Computer1.

Exercise 3: Joining a Computer to the New Domain

In this exercise, you join Computer2 to the new domain.

1. Log on to Computer2 as Administrator.
2. In Control Panel, double-click System.

   The System Properties dialog box opens.
3. On the Computer Name tab, click the Change button.

   The Computer Name Changes dialog box opens.
4. In the Member Of area, select Domain.
5. In the Domain text box, type **domain1.local,** and then click OK.

   The Computer Name Changes dialog box opens, prompting you for an account name and password with the permissions to add Computer2 to Domain1.
6. In the User Name text box, type **administrator**.
7. In the Password text box, type the password that you originally assigned to the Administrator account for Computer1. (This password is now the password for the Administrator account in Domain1.)
8. Click OK.

   The Computer Name Changes message box appears, welcoming you to the domain1.local domain.
9. Click OK.

   A message box indicates that you need to restart the computer for the changes to take effect.
10. Click OK, and then click OK again in the System Properties dialog box.

    The System Settings Change message box appears, asking whether you want to restart the computer now.
11. Click Yes to restart the computer.

    Computer2 restarts.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. How can you use forwarding to increase security of DNS queries?

   _____

   _____

2. Using the DNS server properties dialog box, how can you prevent a multihomed DNS server from answering DNS queries received through specific network cards?

3. You administer a network that consists of a single domain. On this network, you have configured a new DNS server named DNS1 to answer queries for Internet names from the local domain. However, although DNS1 is connected to the Internet, it continues to fail its recursive test on the Monitoring tab of the server properties dialog box. Which of the following could be the potential cause for the failure?
   a. You have configured DNS1 in front of a firewall.
   b. DNS1 hosts a zone named ".".
   c. Your root hints have not been modified from the defaults.
   d. You have not configured DNS1 to forward any queries to upstream servers.
4. Which of the following events could serve as a legitimate reason to modify (but not delete) the default root hints on the Root Hints tab of a DNS server properties dialog box? (Choose all that apply.)
   a. The Internet root servers have changed.
   b. The server will not be used as a root server.
   c. You have disabled recursion on the server.
   d. Your server is not used to resolve Internet names.

Lesson Summary

- The Interfaces tab of the DNS server properties dialog box allows you to specify which of the local computer's IP addresses the DNS server should listen to for DNS requests.
- The Forwarders tab of the DNS server properties dialog box allows you to forward DNS queries received by the local DNS server to upstream DNS servers, called forwarders. This tab also allows you to disable recursion for select queries (as specified by domain).
- By configuring a DNS server inside a firewall to forward external queries to a single DNS forwarder outside your firewall, and by then opening ports through the firewall only to this one forwarder, you can resolve DNS names without exposing your network to outside servers.
- The Root Hints tab provides a simple way to modify the contents in the Cache.dns file. If you are using your DNS server to resolve Internet names, you

do not normally need to modify these entries. However, if you are using your DNS server only to answer queries for hosts in a separate and private DNS namespace, you should alter these root hints to point to the root servers in your network. Finally, if your DNS server computer is itself the root server (named ".") of your private namespace, you should delete the Cache.dns file.

- The Monitoring tab of the DNS server properties dialog box allows you to check basic DNS functionality with two simple tests: a simple query against the local DNS server, and a recursive query to the root DNS servers.

Lesson 2: Configuring Zone Properties and Transfers

You can perform many essential tasks related to administering and managing a DNS infrastructure through the properties dialog boxes of your network's hosted zones. These tasks include configuring and managing zone transfers, enabling dynamic updates, and modifying zone types.

After this lesson, you will be able to

- Configure a DNS zone for dynamic updates
- Change the DNS zone type
- Store zone data in the Active Directory database
- Add name server (NS) resource records to a zone
- Configure zone transfers from secondary zones
- Describe the events that can trigger a zone transfer
- Describe the process of a zone transfer

Estimated lesson time: 70 minutes

Exploring DNS Zone Properties

The primary means to configure zone settings is through the zone properties dialog box, which is accessible through the DNS console. Each properties dialog box for a standard zone has five tabs: General, Start Of Authority (SOA), Name Servers, Windows Internet Name Service (WINS), and Zone Transfers. Properties dialog boxes for Active Directory–integrated zones include a sixth tab, Security, that allows you to configure access permissions for the zone.

To open a properties dialog box for a particular zone, right-click the node of the zone you want to configure in the DNS console, and then select Properties, as shown in Figure 5-14.

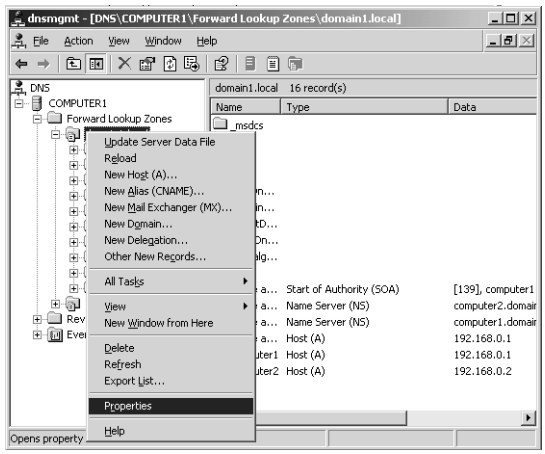


Figure 5-14 Opening the properties dialog box for a zone

General Tab

The General tab, shown in Figure 5-15, allows you to temporarily suspend name resolution and to configure four basic features: zone type (including Active Directory integration), zone file name, dynamic updates, and aging.

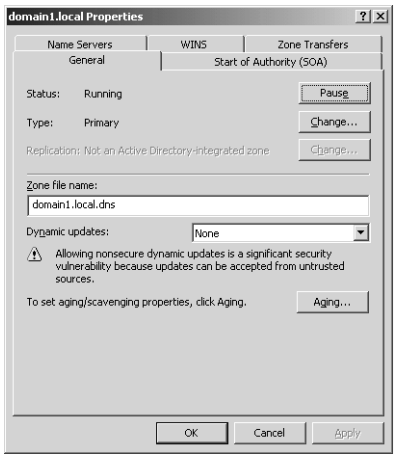


Figure 5-15 General tab

Zone Status The Pause button allows you to pause and resume name resolution for the zone. Note that this feature does not allow you to pause or resume the DNS Server service.

Zone Type Clicking Change opens the Change Zone Type dialog box, as shown in Figure 5-16.

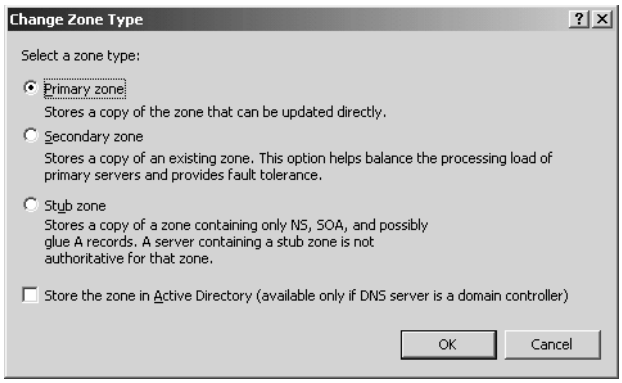


Figure 5-16 Change Zone Type dialog box

The Change Zone Type dialog box allows you to reconfigure the zone as a primary, secondary, or stub zone. A *primary zone* stores the most current records and settings

for the zone. For each standard zone that is not Active Directory–integrated, only one primary DNS server is allowed, and this server contains the only read/write version of the zone database. A *secondary zone* is a read-only copy of the primary zone used to improve performance and fault tolerance. A *stub zone* is a copy of a zone that contains only those resource records necessary to identify the actual authoritative DNS servers for that zone. (Stub zones are discussed in more detail in Lesson 5 of this chapter.)

By default, new zones are standard zones. This means that, by default, zone data is stored on the local DNS server only, in a text file. The alternative to a standard zone is an Active Directory–integrated zone.

Active Directory Integration Selecting the Store The Zone In Active Directory check box in the Change Zone Type dialog box allows you to store the primary zone information in the Active Directory database instead of in the WINDOWS\System32\Dns folder. In Active Directory–integrated zones, zone data is automatically replicated through Active Directory. In most cases, this eliminates the need to configure zone transfers to secondary servers.

Exam Tip There are several things you need to remember about Active Directory–integrated zones for the 70-291 exam. First, remember how to configure them. Second, remember that you can implement Active Directory–integrated zones only on DNS servers that are also domain controllers. Third, they allow DNS data to replicate automatically throughout Active Directory and thus usually eliminate the need for secondary servers. Fourth, they minimize zone transfer traffic because only updated records (as opposed to whole zones) are replicated throughout Active Directory. Finally, Active Directory–integrated zones enable the option for secure dynamic updates (described next).

Tip To migrate a standard primary server, configure a secondary server, transfer the zone to the secondary server, and then promote the secondary server to a primary server. After the secondary server has been promoted, you can delete the original primary server.

There are several advantages to integrating your DNS zone with Active Directory. First, because Active Directory performs zone replication, you do not need to configure a separate mechanism for DNS zone transfers. Fault tolerance, along with improved performance from the availability of multiple read/write primary servers, is automatically supplied by the presence of multimaster replication on your network. Second, Active Directory allows for single properties of resource records to be updated and replicated among DNS servers. Avoiding the transfer of many and complete resource records decreases the load on network resources during zone transfers. Finally, Active Directory integration allows you to configure access security for stored records, which prevents unauthorized updates.

Planning Because of the many benefits of Active Directory–integrated zones, you should plan to deploy your DNS servers on domain controllers whenever possible.

Zone Replication When you opt to store zone information in the Active Directory database, the associated Change button becomes enabled, as shown in Figure 5-17. This button allows you to configure replication parameters for the Active Directory–integrated zone.

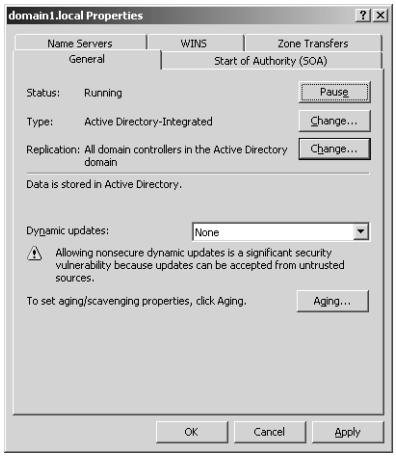


Figure 5-17 Change button for zone replication

Clicking the Change button opens the Change Zone Replication Scope dialog box, shown in Figure 5-18. This dialog box allows you to determine among which servers in the Active Directory forest the zone data should be replicated.

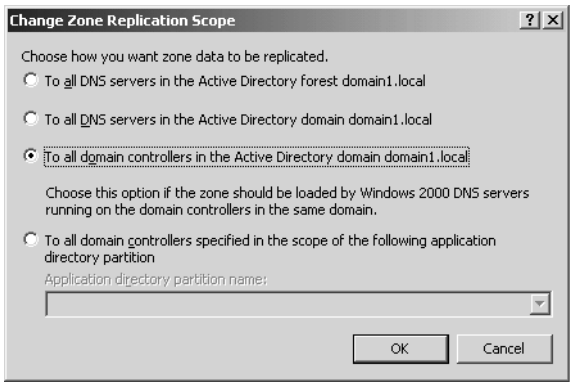


Figure 5-18 Setting the zone replication scope

Table 5-1 describes the four options available in this dialog box.

Table 5-1 Zone Replication Options

Options	Description
To All DNS Servers In The Active Directory Forest	Replicates zone data to all DNS servers running on domain controllers in the Active Directory forest. Usually, this option provides the broadest scope of replication.
To All DNS Servers In The Active Directory Domain	Replicates zone data to all DNS servers running on domain controllers in the Active Directory domain.
To All Domain Controllers In The Active Directory Domain	Replicates zone data to all domain controllers in the Active Directory domain. If you want Microsoft Windows 2000 DNS servers to load an Active Directory zone, you must select this setting for that zone.
To All Domain Controllers Specified In The Scope Of The Following Application Directory Partition	Replicates zone data according to the replication scope of the specified application directory partition. For a zone to be stored in the specified application directory partition, the DNS server hosting the zone must be enlisted in the specified application directory partition.

When deciding which replication option to choose, consider that the broader the replication scope, the greater the network traffic caused by replication. For example, if you choose to have Active Directory–integrated DNS zone data replicated to all DNS servers in the forest, this setting produces greater network traffic than does replicating the DNS zone data to all DNS servers in a single Active Directory domain in that forest. On the other hand, replicating zone data to all DNS servers in a forest can improve forestwide name resolution performance and increase fault tolerance.

Application Directory Partitions and DNS Replication An *application directory partition* is a directory partition that is replicated among a specified subset of domain controllers running Windows Server 2003.

- Built-in application directory partitions

  For DNS, two built-in application directory partitions exist for each Active Directory domain: DomainDnsZones and ForestDnsZones. The DomainDnsZones application directory partition is replicated among all DNS servers that are also domain controllers in an Active Directory domain. The ForestDnsZones application directory partition is replicated among all DNS servers that are also domain controllers in an Active Directory forest. Each of these application directory partitions is designated by a DNS subdomain and an FQDN. For example, in an Active Directory domain named bern.lucernepublishing.com whose root domain in the Active Directory forest is lucernepublishing.com, the built-in DNS application partition directories are specified by these FQDNs: DomainDnsZones.bern.lucernepublishing.com and ForestDnsZones.lucernepublishing.com.

When you select the To All DNS Servers In The Active Directory Forest option in the Change Zone Replication Scope dialog box, you are in fact choosing to store DNS zone data in the ForestDnsZones application directory partition. When you select the To All DNS Servers In The Active Directory Domain option, you are choosing to store DNS zone data in the DomainDnsZones application directory partition.

Note If either of these application directory partitions is deleted or damaged, you can re-create them in the DNS console by right-clicking the server node and selecting Create Default Application Directory Partitions.

- Creating custom application directory partitions

  You can also create your own custom application directory partitions for use with DNS and enlist chosen domain controllers in your network to host replicas of this partition.

  To accomplish this task, first create the partition by typing the following command:

  dnscmd [*servername*]/createdirectorypartition *FQDN*

  Then enlist other DNS servers in the partition by typing the following command:

  dnscmd *servername*/enlistdirectorypartition *FQDN*

  For example, to create an application directory partition named SpecialDns on a computer named Server1 in the Active Directory domain contoso.com, type the following command:

  dnscmd server1 /createdirectorypartition SpecialDns.contoso.com

  To enlist a computer named Server2 in the application directory partition, type the following command:

  dnscmd server2 /enlistdirectorypartition SpecialDns.contoso.com

Note You must be a member of the Enterprise Admins group to create an application directory partition.

  To store DNS data in a custom application directory partition, select the fourth (bottom) option in the Change Zone Replication Scope dialog box, and specify the custom application directory partition in the drop-down list box. This option—To All Domain Controllers Specified In The Scope Of The Following Application Directory Partition—is available only if custom application directory partitions are available for DNS on your network.

- Replication with Windows 2000 servers

  Because application directory partitions are not available on Windows 2000 domain controllers, you must select the third option in the Change Zone Replication Scope

dialog box if you want the zone data to be read by Windows 2000 DNS servers. With this option—To All Domain Controllers In the Active Directory Domain—data is not replicated merely among all DNS server domain controllers, but among all domain controllers regardless of whether they are also DNS servers.

Exam Tip Expect to be tested on application directory partition concepts as well as the options in the Change Zone Replication Scope dialog box. To prepare for simulation questions, also review the procedure of setting zone replication scope.

Zone File Name For standard zones not stored in Active Directory, the default zone filename is created by adding a .dns extension to the zone name. The Zone File Name text box on the General tab allows you to change the default name of this file.

Dynamic Updates The General tab also allows you to configure a zone with dynamic updates in resource records. As shown in Figure 5-19, three dynamic update settings are available for Active Directory–integrated DNS zones: None, Nonsecure And Secure, and Secure Only. For standard zones, only two settings are available: None and Nonsecure And Secure.

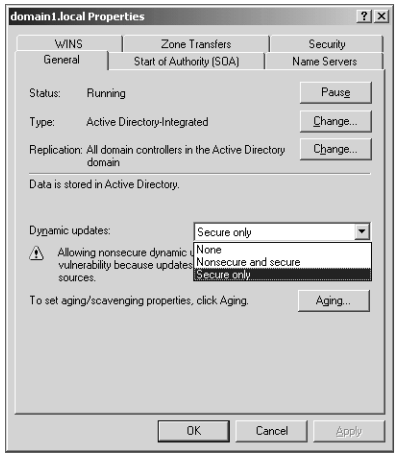


Figure 5-19 Zone settings for dynamic updates

When you select the None setting in the properties for a zone, you must manually perform registrations and updates to zone records. However, when you enable either the Nonsecure And Secure setting or the Secure Only setting, client computers can automatically create or update their own resource records. This functionality greatly reduces the need for manual administration of zone records, especially for DHCP clients and roaming clients.

Figure 5-20 shows a typical dynamic update process.

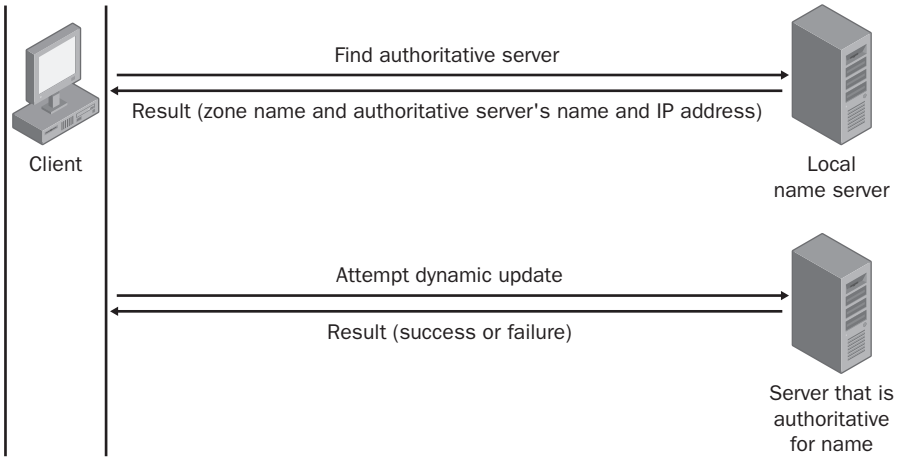
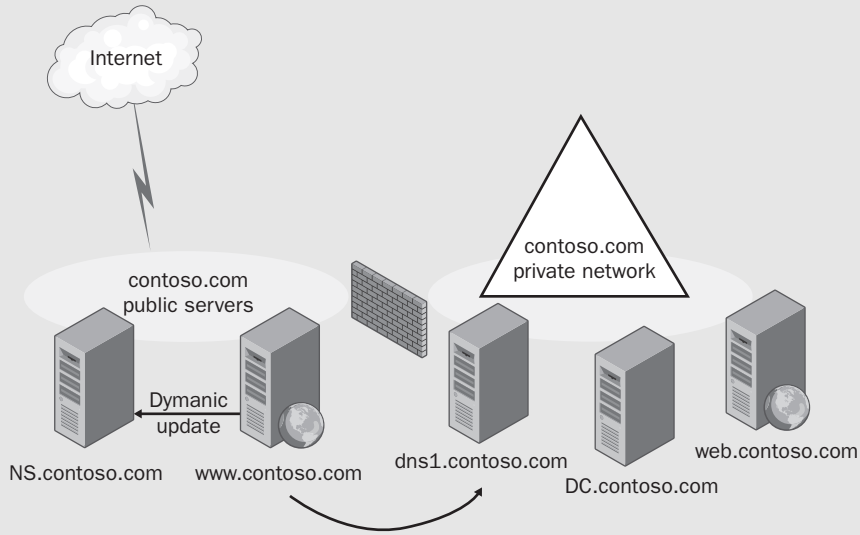


Figure 5-20 Dynamic update process

Whenever a triggering event occurs on a DNS client computer, the DHCP Client service, not the DNS Client service, attempts to perform a dynamic update of the A resource record with the DNS server. This update process is designed so that if a change to the IP address information occurs because of DHCP, this update is immediately sent to the DNS server. The DHCP Client service attempts to perform this dynamic update function for all network connections used on the system, including those not configured to use DHCP. Whether this attempt at a dynamic update is successful depends first and foremost on whether the zone has been configured to allow dynamic updates.

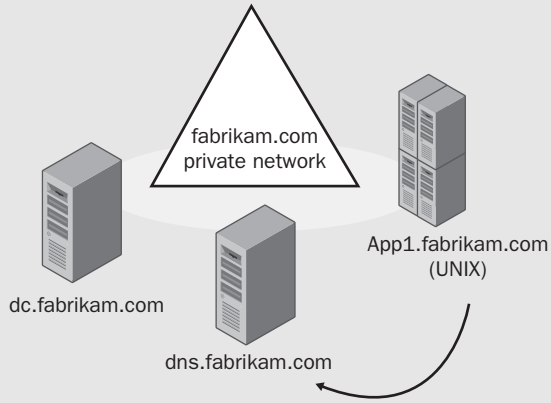
Real World **Manually Adding Host Records**

Even when dynamic updates are enabled for a particular zone, in some scenarios it might be necessary to add host records manually to that zone. For example, a company named Contoso, Inc. uses the domain name contoso.com for both its public namespace and its internal Active Directory domain. In this case, the public Web server named www.contoso.com is located outside the Active Directory domain and performs updates only on the public DNS server authoritative for contoso.com. Internal clients, however, point their DNS requests toward internal DNS servers. Because the A record for www.contoso.com is not updated dynamically on these internal DNS servers, the record must be added manually for internal clients to resolve the name and connect to the public Web server.



Manual creation of A record needed

Another case in which you might need to add host records manually is when you have a UNIX server on your network. For example, a company named Fabrikam, Inc. uses a single Active Directory domain named fabrikam.com for its private network. The network also includes a UNIX server named App1.fabrikam.com that runs an application critical to the company's daily operations. Since UNIX servers cannot perform dynamic updates, you need to add a host record for App1 on the DNS server hosting the fabrikam.com zone. Otherwise, users will not be able to connect to the application server when they specify it by FQDN.



Manual creation of A record needed

Dynamic Update Triggers The following events trigger the DHCP Client service to send a dynamic update to the DNS server:

- An IP address is added, removed, or modified in the Transmission Control Protocol/Internet Protocol (TCP/IP) properties configuration for any one of the local computer's installed network connections.
- An IP address lease changes or renews with the DHCP server for any one of the local computer's installed network connections—for example, when the computer is started or if the Ipconfig /renew command is used.
- The Ipconfig /registerdns command is used on a DNS client computer to manually force a refresh of the client name registration in DNS.
- The DNS client computer is turned on.
- A member server within the zone is promoted to a domain controller.

Secure Dynamic Updates Secure dynamic updates can be performed only in Active Directory–integrated zones. For standard zones, the Secure Only option does not appear in the Dynamic Updates drop-down list box. These updates use the secure Kerberos authentication protocol to create a secure context and ensure that the client updating the resource record is the owner of that record. Secure dynamic updates also ensure that the updating client computer has an account in the Active Directory domain corresponding to the DNS domain in the zone being updated. In addition, that computer account must successfully authenticate before it can update its record in the DNS domain.

Exam Tip To prepare for simulation questions, practice performing the procedure of requiring secure dynamic updates on a zone. For this task, look out for any requirement stating that only *authorized client computers* can perform DNS updates or that *one computer must not be able to overwrite another computer's record*.

Note Only clients running a version of Windows 2000, Microsoft Windows XP, or Windows Server 2003 can attempt to send dynamic updates to a DNS server. Dynamic updates are not available for any version of Windows NT, Windows 95, Microsoft Windows 98, or Microsoft Windows Millennium Edition (Me). However, a DHCP server can perform dynamic updates on behalf of other clients if the server is configured to do so.

Secure Dynamic Updates and the DnsUpdateProxy Group When secure dynamic updates are required in a zone, only the owner of a record can update that record. (The owner of a record is the computer that originally registers the record.) This restriction can cause problems in situations where a DHCP server is being used to register host (A) resource records on behalf of client computers that cannot perform dynamic

updates. In such cases, the DHCP server becomes the owner of the record, not the computers themselves. If the downlevel client computer is later upgraded to Windows 2000 or some other operating system that is capable of performing dynamic updates, the computer will not be recognized as the owner and will consequently be unable to update its own records. A similar problem might arise if a DHCP server fails that has registered records on behalf of downlevel clients: None of the clients will be able to have their records updated by a backup DHCP server.

To avoid such problems, add to the DnsUpdateProxy security group DHCP servers that register records on behalf of other computers. Members of this group are prevented from recording ownership on the resource records they update in DNS. This procedure consequently loosens security for these records until they can be registered by the real owner.

Exam Tip You should understand DnsUpdateProxy before you take the 70-291 exam.

Aging By clicking Aging on the General tab, you can open the Zone Aging/Scavenging Properties dialog box, shown in Figure 5-21. These properties provide a means of finding and clearing outdated records from the zone database.

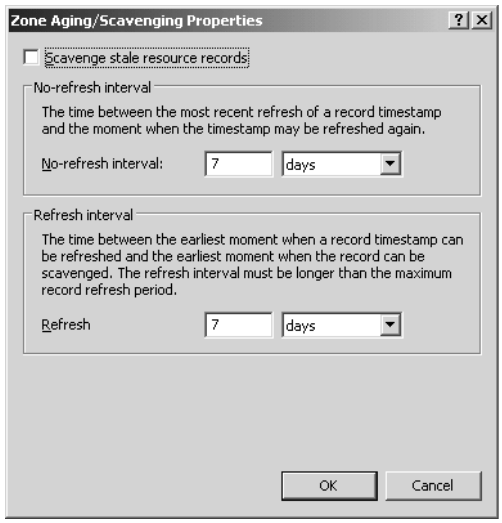


Figure 5-21 Zone Aging/Scavenging Properties dialog box

Enabling Aging Aging in DNS refers to the process of placing a timestamp on a dynamically registered resource record and then tracking the age of this record. Scavenging refers to the process of deleting outdated resource records on which timestamps have been placed. Scavenging can occur only when aging is enabled. Both aging and scavenging are disabled by default.

To enable aging for a particular zone, you have to enable this feature both at the zone level and at the server level. To enable aging at the zone level, in the Zone Aging/Scavenging Properties dialog box, select the Scavenge Stale Resource Records check box. To enable aging at the server level, first open the Server Aging/Scavenging Properties dialog box by right-clicking the server icon in the DNS console and then clicking Set Aging/Scavenging For All Zones. Then, in the Server Aging/Scavenging Properties dialog box, select the Scavenge Stale Resource Records check box.

After aging is enabled, a timestamp based on the current server time is placed on all dynamically registered records in the zone. When the DHCP Client service or DHCP server later performs a dynamic update of the records, a timestamp refresh is attempted. Manually created resource records are assigned a timestamp of 0; this value indicates that they will not be aged.

Note When you enable aging and scavenging for a zone, zone files cannot be read by pre–Windows 2000 DNS servers.

Modifying no-refresh intervals The no-refresh interval is the period after a timestamp during which a zone or server rejects a timestamp refresh. The no-refresh feature prevents unnecessary refreshes from being processed by the server and reduces unnecessary zone transfer traffic. The default no-refresh interval is seven days.

Modifying refresh intervals The *refresh interval* is the time after the no-refresh interval during which timestamp refreshes are accepted and resource records are not scavenged. After the no-refresh and refresh intervals expire, records can be scavenged from the zone. The default refresh interval is 7 days. Consequently, when aging is enabled, dynamically registered resource records can be scavenged after 14 days by default.

Tip If you modify the no-refresh or refresh interval, be sure to follow the guideline that the refresh interval should be equal to or greater than the no-refresh interval.

Exam Tip Prepare for simulation questions in which you have to configure aging and scavenging on a zone. For example, you might be given a requirement that hosts should refresh their records only every 12 days. In this case, you have to know that this requirement relates to the no-refresh interval. Likewise, you might be given a requirement that records not updated after 20 days should be removed from the zone database. In this case, you need to know that this requirement refers to the no-refresh interval plus the refresh interval. If the no-refresh interval is 12, the refresh interval would thus need to be set to 8 to meet this requirement. Last, don't forget to enable aging and scavenging at both the zone and server level.

Performing Scavenging Scavenging in a zone is performed either automatically or manually. For scavenging to be performed automatically, you must enable automatic scavenging of stale resource records on the Advanced tab of DNS server properties. When this feature is not enabled, you can perform manual scavenging in a zone by right-clicking the server icon in the DNS console tree and then selecting Scavenge Stale Resource Records from the shortcut menu.

Start Of Authority (SOA) Tab

The Start Of Authority (SOA) tab, shown in Figure 5-22, allows you to configure the SOA resource record for the zone. When a DNS server loads a zone, it uses the SOA resource record to determine basic, authoritative information about the zone. These settings also determine how often zone transfers are performed between primary and secondary servers.

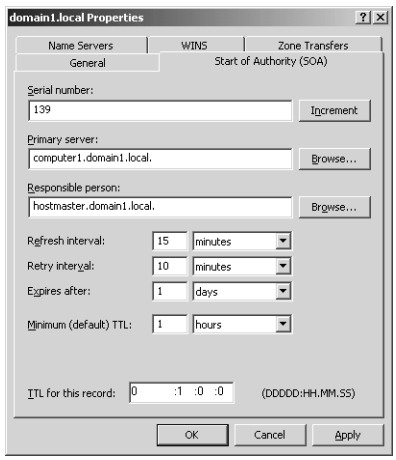


Figure 5-22 Start Of Authority (SOA) tab

Serial Number The Serial Number text box on the Start Of Authority (SOA) tab contains the revision number of the zone file. This number increases each time a resource record changes in the zone or when the value is manually incremented on this tab by clicking Increment.

When zones are configured to perform zone transfers, the master server is intermittently queried for the serial number of the zone. This query is called the *SOA query*. If, through the SOA query, the serial number of the master zone is determined to be equivalent to the local serial number, no transfer is made. However, if the serial number for the zone at the master server is greater than that at the requesting secondary server, the secondary server initiates a transfer.

Exam Tip When you click the Increment button, you force a zone transfer.

Primary Server The Primary Server text box on the Start Of Authority (SOA) tab contains the full computer name for the primary DNS server of the zone. This name must end with a period.

Responsible Person When this text box is configured, it contains a responsible person (RP) resource record of the person responsible for administering the zone. An RP resource record specifies a domain mailbox name for the responsible person. The name of the record entered into this field should always end with a period.

Refresh Interval The value you configure in the Refresh Interval field determines how long a secondary DNS server waits before querying the master server for a zone renewal. When the refresh interval expires, the secondary DNS server requests a copy of the current SOA resource record for the zone from its master server source, which then answers this SOA query. The secondary DNS server then compares the serial number of the source server's current SOA resource record (as indicated in the master's response) with the serial number of its own local SOA resource record. If they are different, the secondary DNS server requests a zone transfer from the primary DNS server. The default value for this setting is 15 minutes.

Tip Increasing the refresh interval decreases zone transfer traffic.

Retry Interval The value you configure in the Retry Interval box determines how long a secondary server waits before retrying a failed zone transfer. Normally, this time is less than the refresh interval. The default value is 10 minutes.

Expires After The value you configure in the Expires After box determines the length of time that a secondary server, without any contact with its master server, continues to answer queries from DNS clients. After this time elapses, the data is considered unreliable. The default value is 1 day.

Minimum (Default) TTL The value you configure in the Minimum (Default) TTL box determines the default Time to Live (TTL) that is applied to all resource records in the zone. The default value is 1 hour.

TTL values are not relevant for resource records within their authoritative zones. Instead, the TTL refers to the cache life of a resource record in nonauthoritative servers. A DNS server that has cached a resource record from a previous query discards the record when that record's TTL has expired.

TTL For This Record The value you configure in this text box determines the TTL of the present SOA resource record. This value overrides the default value setting in the preceding field.

Once configured in the DNS console, an SOA resource record is represented textually in the zone file, as shown in this example:

```
@ IN SOA computer1.domain1.local.hostmaster.domain1.local. (
  5099    ; serial number
  3600    ; refresh (1 hour)
  600    ; retry (10 mins)
  86400   ; expire (1 day)
  60  )  ; minimum TTL (1 min)
```

Exam Tip Make sure you understand all the settings and concepts related to the Start of Authority (SOA) tab.

Name Servers Tab

The Name Servers tab, shown in Figure 5-23, allows you to configure NS resource records for a zone. These records cannot be created elsewhere in the DNS console.

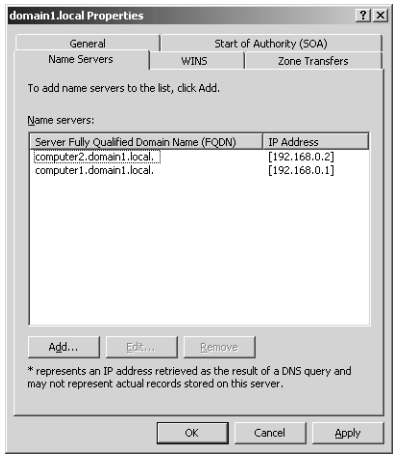


Figure 5-23 Name Servers tab

You use NS resource records to specify the authoritative name servers for a given zone. The NS resource record of the first primary server of a zone is configured automatically.

Note Every zone must contain at least one NS resource record at the zone root.

The following line is an example NS record taken from the database file for the lucernepublishing.com zone:

```
@ NS  dns1.lucernepublishing.com.
```

In this record, the "@" symbol represents the zone defined by the SOA record in the same zone file. The complete entry, then, effectively maps the lucernepublishing.com domain to a DNS server hosted on a computer named dns1.lucernepublishing.com.

Note In primary zones, zone transfers by default are allowed only to servers specified on the Name Servers tab. This restriction is new to Windows Server 2003.

WINS Tab

You use the WINS tab, shown in Figure 5-24—or the WINS-R tab in reverse lookup zones—to configure WINS servers to aid in name resolution for a given zone after DNS servers have failed to resolve a queried name.

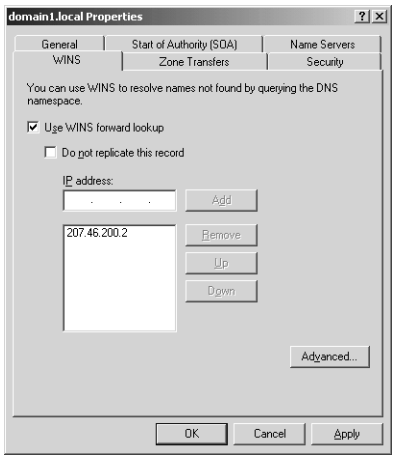


Figure 5-24 WINS tab

Exam Tip You need to know WINS lookup for the 70-291 exam. When you configure WINS lookup for a forward lookup zone, a WINS resource record pointing to the WINS server you specify on the WINS tab is added to the zone database. When you configure WINS-R lookup for a reverse lookup zone, a corresponding WINS-R resource record is added to the zone database. For redundancy, you can add two records to point to different WINS servers.

Zone Transfers Tab

The Zone Transfers tab, shown in Figure 5-25, allows you to restrict zone transfers from the local master server. For primary zones, zone transfers to secondary servers by default are either completely disabled or limited to name servers configured on the Name Servers tab. The former restriction applies when the DNS server has been added by using the Manage Your Server window; the latter, when it has been added by using the Windows Components Wizard. As an alternative to these default restrictions, you can customize zone transfer restrictions by selecting the Only To The Following Servers option and then specifying the IP addresses of allowed secondary servers in the list below this option.

Secondary zones, by default, do not allow zone transfers to other secondary zones, but you can enable this feature simply by selecting the Allow Zone Transfers check box.

Exam Tip For simulation questions, review the procedure of configuring zone transfers. Be sure to remember the differences among the three zone transfers options.

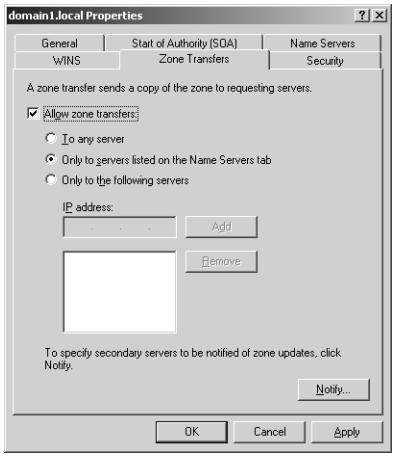


Figure 5-25 Zone Transfers tab

Off the Record In Windows 2000, the default setting on the Zone Transfers tab for primary zones was to allow transfers to any server, but this feature created an unnecessary security hole. Think about it: Why would you want to enable anyone who can access your DNS server to set up a secondary server and peruse your network's resource records? Restricting zone transfers by default is a lot smarter—it allows you to prevent unauthorized copying of zone data.

Notification The Zone Transfers tab also allows you to configure notification to secondary servers. To perform this task, click Notify on the Zone Transfers tab when zone transfers are enabled. This action opens the Notify dialog box, as shown in Figure 5-26, in which you can specify secondary servers that should be notified whenever a zone update occurs at the local master server. By default, when zone transfers are enabled, all servers listed on the Name Servers tab are automatically notified of zone changes.

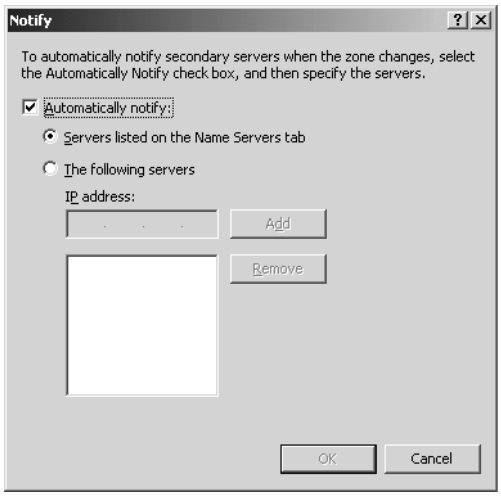


Figure 5-26 Notify dialog box

Exam Tip For simulation questions, review the procedure for enabling notification to other DNS servers in a zone. To spot these questions, look for a requirement stating that changes in a zone should immediately be updated to all secondary zones. Also, remember that you do not need to configure notification for Active Directory–integrated zones.

Notification and Zone Transfer Initiation Zone transfers in standard zones can be triggered by any of three events:

- They can be triggered when the refresh interval of the primary zone's SOA resource record expires.
- They can be triggered when a secondary server boots up.

  In these first two cases, the secondary server initiates an SOA query to find out whether any updates in the zone have occurred. Transfers occur only if the zone database has been revised.
- They are triggered when a change occurs in the configuration of the primary server and this server has specified particular secondary DNS servers to be notified of zone updates.

When a zone transfer initiates, the secondary server performs either an incremental zone transfer (IXFR) query or an all zone transfer (AXFR) query to the master server. Computers running Windows 2000 Server and Windows Server 2003 perform IXFR queries by default. Through IXFR queries, only the newly modified data is transferred across the network. Computers running Windows NT Server do not support IXFR queries and can perform only AXFR queries. Through AXFR queries, the entire zone database is transferred to the secondary server.

Primary DNS servers running Windows Server 2003 support both IXFR and AXFR zone transfers.

Figure 5-27 illustrates the transfer query process between secondary and master servers.

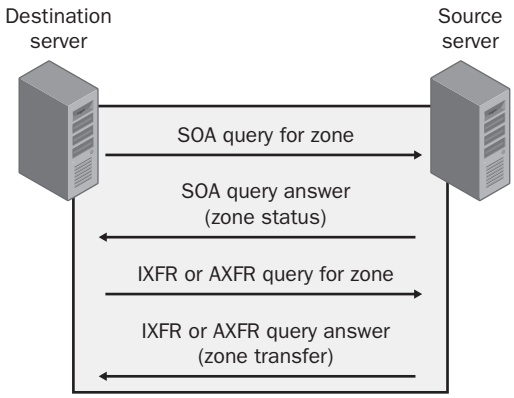


Figure 5-27 Zone transfer negotiations

Important You do not need to configure zone transfers or notification among domain controllers or DNS servers in Active Directory–integrated zones. For the servers within these zones, transfers are conducted automatically.

Practice: Deploying a Secondary DNS Server

In this practice, you create a secondary zone and then configure zone transfers between the two zones.

Exam Tip You should feel comfortable with the topic of secondary zones before you take the 70-291 exam, and you should prepare for a simulation in which you are asked to configure one. To spot questions on secondary zones, look for requirements stating that *name resolution should occur locally* or that *name resolution traffic should be minimized* across the WAN link. Also look for a requirement that *a full copy of the zone should be stored on the DNS server*.

Exercise 1: Configuring a Secondary Zone

In this exercise, you install a DNS server on Computer2 and then configure the new DNS server to host a secondary zone.

Important The following exercise assumes that you have installed the DNS server on Computer1 by using the Windows Components Wizard (as described in Chapter 4, Lesson 3). In this case, zone transfers from the Domain1.local zone are enabled by default but restricted to authoritative name servers. If, instead, you have installed the DNS server on Computer1 by using the Manage Your Server window to add the DNS server role, zone transfers for all locally hosted zones are disabled by default. In this case, before beginning this exercise, be sure to enable zone transfers for the Domain1.local zone and restrict zone transfers to servers listed on the Name Servers tab.

1. From Computer2, log on to Domain1 as Administrator. Remember to specify the password you originally assigned to the Administrator account on Computer1.
2. On Computer2, install the Windows Support Tools, as explained in Lesson 2 of Chapter 3.

   Windows Support Tools includes the Dnscmd command-line utility.
3. On Computer2, install the Domain Name System (DNS) Windows subcomponent of the Networking Services Windows component, as explained in Lesson 3 of Chapter 4. For the purposes of this exercise, you can safely dismiss any messages or errors you receive about Computer2 having a dynamically assigned IP address. Do not change the address configuration on Computer2.
4. Once the installation of the Domain Name System (DNS) subcomponent is complete, open a command prompt.
5. At the command prompt, enter the following command: **dnscmd computer1 /recordadd domain1.local @ ns computer2.domain1.local**.

   This command adds an NS record in domain1.local for Computer2, which makes Computer2 an authoritative server in the zone. By default, when a DNS server has been installed by using the Windows Components Wizard, zone transfers are allowed only to authoritative servers.
6. On Computer2, open the DNS console.
7. In the DNS console tree, right-click Forward Lookup Zones and select New Zone.
8. In the New Zone Wizard, click Next.
9. On the Zone Type page, select the Secondary Zone option, and then click Next.
10. On the Zone Name page, in the Zone Name text box, type **domain1.local** and then click Next.
11. In the Master DNS Server page, in the IP Address text box, type **192.168.0.1**, click Add, and then click Next.
12. On the Completing The New Zone Wizard page, click Finish.

13. In the DNS console tree, expand Forward Lookup Zones and select the Domain1.local node.
14. Right-click the Domain1.local node, and then select Transfer From Master.
15. If the zone fails to load, wait 1 minute and then try again. Repeat this step until the zone loads successfully.
16. When a copy of the domain1.local zone appears in the DNS console on Computer2, take a few moments to browse the zone properties dialog box and the items on the zone's Action (shortcut) menu.
17. Right-click the DNS node in the DNS console, and then click Connect To DNS Server.

    The Connect To DNS Server dialog box opens.
18. Select the option The Following Computer, and then type **COMPUTER1** in the associated text box.
19. Click OK. The COMPUTER1 node now appears above the COMPUTER2 node in the DNS console. Use both server nodes in the DNS console on Computer2 to answer the following questions in the spaces provided.

    Which functions on the Action menu are available for the domain1.local zone through the COMPUTER2 node that are not available on the Action menu for the same zone through the COMPUTER1 node?

    _____

    _____

    Can you create or configure resource records for domain1.local through the COMPUTER2 node in the DNS console?

    _____

    _____

Exercise 2: Reviewing Notification Settings

In this exercise, you review the default configuration for zone transfer notification.

1. From Computer2, while you are logged on to Domain1 as Administrator, expand the COMPUTER1 icon in the DNS console, and then open the Domain1.local Properties dialog box associated with this primary zone.
2. Click the Name Servers tab.

   Computer2 has been added as a result of adding an NS command in Exercise 1 of this chapter.
3. On the Zone Transfers tab, click Notify. The Notify dialog box opens.

   By default, the primary zone automatically notifies the servers listed on the Name Servers tab of zone changes.

Because Computer2 is now configured on the Name Servers tab, the secondary server is notified of any zone changes. When Computer2 receives notification from the primary server, this secondary DNS server normally initiates an IXFR query for an incremental zone transfer.

4. Click Cancel.
5. In the Domain1.local Properties dialog box, click the Start Of Authority (SOA) tab. Using the settings configured on this tab, answer the following questions in the spaces provided.

   According to the settings on the Start Of Authority (SOA) tab, if Computer2 loses contact with Computer1, how long will the DNS server on Computer2 continue to answer queries from DNS clients?

   _____

   _____

   How often is Computer2 configured to query Computer1 to find out whether any changes have been made to the zone?

   _____

   _____

   If Computer2 discovers it cannot contact Computer1 when it initiates an SOA query, how long does it wait before trying again?

   _____

   _____

   If another primary DNS server named dns.domain2.local successfully queries Computer1 for the IP address of Computer2, how long does Computer2's A resource record stay alive in the cache of dns.domain2.local?

   _____

   _____

6. Click OK to close the Domain1.local Properties dialog box.
7. In the DNS Console, right-click the Computer1 icon, and then click Delete.

   A DNS message box appears asking you to confirm the deletion.

8. In the DNS message box, click Yes.

   Computer1 is removed from the DNS console on Computer2, but the server settings remain intact in the DNS console on Computer1.

9. Log off Computer2.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. Describe the process by which secondary servers determine whether a zone transfer should be initiated.

2. What is the difference between IXFR and AXFR queries?

3. You have multiple DHCP servers on your network, some of which are configured to register DNS records on behalf of pre–Windows 2000 clients. You have configured DNS to allow only secure updates. However, you find that some DNS records are not being updated properly. How can you solve this problem?

4. You oversee administration for a WAN belonging to the Proseware company, which has one central office in Rochester and two branch offices in Buffalo and Syracuse. The network, which consists of one domain, has one primary DNS zone running on a Windows Server 2003 computer at the central office, and one secondary DNS zone at each branch. Network users are complaining that they often cannot connect to sites at remote branches. Administrators have determined that network bandwidth between the central office and branches has become saturated with zone transfers, and that zone transfers are being initiated before they can complete. Which of the following steps would help resolve the problem with the least effort?

   a. Install Active Directory on the network, and promote the servers hosting the secondary DNS zones to domain controllers.

   b. Increase the network bandwidth by establishing a fiber-optic connection between the two sites.

   c. Increase the refresh interval on the primary DNS server.

   d. Increase the refresh interval on the secondary DNS servers.

5. You discover that an administrator has adjusted the default TTL value for your company's primary DNS zone to 5 minutes. Which of the following is the most likely effect of this change?

a. Resource records cached on the primary DNS server expire after 5 minutes.

b. DNS clients have to query the server more frequently to resolve names for which the server is authoritative.

c. Secondary servers initiate a zone transfer every 5 minutes.

d. DNS hosts reregister their records more frequently.

6. Which of the following is not a benefit of storing DNS zones in the Active Directory database?

a. Less frequent transfers

b. Decreased need for administration

c. Less saturation of network bandwidth

d. Secure dynamic updates

Lesson Summary

- When you deploy a DNS server on a domain controller, you can choose to store the zone data in the Active Directory database. Active Directory–integrated zones minimize zone transfer traffic, improve security, decrease administrative overhead, and improve fault tolerance. Zone data can be configured to be replicated among all DNS servers in the Active Directory forest, all DNS servers in the Active Directory domain, all domain controllers in the Active Directory domain, or all servers enlisted in a custom application directory partition.
- When a DNS zone allows dynamic updates, certain DNS client computers can register and update their resource records with a DNS server. When secure dynamic updates are required in the zone, only the owner of the record can update the record. Secure dynamic updates can be required only on Active Directory–integrated zones. Client computers running Windows 2000, Windows XP, and Windows Server 2003 can perform dynamic updates.
- The DnsUpdateProxy group is typically used for DHCP servers performing dynamic DNS updates on behalf of other computers. Members of this group do not record ownership on the resource records they register in DNS. This behavior restriction prevents problems from arising in zones that allow only secure dynamic updates.
- The Start Of Authority (SOA) tab allows you to configure the zone's SOA resource record and several parameters that affect zone transfers, such as Refresh Interval, Retry Interval, Expires After, and Minimum (Default) TTL.
- The Zone Transfers tab allows you to control transfers from the current zone. By default, zone transfers are either completely disabled or limited to servers specified on the Name Servers tab. The nature of this restriction depends on the zone type and the manner in which the DNS server has been installed.

Lesson 3: Configuring Advanced DNS Server Properties

Advanced DNS server properties refer to the nine settings that can be configured on the Advanced tab of the DNS server properties dialog box. These properties relate to server-specific features such recursion, round robin, and netmask ordering.

After this lesson, you will be able to

- Describe the function and purpose of all of the options available for configuration on the Advanced tab of the DNS server properties dialog box
- Reset all advanced server settings to defaults

Estimated lesson time: 50 minutes

Tuning Advanced Server Options

When initialized for service, DNS servers running on Windows Server 2003 apply installation settings taken either from the boot information file, the Registry, or the Active Directory database. You can modify these settings on the Advanced tab of the server properties dialog box in the DNS console, as shown in Figure 5-28.

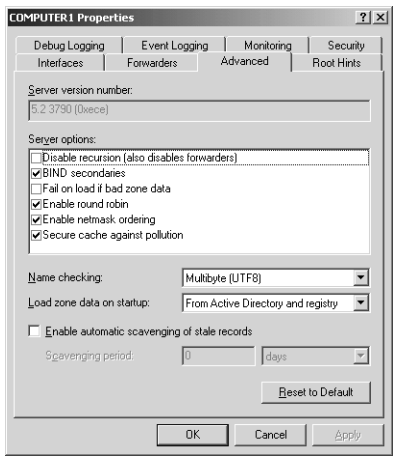


Figure 5-28 DNS server properties Advanced tab

The server installation settings include six server options, which are either on or off, and three other server features with various selections for configuration. Table 5-2 shows the default settings for all nine features.

Table 5-2 Default DNS Installation Settings

Property	Setting
Disable Recursion	Off
BIND Secondaries	On
Fail On Load If Bad Zone Data	Off
Enable Round Robin	On
Enable Netmask Ordering	On
Secure Cache Against Pollution	On
Name Checking	Multibyte (UTF8)
Load Zone Data On Startup	From Active Directory And Registry
Enable Automatic Scavenging Of Stale Records	Off (requires configuration when enabled)

In most situations, these installation defaults are acceptable and do not require modification. However, when needed, you can use the DNS console to tune these advanced parameters and accommodate special deployment needs and situations.

Exam Tip For the 70-291 exam, make sure that you at least understand Disable Recursion, BIND Secondaries, Enable Round Robin, and Enable Netmask Ordering.

You can restore these default settings at any time using the Advanced tab by clicking Reset To Default.

To restore DNS server default preferences, complete the following steps:

1. Open the DNS console.
2. In the console tree, right-click the applicable DNS server, and then select Properties.
3. In the server properties dialog box, click the Advanced tab.
4. Click Reset To Default, and then click OK.

The following sections describe the available installation options in more detail.

Disable Recursion

The Disable Recursion server option is disabled by default. Consequently, the DNS server performs recursion to resolve client queries unless a special client configuration overrides this default behavior. Through recursion, the DNS server queries other servers on behalf of the requesting client and attempts to fully resolve an FQDN. Queries

continue through iteration until the server receives an authoritative answer for the queried name. The server then forwards this answer back to the original requesting client.

When the Disable Recursion option is enabled, however, the DNS Server service does not answer the query for the client but instead provides the client with *referrals*, which are resource records that allow a DNS client to perform iterative queries to resolve an FQDN. This option might be appropriate, for example, when clients need to resolve Internet names but the local DNS server contains resource records only for the private namespace. Another case in which recursion might be disabled is when, because of its configuration or placement within a local network, a DNS server is incapable of resolving DNS names external to the local network.

Warning If you disable recursion on a DNS server using the Advanced tab, you will not be able to use forwarders on the same server, and the Forwarders tab becomes inactive.

BIND Secondaries

The BIND Secondaries option is enabled by default. As a result, DNS servers running on Windows Server 2003 do not use fast transfer format when performing a zone transfer to secondary DNS servers based on BIND. This restriction allows for zone transfer compatibility with older versions of BIND.

Note BIND is a common implementation of DNS written and ported to most available versions of the UNIX operating system.

Fast transfer format is an efficient means of transferring zone data that provides data compression and allows multiple records to be transferred per individual Transmission Control Protocol (TCP) message. Fast zone transfer is always used among Windows-based DNS servers, so the BIND Secondaries option does not affect communications among Windows servers. However, only BIND versions 4.9.4 and later can handle these fast zone transfers.

If you know your DNS server will be performing zone transfers with DNS servers using BIND version 4.9.4 or later, you should disable this option to allow fast zone transfers to occur.

Note As of this writing, the most current version of BIND is 9.3.2.

To enable or disable fast transfer format during zone transfers, complete the following steps:

1. Open the DNS console.

2. In the console tree, select the applicable DNS server.
3. From the Action menu, select Properties.

   The server properties dialog box opens.
4. Click the Advanced tab.
5. In the Server Options list, select or clear the BIND Secondaries check box, and then click OK. (This option is enabled by default.)

Fail On Load If Bad Zone Data

By default, the Fail On Load If Bad Zone Data option is disabled. As a result, a DNS server running on Windows Server 2003 loads a zone even when it determines that errors exist in the zone's database file. Errors are logged, but the zone load still proceeds. After the zone loads, the DNS server can attempt to answer queries for the zone in question.

When you enable this option, however, the DNS server does not load a zone when the server determines that errors exist in the zone's database file.

Enable Netmask Ordering

The Enable Netmask Ordering option is selected by default. This default setting ensures that, in response to a request to resolve a single computer name matching multiple host (A) resource records, DNS servers in Windows Server 2003 first return to the client any IP address that is in the same subnet as the client.

Note Multihomed computers typically have registered multiple host (A) resource records for the same host name. When a client attempts to resolve the host name of a multihomed computer by contacting a DNS server, the DNS server returns to the client a *response list* or *answer list* containing all the resource records matching the client query. Upon receiving the response list from the DNS server, a DNS client attempts to contact the target host with the first IP address in the response list. If this attempt fails, the client then attempts to contact the second IP address, and so on. The Enable Netmask Ordering option and the Enable Round Robin option are both used to change the order of resource records returned in this response list.

Simple Example: Local Network Priority A multihomed computer, server1.lucernepublishing.com, has three A resource records for each of its three IP addresses in the lucernepublishing.com zone. These three records appear in the following order in the zone, either in the zone file or in Active Directory:

```
server1   IN  A  192.168.1.27
server1   IN  A  10.0.0.14
server1   IN  A  172.16.20.4
```

When a DNS client resolver at IP address 10.4.3.2 queries the server for the IP addresses of the host server1.lucernepublishing.com, the DNS Server service notes that the originating IP network address (10.0.0.0) of the client matches the network (class A) ID of the 10.0.0.14 address in the answer list of resource records. The DNS Server service then reorders the addresses in the response list, as follows:

```
server1   IN  A  10.0.0.14
server1   IN  A  192.168.1.27
server1   IN  A  172.16.20.4
```

If the IP address of the requesting client has no local network match with any of the resource records in the answer list, the list is not prioritized in this manner.

Complex Example: Local Subnet Priority In a network that uses IP subnetting (nondefault subnet masks), a DNS server first returns any IP addresses that match both the client's network ID and subnet ID before returning any IP addresses that match only the client's network ID.

For example, a multihomed computer, server1.lucernepublishing.com, has four A resource records corresponding to each of its four IP addresses in the lucernepublishing .com zone. Two of these IP addresses are for distinct and separate networks. The other two IP addresses share a common IP network address, but because custom netmasks of 255.255.248.0 are used, the IP addresses are located in different subnets. These example resource records appear in the following order in the zone, either in the zone file or in Active Directory:

```
server1   IN  A  192.168.1.27
server1   IN  A  172.16.22.4
server1   IN  A  10.0.0.14
server1   IN  A  172.16.31.5
```

If the IP address of the requesting client is 172.16.22.8, both of the IP addresses that match the same IP network as the client, the 172.16.0.0 network, are returned at the top of the response list to the client. However, in this example, the 172.16.22.4 address is placed ahead of the 172.16.31.5 address because it matches the client IP address down through the 172.16.20.0 subnet address.

The reordered answer list returned by the DNS service follows:

```
server1   IN  A  172.16.22.4
server1   IN  A  172.16.31.5
server1   IN  A  192.168.1.27
server1   IN  A  10.0.0.14
```

To disable local subnet prioritization for multihomed names, complete the following steps:

1. Open the DNS console and select the applicable DNS server.
2. From the Action menu, select Properties.

3. In the server properties dialog box, click the Advanced tab.
4. In the Server Options list, clear the Enable Netmask Ordering check box, and then click OK.

Enable Round Robin

The Enable Round Robin option is selected by default. This setting ensures that, in response to a request to resolve the name of a multihomed computer, DNS servers in Windows Server 2003 rotate the order of matching A resource records in the response list returned to subsequent clients. This feature provides a simple way to balance the network load for frequently queried multihomed computers among all the computer's network adapters. This feature is also commonly used to balance requests among multiple servers that offer identical network services, such as an array of Web servers providing content for a single Web site.

Note Netmask ordering supersedes the use of round robin rotation for multihomed computers. When enabled, however, round robin is used as a secondary method to sort multiple records returned in a response list.

Round Robin Example The Web server named server1.lucernepublishing.com has three network adapters and three distinct IP addresses. In the stored zone (either in a database file or in Active Directory), the three A resource records mapping the host name to each of its IP addresses appear in this fixed order:

```
server1   IN  A  10.0.0.1
server1   IN  A  10.0.0.2
server1   IN  A  10.0.0.3
```

The first DNS client—Client1—that queries the server to resolve this host's name receives the list in this default order. However, when a second client—Client2—sends a subsequent query to resolve this name, the list is rotated as follows:

```
server1   IN  A  10.0.0.2
server1   IN  A  10.0.0.3
server1   IN  A  10.0.0.1
```

Exam Tip You need to know how to configure round robin on the 70-291 exam.

Disabling Round Robin When you clear the Enable Round Robin check box, round robin is disabled for the DNS server. In this case, when clients query the DNS server to resolve the host name of a multihomed computer, the server always returns the matching A resource records in the order in which those records appear in the zone.

Secure Cache Against Pollution

By default, the Secure Cache Against Pollution option is enabled. This setting allows the DNS server to protect its cache against referrals that are potentially polluting or nonsecure. When the setting is enabled, the server caches only those records with a name that corresponds to the domain for which the original queried name was made. Any referrals received from another DNS server along with a query response are simply discarded.

For example, if a query is originally made for example.microsoft.com, and a referral answer provides a record for a name outside the microsoft.com domain name tree (such as msn.com), that name is discarded if the Secure Cache Against Pollution option is enabled. This setting helps prevent unauthorized computers from impersonating another network server.

When this option is disabled, however, the server caches all the records received in response to DNS queries—even when the records do not correspond to the queried-for domain name.

Name Checking

By default, the Name Checking drop-down list box on the Advanced tab of the DNS server properties dialog box is set to Multibyte (UTF8). Thus, the DNS service, by default, verifies that all domain names handled by the DNS service conform to the Unicode Transformation Format (UTF). *Unicode* is a 2-byte encoding scheme, compatible with the traditional 1-byte US-ASCII format, that allows for binary representation of most languages.

Figure 5-29 shows the four name-checking methods you can select from the Name Checking drop-down list box, and each is described in Table 5-3.

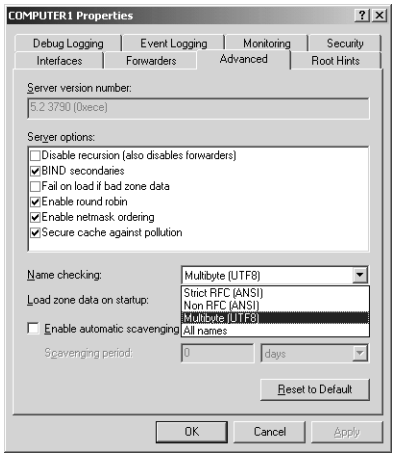


Figure 5-29 Name-checking methods

Table 5-3 Name-Checking Methods

Method	Description
Strict RFC (ANSI)	Uses strict checking of names. These restrictions, set in Request for Comments (RFC) 1123, include limiting names to uppercase and lowercase letters (A–Z, a–z), numbers (0–9), and hyphens (-). The first character of the DNS name can be a number.
Non RFC (ANSI)	Permits names that are nonstandard and that do not follow RFC 1123 Internet host naming specifications.
Multibyte (UTF8)	Permits recognition of characters other than ASCII, including Unicode, which is normally encoded as more than one octet (8 bits) in length. With this option, multibyte characters can be transformed and represented using UTF-8 support, which is provided with Windows Server 2003. Names encoded in UTF-8 format must not exceed the size limits clarified in RFC 2181, which specifies a maximum of 63 octets per label and 255 octets per name. Character count is insufficient to determine size because some UTF-8 characters exceed one octet in length. This option allows for domain names using non-English alphabets.
All Names	Permits any naming conventions.

Despite the flexibility of the UTF-8 name-checking method, you should consider changing the Name Checking option to Strict RFC when your DNS servers perform zone transfers to non-Windows servers that are not UTF-8–aware. Although DNS server implementations that are not UTF-8–aware might be able to accept the transfer of a zone containing UTF-8 encoded names, these servers might not be able to write back those names to a zone file or reload those names from a zone file.

You should use the other two Name Checking options, Non RFC and All Names, only when a specific application requires them.

Load Zone Data On Startup

By default, the Load Zone Data On Startup drop-down list box is set to the From Active Directory And Registry option. Thus, by default, DNS servers in Windows Server 2003 initialize with the settings specified in the Active Directory database and the server Registry.

However, this setting includes two other options, From Registry and From File, as shown in Figure 5-30.

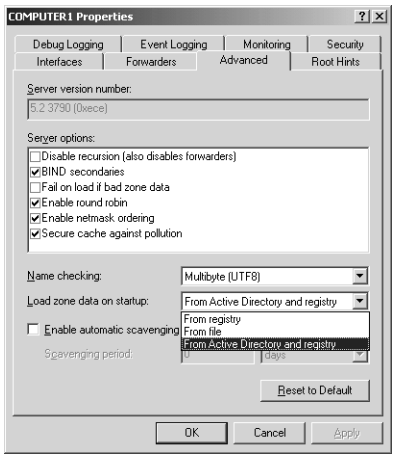


Figure 5-30 Server initialization options

When you select the From Registry option for the Load Zone Data On Startup setting, the DNS server is initialized by reading parameters stored in the Windows Registry. When you select the From File option, the DNS server is initialized by reading parameters stored in a boot file, such as those used by BIND servers.

To use such a file, you should supply a copy of a boot file from a BIND-based DNS server. On BIND-based DNS servers, this file is typically called the Named.boot file. The format of this file must be the older BIND 4 format, not the more recent BIND 8 boot file format. When a boot file is used, settings in the file are applied to the server, overriding the settings stored in the Registry on the DNS server. However, for any parameters not configurable using boot file directives, Registry defaults (or stored reconfigured server settings) are applied by the DNS Server service.

Enable Automatic Scavenging Of Stale Records

By default, the Enable Automatic Scavenging Of Stale Records option is cleared on the Advanced tab. According to this setting, DNS servers in Windows Server 2003 by default do not automatically delete stale or outdated resource records from a zone for which Aging has been enabled.

When this setting is enabled, scavenging of stale resource records is performed automatically at the interval configured in the Scavenging Period.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. You are the network administrator for Lucerne Publishing. The Lucerne Publishing network consists of a single domain, lucernepublishing.com, that is protected from the Internet by a firewall. The firewall runs on a computer named NS1 that is directly connected to the Internet. NS1 also runs the DNS Server service, and its firewall allows DNS traffic to pass between the Internet and the DNS Server service on NS1 but not between the Internet and the internal network. The DNS Server service on NS1 is configured to use round robin. Behind the firewall, two computers are running Windows Server 2003—NS2 and NS3—a primary and secondary DNS server, respectively, for the lucernepublishing.com zone.

   Users on the company network report that, although they use host names to connect to computers on the local private network, they cannot use host names to connect to Internet destinations such as *www.microsoft.com*.

   Which of the following actions requires the least amount of administrative effort to enable network users to connect to Internet host names?

   a. Disable recursion on NS2 and NS3.

   b. Enable netmask ordering on NS1.

   c. Configure NS2 and NS3 to use NS1 as a forwarder.

   d. Disable round robin on NS1.

2. You are the administrator for a large network consisting of 10 domains. You have configured a standard primary zone for the mfg.lucernepublishing.com domain on a DNS server computer named Server1. You have also configured a UNIX server, named Server2, to host a secondary zone for the same domain. The UNIX server is running BIND 8.2.1.

   You notice that zone transfers between the primary and secondary servers seem to generate more traffic than expected, putting a strain on network resources.

   What can you do to decrease the network burden of zone transfers between the primary and secondary servers?

   a. Clear the BIND Secondaries check box on Server1.

   b. Configure a boot file on Server1 to initialize BIND-compatible settings.

   c. Select the BIND Secondaries check box on Server1.

   d. Configure a boot file on Server2 to enable fast zone transfers.

3. What is the function of round robin? Which feature takes priority, round robin or netmask ordering?

   _____

   _____

4. You are the chief network administrator for the Proseware company network, which has four branch offices. Each branch office has its own LAN, which is connected to the Internet using a T1 line. Through virtual private network (VPN) connectivity over the Internet, a single intranet is maintained and replicated over Web servers at each branch office. The four Web servers have unique IP addresses but share a single FQDN, intranet.proseware.com, as shown in Figure 5-31.

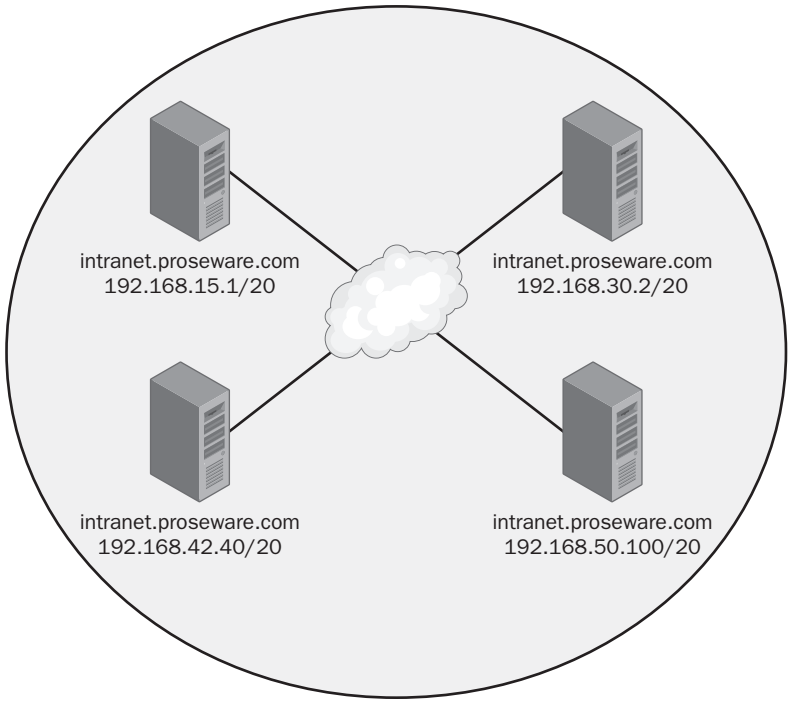


Figure 5-31 Proseware intranet servers

Within the Proseware network, a DNS client computer with the IP address 192.168.33.5 submits a query to a DNS server for the name intranet.proseware.com. Assuming that the Netmask Ordering option is enabled on the DNS server, which IP address is returned to the DNS client? (Hint: Determine which of the four Web servers shares the same subnet ID as that of the querying client computer.)

_____

_____

Lesson Summary

- The Advanced tab of the DNS server properties dialog box allows you to configure nine installation settings.
- The Disable Recursion server option is disabled by default, so recursion is enabled for the DNS server, and the server performs queries for its clients unless a special client configuration overrides this behavior.
- The BIND Secondaries option is enabled by default. Thus, DNS servers in Windows Server 2003 do not use fast transfer format when performing a zone transfer to BIND-based DNS servers. This feature allows for zone transfer compatibility with older versions of BIND.
- The Enable Netmask Ordering option is selected by default. As a result, in response to a request to resolve the name of a multihomed computer (a computer with more than one IP address), DNS servers in Windows Server 2003 by default first return to the client any IP address that is in the same subnet as the client's.
- The Enable Round Robin option is selected by default. Thus, in response to a request to resolve a name hosted at multiple addresses, and in cases where subnet prioritization does not apply, DNS servers in Windows Server 2003 by default rotate the order of matching A resource records in the response list returned to different clients.

Lesson 4: Creating Zone Delegations

Managing a large namespace such as that of the Internet would be impossible were it not for the potential to delegate the administration of domains. Through the delegation process, a new zone is created when the responsibility for a subdomain within a DNS namespace is assigned to a separate entity. This separate entity can be an autonomous organization or a branch within your company.

You can create a zone delegation in the DNS console by running the New Delegation Wizard.

After this lesson, you will be able to

- Create a delegated zone within a DNS namespace
- Explain the benefits of zone delegations

Estimated lesson time: 30 minutes

Delegating Zones

To delegate a zone means to assign authority over portions of your DNS namespace to subdomains within this namespace. A zone delegation occurs when the responsibility for the resource records of a subdomain is passed from the owner of the parent domain to the owner of the subdomain. For example, in Figure 5-32, the management of the microsoft.com domain is delegated across two zones: microsoft.com and mydomain.microsoft.com. In the example, the administrator of the mydomain.microsoft.com zone controls the resource records for that subdomain.

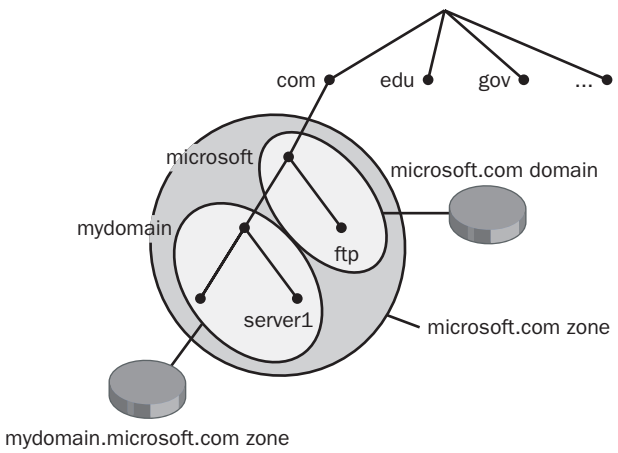


Figure 5-32 Zone delegation example

When to Delegate Zones

You should consider delegating a zone within your network whenever any of the following conditions are present:

- You need to delegate management of a DNS domain to a branch or department within your organization.
- You need to distribute the load of maintaining one large DNS database among multiple name servers to improve name resolution performance and fault tolerance.
- You need hosts and host names to be structured according to branch or departmental affiliation within your organization.

When choosing how to structure zones, you should use a plan that reflects the structure of your organization.

How Delegations Work

For a delegation to be implemented, the parent zone must contain both an A resource record and an NS resource record pointing to the authoritative server of the newly delegated domain. These records are necessary both to transfer authority to the new name servers and to provide referrals to clients performing iterative queries. In this section, you walk through an example of delegating a subdomain to a new zone.

Note These records are automatically created by the DNS console when you create a new delegation.

In Figure 5-33, an authoritative DNS server computer for the newly delegated example .microsoft.com subdomain is given a name based on a derivative subdomain included in the new zone (ns1.us.example.microsoft.com). To make this server known to others outside the newly delegated zone, two resource records are needed in the microsoft.com zone to complete delegation to the new zone. These records are automatically created when you run the New Delegation Wizard in the DNS console.

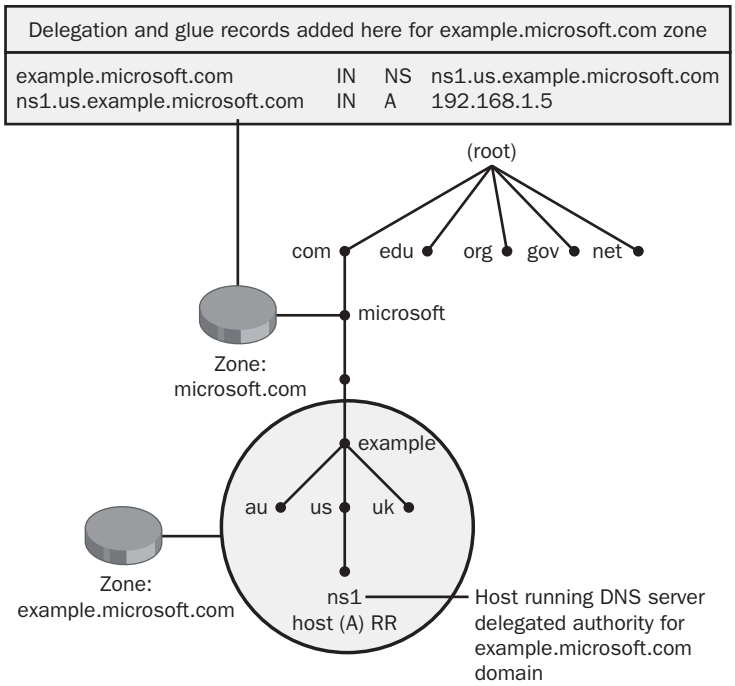


Figure 5-33 Resource records for delegation

These records include the following:

- An NS record (also known as a *delegation record*) to create the actual delegation. This record is used to advertise to querying clients that the computer named ns1.us.example.microsoft.com is an authoritative server for the delegated subdomain.
- An A resource record (also known as a *glue record*) to resolve the name of the server specified in the NS record to its IP address. Glue records are necessary when the name server authoritative for the delegated zone is also a member of the delegated domain. The process of resolving the host name in this record to the delegated DNS server in the NS record is sometimes referred to as *glue chasing*.

Note After you have created a delegation through the DNS console, a glue record appears automatically in the zone data. However, this record is hidden from view in the DNS console.

Delegation Example

An example of DNS delegation is shown in Figure 5-34. In this example, the network for the company Contoso, Inc. includes two Active Directory domains, contoso.com

and asia.contoso.com. When a client in the contoso.com domain queries for the name of hk4.asia.contoso.com, the query is directed to the local DNS server, ns.contoso.com.

Within the data file of the zone contoso.com, the name "asia" is directed to another DNS server, ns1.asia.contoso.com, by means of an NS record. A glue or host (A) record resolves that DNS server name to 192.168.3.5, to which address the query is then sent. These two records in a zone's data file thus work together to create the delegation. After the query is delegated to the server ns1.asia.contoso.com, this second DNS server then consults its own zone data to resolve the name of hk4 to the address 192.168.3.10. This response is then returned to ns.contoso.com, which then returns the response to the original client.

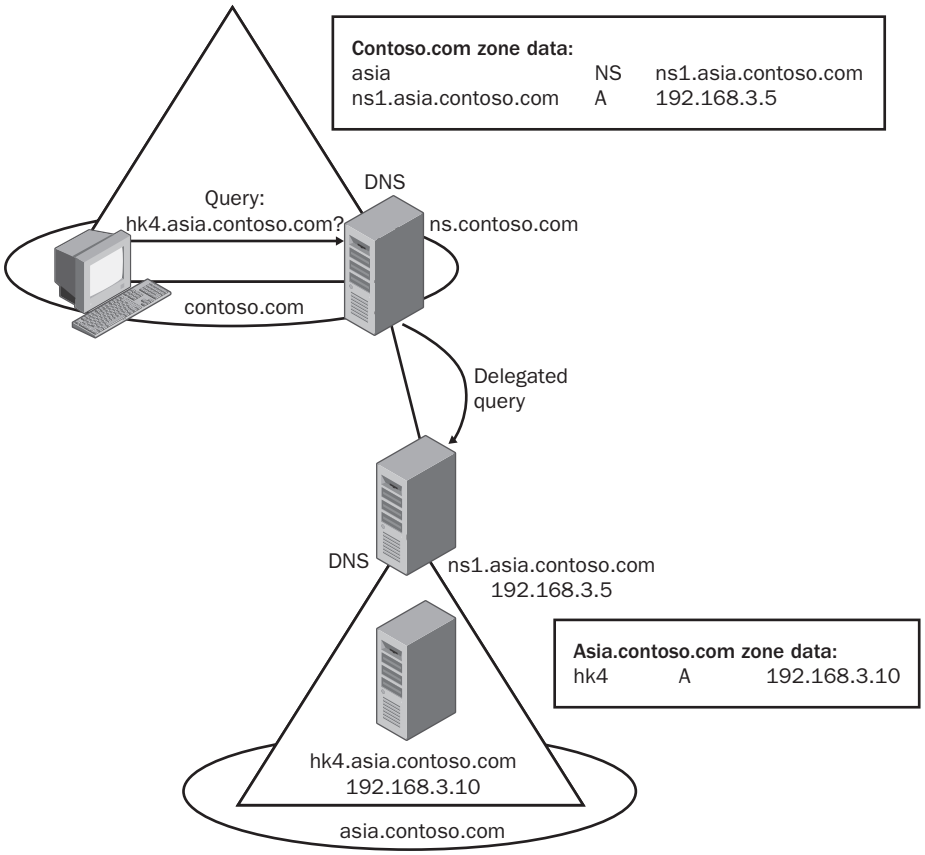


Figure 5-34 DNS delegation

Note Delegations take precedence over forwarding. If, in the preceding example, the server authoritative for the contoso.com domain were configured to forward all queries that it could not answer, the server would still answer a query for the name hk4.asia.contoso.com by contacting ns1.asia.contoso.com, not by contacting the forwarder specified on the Forwarders tab.

Creating a Zone Delegation

To create a zone delegation, first create the domain to be delegated on the server that will be hosting the delegated zone. Then run the New Delegation Wizard on the server hosting the parent zone by right-clicking the parent zone node in the DNS console and selecting New Delegation.

To complete the New Delegation Wizard, you need to specify the name of the delegated subdomain and the name of at least one name server that will be authoritative for the new zone. After you run the wizard, a node appears in the DNS console tree representing the newly delegated subdomain, and this node contains the delegation (NS) resource record of the authoritative server you have just specified. The glue record appears in the zone data but not in the DNS console.

To create a zone delegation, complete the following steps:

1. Open the DNS console.
2. In the console tree, right-click the applicable domain and select New Delegation.

   The New Delegation Wizard launches.
3. Follow the instructions provided in the New Delegation Wizard to finish creating the newly delegated domain.

Exam Tip In this lesson, we have discussed delegations of forward lookup zones, but delegations of reverse lookup zones are also used. According to RFC 2317, by using an NS record, you can configure your DNS server to delegate to another DNS server the job of resolving IP addresses to host names within your address space. (This reverse delegation may also be performed at your ISP and point to your internal DNS servers.) For example, to configure a DNS server named ns.contoso.com to delegate to another server named ns1.contoso.com reverse lookups of the address space 192.168.1.0/24, you would configure a zone named 0.1.168.192.in-addr.arpa on ns.contoso.com and add an NS record to perform the delegation. The NS record would adopt the following format: `0/24 NS ns1.contoso.com`.

Practice: Creating a Zone Delegation

In this practice, you create a new zone on Computer2 that becomes a delegated subdomain of the domain1.local domain. You then create a delegation on Computer1 that is linked to this new zone on Computer2. Finally, you verify the new configuration.

Exam Tip For simulation questions, be sure to review the procedure for creating a delegation. Performing this task will be necessary when you see a requirement stating that clients pointing to DNS servers in a parent domain must be able to resolve names in the child or subdomain.

Exercise 1: Creating a Zone to Be Delegated

In this exercise, you create a new zone on Computer2.

1. From Computer2, log on to Domain1 as Administrator.
2. Open the DNS console.
3. In the DNS console tree, right-click the Forward Lookup Zones node and select New Zone.

   The New Zone Wizard launches.
4. Click Next.

   The Zone Type page appears.
5. Click Next to accept the default selection, Primary Zone.

   The Zone Name page appears.
6. In the Name text box, type **sub.domain1.local** and click Next.

   The Zone File page appears.
7. Click Next to accept the default selection, Create A New File With This File Name.

   The Dynamic Update page appears.
8. Select Allow Both Nonsecure And Secure Dynamic Updates, and click Next.

   The Completing The New Zone Wizard page appears.
9. Click Finish.

Exercise 2: Adding Host (A) Resource Records to the Zone

In this exercise, you add records to the new zone that you will later use to verify the zone delegation.

1. From Computer2, while you are logged on to Domain1 as Administrator, open the DNS console if it is not already open.
2. In the DNS console tree, select the sub.domain1.local node. Next, right-click the Sub.domain1.local node and select New Host (A).

   The New Host dialog box appears.
3. In the Name text box, type **computer1**.
4. In the IP Address text box, type **192.168.0.1** (the IP address currently assigned to Computer1), and then click Add Host.

   A message box indicates that the host record was successfully created.

5. Click OK. The New Host dialog box remains open, with the Name text box and IP Address text box now empty.
6. In the Name text box, type **computer2**.
7. In the IP Address text box, type the IP address currently assigned to Computer2.
8. Click Add Host.

   A message box indicates that the host record was successfully created.
9. Click OK and then click Done.
10. Log off Computer2.

Exercise 3: Creating a Delegation

In this exercise, you create a delegation on Computer1 that connects to the zone sub.domain1.local on Computer2.

1. From Computer1, log on to Domain1 as Administrator.
2. Open the DNS console.
3. In the DNS console tree, select the Domain1.local node. Next, right-click the Domain1.local node and select New Delegation

   The New Delegation Wizard launches.
4. Click Next.

   The Delegated Domain Name page appears.
5. In the Delegated Domain text box, type **sub**, and then click Next.

   The Name Servers page appears.
6. Click Add.

   The New Resource Record dialog box appears.
7. In the Server Fully Qualified Domain Name text box, type **computer2.sub .domain1.local**.
8. In the IP Address text box, type the IP address currently assigned to Computer2.
9. Click Add and then click OK.
10. On the Name Servers page of the New Delegation Wizard, click Next.

    The Completing The New Delegation Wizard page appears.
11. Click Finish.

    In the DNS console tree, you will now see the sub delegation node under the domain1.local zone.

12. Use the DNS console to answer the following question: How many host (A) resource records does Computer1 hold for the sub.domain1.local domain?

_____

_____

Exercise 4: Testing the Configuration

In this exercise, you ping the hosts in the newly delegated domain. You perform this exercise on Computer1, which uses the local DNS server for name resolution.

1. If you have not already done so, from Computer1, log on to Domain1 as Administrator.
2. Open a command prompt and type **ping computer1.sub.domain1.local**. Then press ENTER.

   An output indicates that the host computer1.sub.domain1.local is responding from the IP address 192.168.0.1. If the ping is unsuccessful, at the command prompt, type **ipconfig / flushdns**, wait 2 minutes, and then press ENTER.
3. After the Ping output has completed, at the command prompt, type **ping computer2.sub.domain1.local**, and then press ENTER.

   An output indicates that computer2.sub.domain1.local is responding from the IP address 192.168.0.2. If the ping is unsuccessful, at the command prompt type **ipconfig / flushdns**, wait 2 minutes, and then press ENTER.

   The new computer names are being resolved to IP addresses even though the local computer, Computer1, conducts name resolution through the local DNS server, which contains no host records for the sub.domain1.local domain. The local DNS server is correctly forwarding queries for hosts within the sub.domain1.local subdomain to the name server authoritative for that domain, which is Computer2.
4. Log off Computer1.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. You are designing the DNS namespace for a company named Proseware, which has a registered domain name of proseware.com. Proseware has a central office in Rochester and one branch office each in Buffalo and Syracuse. Each office has a

separate LAN and network administrator. You want to configure a single DNS server at each location, and you want the central office to host the proseware.com domain. In addition, you want the administrators in Buffalo and Syracuse to maintain responsibility for DNS names and name resolution within their networks.

Which of the following steps should you take?

a. Configure a standard primary server in Rochester to host the proseware.com zone. Delegate a subdomain to each of the branch offices. Configure a secondary server in both Buffalo and Syracuse to host each of the delegated subdomains.

b. Configure a standard primary server in Rochester to host the proseware.com zone. Configure a secondary server in both Buffalo and Syracuse to improve performance and fault tolerance to the zone.

c. Configure the DNS server in Rochester to host a standard primary zone for the proseware.com domain. Configure the DNS servers in both Buffalo and Syracuse to each host a standard primary zone for a subdomain of proseware.com. Create a delegation from the DNS server in Rochester to each of these subdomains.

d. Configure the DNS server in Rochester to host a standard primary zone for the proseware.com domain. Configure the DNS servers in both Buffalo and Syracuse to host a standard primary zone for a subdomain of proseware.com. Add secondary zones on each DNS server to pull transfers from the primary zones hosted on the other two DNS servers.

2. You are the administrator for your company's network, which consists of a central office LAN and three branch office LANs, all in different cities. You have decided to design a new DNS infrastructure while deploying Active Directory on your network. Your goals for the network are, first, to implement a single Active Directory forest across all four locations, and, second, to minimize response times for users connecting to resources anywhere on the network. Assume that all branch offices have domain controllers running DNS servers.

Which of the following actions best meets these goals?

a. Configure a single Active Directory domain for all four locations and configure a single Active Directory–integrated DNS zone that replicates through the entire domain.

b. Configure a single Active Directory domain for all four locations, and configure a standard primary zone at the central office with zone transfers to secondary zones at each branch office.

c. Configure an Active Directory domain and a DNS domain for the central office, delegate a DNS subdomain to each branch office, and configure an

Active Directory–integrated zone in each location that replicates through the entire forest.

d. Configure an Active Directory domain and a DNS domain for the central office, delegate a DNS subdomain to each branch office, and configure an Active Directory–integrated zone in each location that replicates through the entire domain.

3. Which resource records are added to a parent zone to delegate a given subdomain? What are the specific functions of these records?

4. The DNS server NS1 hosts the zone lucernepublishing.com and is configured to forward all queries for which the server is not authoritative. NS1 receives a query for sub.lucernepublishing.com, a delegated subdomain. Where will the query be directed?

Lesson Summary

- To delegate a zone means to assign authority over portions of your DNS namespace to subdomains within this namespace. A zone delegation occurs when the responsibility for the resource records of a subdomain is passed from the owner of the parent domain to the owner of the subdomain.
- You should consider delegating a zone within your network when you need to delegate management of a DNS domain to a branch or department within your organization; when you need to distribute the load of maintaining one large DNS database among multiple name servers to improve name resolution performance and fault tolerance; or when you need hosts and host names to be structured according to branch or departmental affiliation within your organization.
- For a delegation to be implemented, the parent zone must contain both an A resource record and an NS resource record pointing to the authoritative server of the newly delegated domain. These records are necessary to both transfer authority to the new name servers and provide referrals to clients performing iterative queries. These records are automatically created by the DNS console when you create a new delegation.
- To create a zone delegation, first create the domain to be delegated on the server that will be hosting the delegated zone. Then run the New Delegation Wizard on the server hosting the parent zone by right-clicking the parent zone node in the DNS console and selecting New Delegation.

Lesson 5: Deploying Stub Zones

A *stub zone* is an abbreviated copy of a zone, updated regularly, that contains only the NS records belonging to a master zone. A server hosting a stub zone does not answer a query directly for the zone, but instead directs these queries to any of the name servers specified in the stub zone's NS resource records. In this way, a stub zone is functionally identical to a zone delegation. However, because stub zones can initiate and receive zone transfers from the master (delegated) zone, stub zones provide the added benefit of informing parent zones of updates in the NS records of child zones.

After this lesson, you will be able to

- Create a stub zone
- Describe the benefits and limitations of stub zones

Estimated lesson time: 30 minutes

Understanding Stub Zones

When you configure a new zone using the New Zone Wizard, you have the option of creating the new zone as a primary, secondary, or stub zone, as shown in Figure 5-35. When you create a stub zone, a zone is configured that maintains only those records—NS resource records—needed to locate the name servers of the master zone specified by the name of the stub zone.

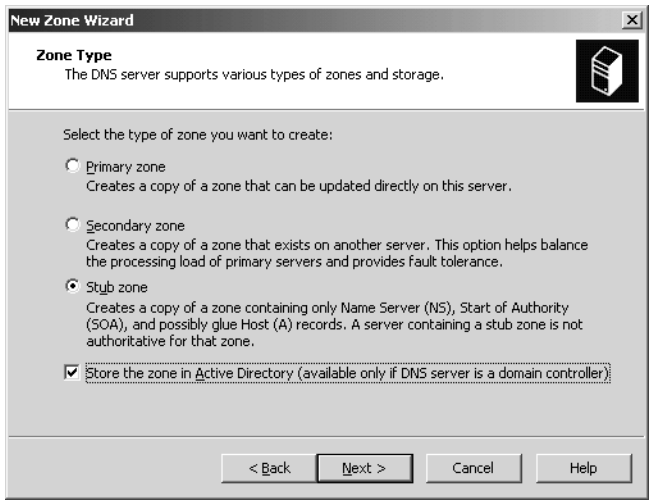


Figure 5-35 Creating a stub zone

Stub zones are used to keep all the NS resource records from a master zone current. To configure a stub zone, you need to specify at least one name server, the master, whose

IP address doesn't change. Any new name servers that you add to the master zone later are updated to the stub zone automatically through zone transfers.

You cannot modify a stub zone's resource records. Any changes you want to make to these records in a stub zone must be made in the original primary zone from which the stub zone is derived.

To add a stub zone, complete the following steps:

1. Open the DNS console.
2. In the console tree, right-click a DNS server, and then select New Zone to open the New Zone Wizard.
3. Follow the instructions to create a new stub zone.

Benefits of Stub Zones

Stub zones allow you to achieve the following benefits:

- **Improve name resolution** Stub zones enable a DNS server to perform recursion by using the stub zone's list of name servers without querying the root server.
- **Keep foreign zone information current** By updating the stub zone regularly, the DNS server hosting the stub zone maintains a current list of name servers for a different zone, such as a delegated zone on a different DNS server.
- **Delegation with updates** You can use stub zones as an alternative to zone delegations. Instead of delegating to a subdomain, in the parent domain, simply create a stub zone of the subdomain. Unlike zone delegations, stub zones enable the updates to NS records to be accounted for in the parent domain.
- **Simplify DNS administration** By using stub zones throughout your DNS infrastructure, you can distribute zone information without using secondary zones.

Important Stub zones do not serve the same purpose as secondary zones and are not an alternative when planning for fault tolerance, redundancy, or load sharing.

When to Use Stub Zones

Stub zones are most frequently used as a way to perform a zone delegation when the name servers of the delegated zone are subject to change. Most often, therefore, stub zones are hosted on the parent DNS servers of those delegated zones.

A DNS server that has delegated a subdomain to a different DNS server is usually informed of new authoritative DNS servers added to the child zone only when the resource records for these new DNS servers are added to the parent zone manually.

With stub zones, a DNS server can host a stub zone for one of its delegated zones and obtain updates of that zone's authoritative servers whenever additional name servers are added to the master zone. This functionality is explained in the example below and illustrated in Figure 5-36.

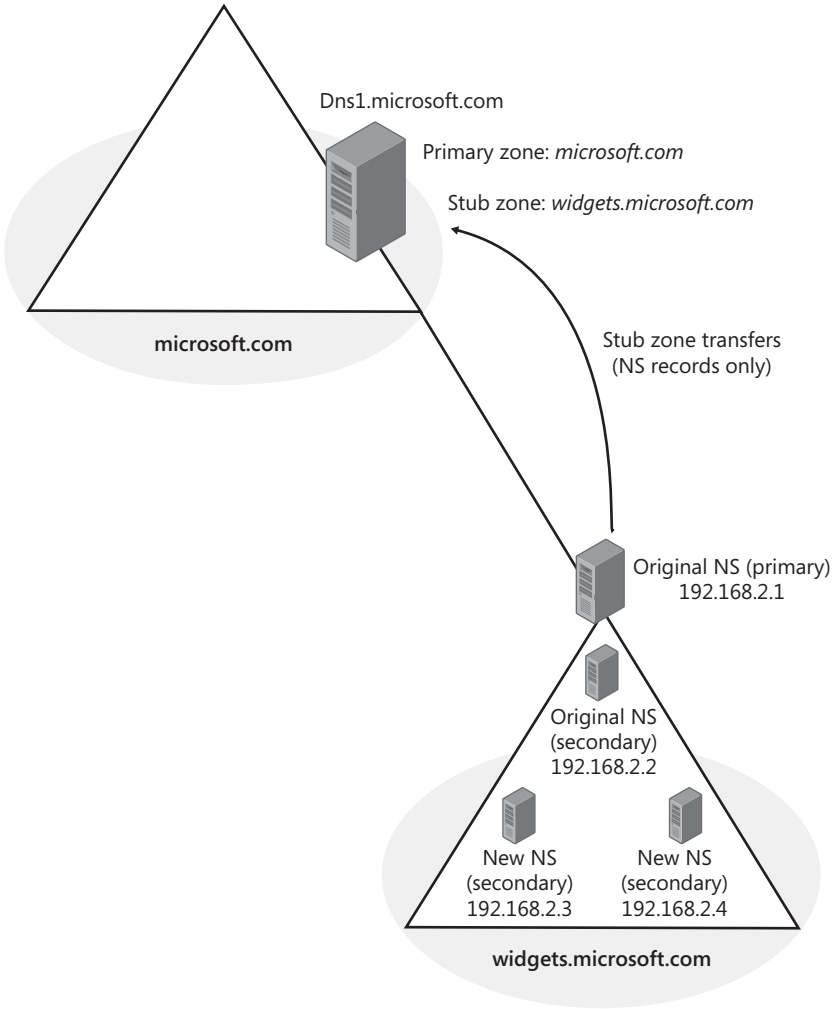


Figure 5-36 Stub zones and delegations

Exam Tip Expect to be tested on stub zones on the 70-291 exam. First and foremost, you need to be able to recognize scenarios in which deploying a stub zone is appropriate. For simulation questions, make sure that you review the procedure for creating a stub zone. To spot questions about stub zones, look for requirements stating that *any new DNS servers* added to the target zone *will appear on the list of servers* to query.

Stub Zone Example

You are an administrator for the DNS server named Dns1.microsoft.com, which is authoritative for the parent zone microsoft.com. You delegate a subdomain, widgets.microsoft.com, to separate DNS servers. When the delegation for the subdomain widgets.microsoft.com is performed, the subdomain contains only two authoritative DNS servers: 192.168.2.1 and 192.168.2.2. Later, administrators of the widgets.microsoft.com zone configure additional DNS servers as authoritative for the zone but do not notify you of this change. As a result, Dns1.microsoft.com is not configured with all the records of the new DNS servers authoritative for widgets.microsoft.com and continues to query the only two DNS servers that were defined in the original delegation.

You can remedy this situation by configuring Dns1.microsoft.com to host a stub zone for widgets.microsoft.com. When Dns1 initiates a zone transfer from the widgets.microsoft.com master zone, the server queries the widgets.microsoft.com primary server—named primary.widgets.microsoft.com—to provide the stub zone with all of the NS server records for the widgets.microsoft.com domain. As a result of this new stub zone, Dns1 learns about the new name servers authoritative for the widgets.microsoft.com child zone and is able to direct queries to all of the child zone's authoritative DNS servers.

Other Uses for Stub Zones

You can also use stub zones to facilitate name resolution across domains in a manner that avoids querying a root server or forwarder. Stub zones can thus replace secondary zones in cases where achieving DNS connectivity across domains is important but providing data redundancy for the master zone is not. Also note that stub zones improve name resolution and eliminate the burden on network resources that would otherwise result from large zone transfers.

Exam Tip Like stub zones, you can also implement conditional forwarding as a means to speed name resolution, as described in this section.

Figure 5-37 illustrates using stub zones to facilitate name resolution in this way. In the example, a query for the host name ns.mgmt.ldn.microsoft.com is submitted to two different name servers. In the first case, the server authoritative for the mfg.wa.microsoft.com domain accepts the query. Many other name servers must then be contacted before the destination name server authoritative for the appropriate domain (mgmt.ldn.microsoft.com) receives the query. In the second case, the DNS server authoritative for the actg.wa.microsoft.com domain receives a query for the same name, ns.mgmt.ldn.microsoft.com. Because this second server also hosts a stub zone for the destination mgmt.ldn.microsoft.com, the server already knows the address of

the server authoritative for ns.mgmt.ldn.microsoft.com, and it sends a recursive query directly to the authoritative server.

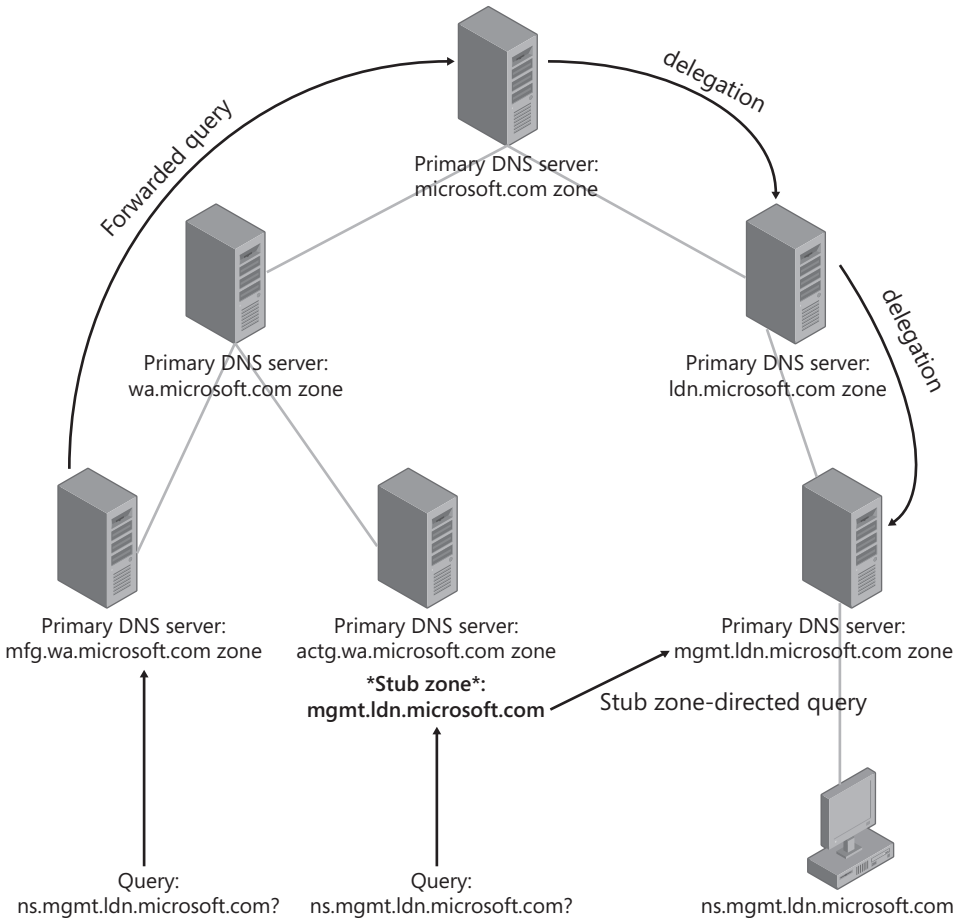


Figure 5-37 Using stub zones across domains

Stub Zone Resource Records

A stub zone contains SOA, NS, and A glue resource records for authoritative DNS servers in a zone. The SOA type identifies the primary DNS server for the actual zone (master server) and other zone property information. The NS resource record type contains a list of authoritative DNS servers for a zone (primary and secondary servers). The A glue resource records hold the IP addresses of the DNS servers authoritative for the zone.

Note As with delegations, stub zones contain glue records in the zone data, but these glue records are not visible in the DNS console.

Stub Zone Resolution

When a DNS client performs a recursive query operation on a DNS server hosting a stub zone, the DNS server may use the stub zone's resource records to resolve the query. In doing so, the DNS server first queries the authoritative servers specified in the stub zone's NS resource records. If the DNS server cannot find any of the authoritative name servers listed in its stub zone, it attempts standard recursion.

The DNS server stores the resource records it receives from a stub zone's authoritative servers in its cache and not in the stub zone itself; only the SOA, NS, and A resource records returned in response to the query are stored in the stub zone. The resource records stored in the cache are cached according to the Time to Live (TTL) value in each resource record. The SOA, NS, and A resource records, which are not written to the cache, expire according to the interval specified in the stub zone's SOA resource record, which is created during the creation of the stub zone and updated during transfers to the stub zone from the original primary zone.

When a DNS server receives a query for which recursion has been disabled, the DNS server returns to the client a referral pointing to the servers specified in the stub zone.

Stub Zone Updates

When a DNS server loads a stub zone, it queries the zone's master server for the SOA resource record, NS resource records at the zone's root, and A resource records. During updates to the stub zone, the master server is queried by the DNS server hosting the stub zone for the same resource record types requested during the loading of the stub zone. The SOA resource record's refresh interval determines when the DNS server hosting the stub zone attempts a zone transfer (update). Should an update fail, the SOA resource record's retry interval determines when the update is retried. After the retry interval has expired without a successful update, the expiration time as specified in the SOA resource record's Expires field determines when the DNS server stops using the stub zone data.

You can use the DNS console to perform the following stub zone update operations:

- **Reload** This operation reloads the stub zone from the local storage of the DNS server hosting it.
- **Transfer From Master** The DNS server hosting the stub zone determines whether the serial number in the stub zone's SOA resource record has expired and then performs a zone transfer from the stub zone's master server.
- **Reload From Master** This operation performs a zone transfer from the stub zone's master server regardless of the serial number in the stub zone's SOA resource record.

Exam Tip For the 70-291 exam, you need to understand the differences among these three operations, which can apply to secondary zones as well as stub zones.

Practice: Deploying a Stub Zone

In this practice, you create on Computer1 a stub zone that pulls transfers from the delegated subdomain sub.domain1.local.

Note Although this exercise describes the process of adding a stub zone for a subdomain that has already been delegated, a delegation does not actually need to be configured for the stub zone to function. In other words, you can think of a stub zone as a replacement for a delegation and not merely as a feature added to a delegation, as is the case in this scenario.

Exercise 1: Creating a Stub Zone

In this exercise, you run the New Zone Wizard on Computer1 to create a stub zone.

Important The following exercise assumes that you have installed the DNS server on Computer2 by using the Windows Components Wizard (as described in Chapter 4, Lesson 3). In this case, zone transfers from the Sub.domain1.local zone are enabled by default but restricted to authoritative name servers. If instead you have installed the DNS server on Computer2 by using the Manage Your Server window to add the DNS server role, zone transfers for all locally hosted zones are disabled by default. In this case, before beginning this exercise, be sure to enable zone transfers for the Sub.domain1.local zone and restrict zone transfers to servers listed on the Name Servers tab.

1. From Computer1, log on to Domain1 as Administrator.
2. At a command prompt, type the following command: **dnscmd computer2 /recordadd sub.domain1.local @ ns computer1.domain1.local**.

   This command adds Computer1 to the Name Servers tab in the Sub.domain1.local Properties dialog box in the DNS console on Computer2.
3. Open the DNS console, right-click the Forward Lookup Zones node, and select New Zone.

   The New Zone Wizard launches.
4. Click Next.

   The Zone Type page appears.

5. Select Stub Zone, clear the Store The Zone In Active Directory check box, and click Next.

   The Zone Name page appears.

6. In the Zone Name text box, type **sub.domain1.local**, and then click Next.

   The Zone File page appears.

7. Click Next to accept the default selection, Create A New File With This File Name.

   The Master DNS Servers page appears.

8. In the IP Address text box, type the IP address currently assigned to Computer2, click Add, and then click Next.

   The Completing The New Zone Wizard page appears.

9. Click Finish.

   The sub.domain1.local zone now appears in the DNS console tree under the Forward Lookup Zones node.

10. Right-click the Sub.domain1.local node in the console tree (not the details pane), and then select Transfer From Master.

Tip If you receive an error message, wait 10 seconds and try step 10 again.

11. When the zone loads successfully, the node shows only three resource records: the SOA resource record for the zone and the NS resource records pointing to Computer2 and Computer1.

12. Log off Computer1.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. What is the most common use of a stub zone?

   _____

   _____

2. Which of the following is *not* a benefit of using a stub zone?

   a. Improving name resolution performance

   b. Keeping foreign zone information current

c. Simplifying DNS administration

d. Increasing fault tolerance for DNS servers

3. When would you choose to implement a stub zone over a secondary zone? When would you choose to implement a secondary zone over a stub zone?

Lesson Summary

- A stub zone is an abbreviated copy of a zone, updated regularly, that contains only the NS records belonging to a master zone. Stub zones are most frequently used as an alternative to delegation. Compared to delegations, stub zones provide the added benefit of enabling parent zones to keep an updated list of authoritative name servers in the subzone.
- Stub zones can also be used to facilitate name resolution across domains in a manner that avoids querying the root server or forwarder in the root domain of a DNS namespace.
- To create a stub zone, you open the New Zone Wizard by right-clicking the DNS server icon in the DNS console and selecting New Zone. In the New Zone Wizard, you select the stub zone type and then follow the wizard's instructions.
- To configure a stub zone, you need to specify at least one name server, the master, with an IP address that does not change. Any new name servers that you add to the master zone are later updated to the stub zone automatically through zone transfers.
- Stub zones do not serve the same purpose as secondary zones and are not an alternative when planning for fault tolerance, redundancy, or load sharing.

Case Scenario Exercise

You have been hired as a consultant by Lucerne Publishing, which is in the process of redeploying its DNS server infrastructure on Windows Server 2003. Lucerne Publishing's in-house network designer, Klaus, has requested your services for your expertise in Windows Server 2003.

Lucerne Publishing has its headquarters in Lucerne and has two branch offices in Bern and Geneva. The Lucerne branch hosts the parent domain, lucernepublishing.com. The Bern and Geneva offices each host child domains and contain their own domain

controllers. The DNS servers in Bern and Geneva have been configured to forward unresolved queries to the DNS server in Lucerne.

Figure 5-38 presents the relevant portion of the network.

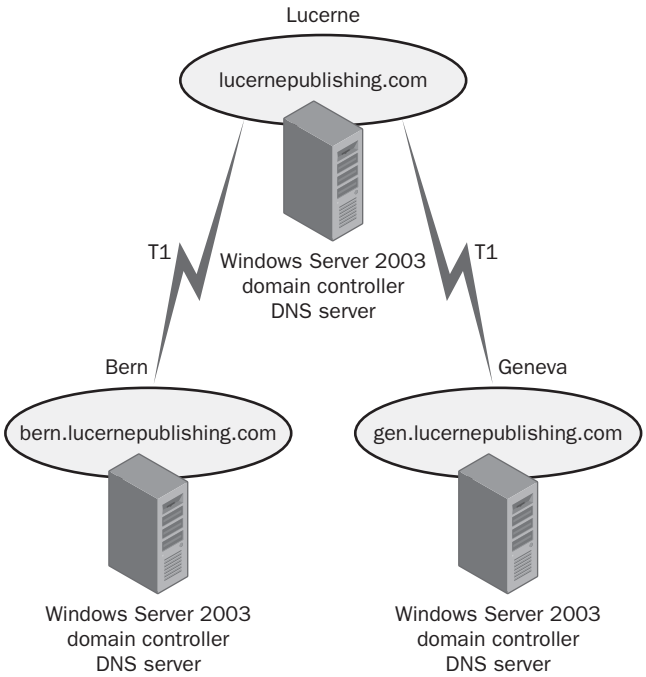


Figure 5-38 Lucerne Publishing's network

Klaus wants to achieve four goals in his network:

- Minimize name resolution traffic across WAN links
- Minimize DNS replication traffic across WAN links
- Secure DNS replication traffic across WAN links
- Optimize name resolution traffic for client computers

1. Which of these goals are met by deploying an Active Directory–integrated zone with the default replication scope on domain controllers in all three locations throughout the network?

_____

_____

2. If an Active Directory–integrated zone is deployed for the lucernepublishing.com domain, which option should you recommend be configured in the Change Zone

Replication Scope dialog box shown in Figure 5-39? Assume that improving name resolution response time is more important than minimizing network traffic.

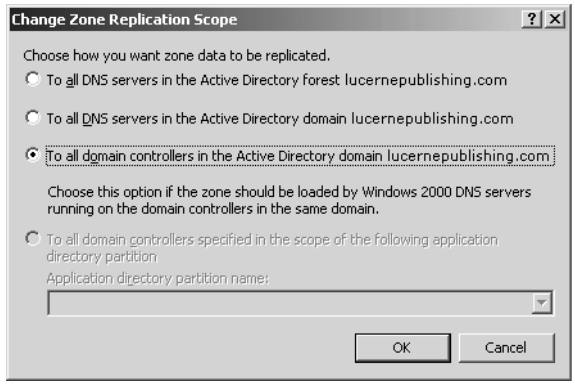


Figure 5-39 Zone replication scope settings for the lucernepublishing.com domain

3. The Bern branch office has 200 employees, and you want to deploy DNS in a way that minimizes the administrative load for network managers at the Lucerne office. However, you also want DNS servers in headquarters to be updated on any new authoritative servers deployed in the Bern office. How can you achieve these goals?

4. Klaus has informed you that his network administrators have unsuccessfully attempted to deploy a test secondary DNS server in one of the branch offices. He says the administrators specified the correct IP address of a primary DNS server running Windows Server 2003 in the Lucerne office, yet the secondary server was unable to transfer data from the primary zone. Given that this test network was successfully deployed on Windows 2000 a few years ago, what is the most likely cause of the problem?

Troubleshooting Lab

In the following exercise, you fix a faulty Active Directory installation on Computer1 by automatically recreating missing SRV resource records with the Netdiag utility. You then configure the domain1.local zone to allow only secure dynamic updates. This strategy can be useful in troubleshooting fake networked computers, in which malicious intruders assume DNS registrations owned by domain computers.

1. From Computer1, log on to Domain1 as Administrator.
2. Open the DNS console.
3. Delete the following two SRV resource records: _kerberos._tcp.dc._msdcs.domain1.local, and _ldap._tcp.dc._msdcs.domain1.local.
4. Close the DNS console.

   Make sure Computer1 is not connected to the Internet when you perform the following step.

5. At a command prompt, type **netdiag /fix**.
6. The utility runs for a few moments. After it has completed, browse the output. You will see that some tests have failed and some fixes have been applied.
7. Open the DNS console and browse to the _tcp.dc._msdcs.domain1.local domain.

   In the details pane, you can see that the two records you deleted have been recreated.

8. Close the DNS console.
9. Open a command prompt and enter **dnscmd /zoneresettype domain1.local /dsprimary**.

   This command changes the domain1.local zone to an Active Directory–integrated zone. This type of zone allows you to require secure dynamic updates.

10. At the command prompt, type **dnscmd . / config domain1.local /allowupdate 2**.

    This command configures domain1.local to allow only secure updates. When secure updates are required, only the computer that first created a resource record is allowed to update that record.

11. Open the DNS console, and then open the Domain1.local Properties dialog box. On the General tab, you can see that the zone is now described as Active Directory–Integrated and that it allows only secure dynamic updates.
12. Close the DNS console, and then log off Computer1.

Chapter Summary

- The Forwarders tab of the DNS server properties dialog box allows you to forward DNS queries received by the local DNS server to upstream DNS servers, called forwarders. This tab also allows you to disable recursion for select queries (as specified by domain).
- The Root Hints tab of the DNS server properties dialog box provides a simple way to modify the contents in the Cache.dns file. If you are using your DNS server to resolve Internet names, you do not normally need to modify these entries. However, if you are using your DNS server only to answer queries for hosts in a separate and private DNS namespace, you should alter these root hints to point to the root servers in your network. Finally, if your DNS server computer is itself the root server (named ".") of your private namespace, you should delete the Cache.dns file.
- When you deploy a DNS server on a domain controller, you can choose to store the zone data in the Active Directory database. Active Directory–integrated zones minimize zone transfer traffic, improve security, decrease administrative overhead, and improve fault tolerance. You can configure zone data to be replicated among all DNS servers in the Active Directory forest, among all DNS servers in the Active Directory domain, among all domain controllers in the Active Directory domain, or among all servers enlisted in a custom application directory partition.
- When nonsecure dynamic updates are allowed in a zone, any computer can update a resource record in a DNS zone. When only secure dynamic updates are allowed, only the owner of a record can update it. Secure dynamic updates can be required only on Active Directory–integrated zones.
- The Zone Transfers tab allows you to restrict transfers from the current zone. By default, zone transfers from primary servers are either completely disabled or limited to servers specified on the Name Servers tab. The nature of this restriction depends upon the manner in which the DNS server has been installed.
- To delegate a zone means to assign authority over portions of your DNS namespace to subdomains within this namespace. A zone delegation occurs when the responsibility for the resource records of a subdomain is passed from the owner of the parent domain to the owner of the subdomain.
- A stub zone is an abbreviated copy of a zone, updated regularly, that contains only the SOA and NS resource records belonging to the master zone. Stub zones are most frequently used as an alternative to delegation. Compared to delegations, stub zones provide the added benefit of enabling parent zones to keep an updated list of authoritative name servers in the subzone.

Exam Highlights

Before taking the exam, review the key points and terms that are presented in this chapter.

Key Points

- DNS is the most highly tested area on the 70-291 exam. Therefore, you should be comfortable with all of the settings on the DNS server properties tabs and all of the settings on the zone properties tabs.
- Be very comfortable with the DNS console interface because you are likely to see at least one simulation question related to DNS.
- Understand the various zone replication scope options available for Active Directory–integrated zones.
- Understand the scenarios in which forwarding or conditional forwarding is likely to be deployed.
- Understand the difference between secure and nonsecure dynamic updates.
- Understand the scenarios in which primaries, secondaries, stub zones, and Active Directory–integrated zones are likely to be deployed.
- Understand the scenarios in which delegations are likely to be configured.

Key Terms

application directory partition A partition of data replicated in the Active Directory database on a subset of domain controllers. Application directory partitions contain information for use by a particular application or service, such as DNS.

recursion The process of answering a DNS query on behalf of a DNS client.

Questions and Answers

Page 5-13

Lesson 1, Practice 1, Exercise 1

15. What is the essential difference between the two captures?

In Name Resolution 2, the first two frames are a DNS query and DNS response for the name computer1.domain1.local. In Name Resolution 1, the NetBIOS over TCP/ IP (NetBT) protocol was used to resolve the name Computer2 on the LAN. This difference shows that DNS has replaced NetBIOS as the name resolution method on the network.

What accounts for the difference in name resolution methods?

In Windows Server 2003 networks, DNS name resolution is attempted before NetBIOS name resolution. NetBIOS resolution was performed in the first example because DNS was not fully configured on the network.

Page 5-15

Lesson 1, Practice 2, Exercise 1

9. What is the restriction that applies to clients running Microsoft Windows 95 and Microsoft Windows NT 4 SP3 or earlier?

By default, these clients will not be able to log on to a domain through a domain controller running Windows Server 2003.

Page 5-18

Lesson 1 Review

1. How can you use forwarding to increase security of DNS queries?

When an internal DNS server performs iterative queries on the Internet to resolve names, this process requires your internal network to be exposed to outside servers. Through forwarding, you can restrict cross-firewall DNS traffic to only two computers—the internal forwarding DNS server and the DNS forwarder outside a firewall. With this arrangement, the external forwarder can perform iterative queries on behalf of internal servers without exposing the network.

2. Using the DNS server properties dialog box, how can you prevent a multihomed DNS server from answering DNS queries received through specific network cards?

On the Interfaces tab, you can configure the server to listen for DNS queries through only one IP address.

3. You administer a network that consists of a single domain. On this network, you have configured a new DNS server named DNS1 to answer queries for Internet names from the local domain. However, although DNS1 is connected to the Internet, it continues to fail its recursive test on the Monitoring tab of the server properties dialog box. Which of the following could be the potential cause for the failure?

a. You have configured DNS1 in front of a firewall.

b. DNS1 hosts a zone named ".".

c. Your root hints have not been modified from the defaults.

d. You have not configured DNS1 to forward any queries to upstream servers.

b

4. Which of the following events could serve as a legitimate reason to modify (but not delete) the default root hints on the Root Hints tab of a DNS server properties dialog box? (Choose all that apply.)

a. The Internet root servers have changed.

b. The server will not be used as a root server.

c. You have disabled recursion on the server.

d. Your server is not used to resolve Internet names.

a, d

Page 5-39

Lesson 2, Practice, Exercise 1

19. Which functions on the Action menu are available for the domain1.local zone through the COMPUTER2 node that are not available on the Action menu for the same zone through the COMPUTER1 node?

New functions are Transfer From Master and Reload From Master.

Can you create or configure resource records for domain1.local through the COMPUTER2 node in the DNS console?

No, you cannot create or configure resource records for domain1.local through the COMPUTER2 node.

Page 5-41

Lesson 2, Practice, Exercise 2

5. According to the settings on the Start Of Authority (SOA) tab, if Computer2 loses contact with Computer1, how long will the DNS server on Computer2 continue to answer queries from DNS clients?

One day

How often is Computer2 configured to query Computer1 to find out whether any changes have been made to the zone?

Every 15 minutes

If Computer2 discovers it cannot contact Computer1 when it initiates an SOA query, how long does it wait before trying again?

10 minutes

If another primary DNS server named dns.domain2.local successfully queries Computer1 for the IP address of Computer2, how long does Computer2's A resource record stay alive in the cache of dns.domain2.local?

1 hour

Page 5-43

Lesson 2 Review

1. Describe the process by which secondary servers determine whether a zone transfer should be initiated.

The secondary server conducts an SOA query, in which the serial number value in the primary zone's SOA resource record is compared to the serial number value in the secondary server's own version of the zone database. If the secondary server determines that the master zone has a higher serial number, a transfer is initiated.

2. What is the difference between IXFR and AXFR queries?

IXFR queries initiate an incremental zone transfer. In these transfers, only the updated information is transferred across the network. AXFR queries initiate an all zone transfer. In these transfers, the complete zone database is transferred across the network.

3. You have multiple DHCP servers on your network, some of which are configured to register DNS records on behalf of pre–Windows 2000 clients. You have configured DNS to allow only secure updates. However, you find that some DNS records are not being updated properly. How can you solve this problem?

Add the DHCP servers to the DnsUpdateProxy built-in security group.

4. You oversee administration for a WAN belonging to the Proseware company, which has one central office in Rochester and two branch offices in Buffalo and Syracuse. The network, which consists of one domain, has one primary DNS zone running on a Windows Server 2003 computer at the central office, and one secondary DNS zone at each branch. Network users are complaining that they often cannot connect to sites at remote branches. Administrators have determined that network bandwidth between the central office and branches has become saturated with zone transfers, and that zone transfers are being initiated before they can complete. Which of the following steps would help resolve the problem with the least effort?

a. Install Active Directory on the network, and promote the servers hosting the secondary DNS zones to domain controllers.

b. Increase the network bandwidth by establishing a fiber-optic connection between the two sites.

c. Increase the refresh interval on the primary DNS server.

d. Increase the refresh interval on the secondary DNS servers.

c

5. You discover that an administrator has adjusted the default TTL value for your company's primary DNS zone to 5 minutes. Which of the following is the most likely effect of this change?

   a. Resource records cached on the primary DNS server expire after 5 minutes.

   b. DNS clients have to query the server more frequently to resolve names for which the server is authoritative.

   c. Secondary servers initiate a zone transfer every 5 minutes.

   d. DNS hosts reregister their records more frequently.

   b

6. Which of the following is not a benefit of storing DNS zones in the Active Directory database?

   a. Less frequent transfers

   b. Decreased need for administration

   c. Less saturation of network bandwidth

   d. Secure dynamic updates

   a

Page 5-53

Lesson 3 Review

1. Which of the following actions requires the least amount of administrative effort to enable network users to connect to Internet host names?

   a. Disable recursion on NS2 and NS3.

   b. Enable netmask ordering on NS1.

   c. Configure NS2 and NS3 to use NS1 as a forwarder.

   d. Disable round robin on NS1.

   c

2. What can you do to decrease the network burden of zone transfers between the primary and secondary servers?

   a. Clear the BIND Secondaries check box on Server1.

   b. Configure a boot file on Server1 to initialize BIND-compatible settings.

   c. Select the BIND Secondaries check box on Server1.

   d. Configure a boot file on Server2 to enable fast zone transfers.

   a

3. What is the function of round robin? Which feature takes priority, round robin or netmask ordering?

   Round robin rotates the order of matching resource records in the response list returned to DNS clients. Each successive DNS client that queries for a multihomed name gets a different resource record at the top of the list. Round robin is secondary to subnet prioritization. When the Enable Netmask Ordering check box is also selected, round robin is used as a secondary means to order returned resource records for multihomed names.

4. You are the chief network administrator for the Proseware company network, which has four branch offices. Each branch office has its own LAN, which is connected to the Internet using a T1 line. Through virtual private network (VPN) connectivity over the Internet, a single intranet is maintained and replicated over Web servers at each branch office. The four Web servers have unique IP addresses but share a single FQDN, intranet.proseware.com, as shown in Figure 5-40.

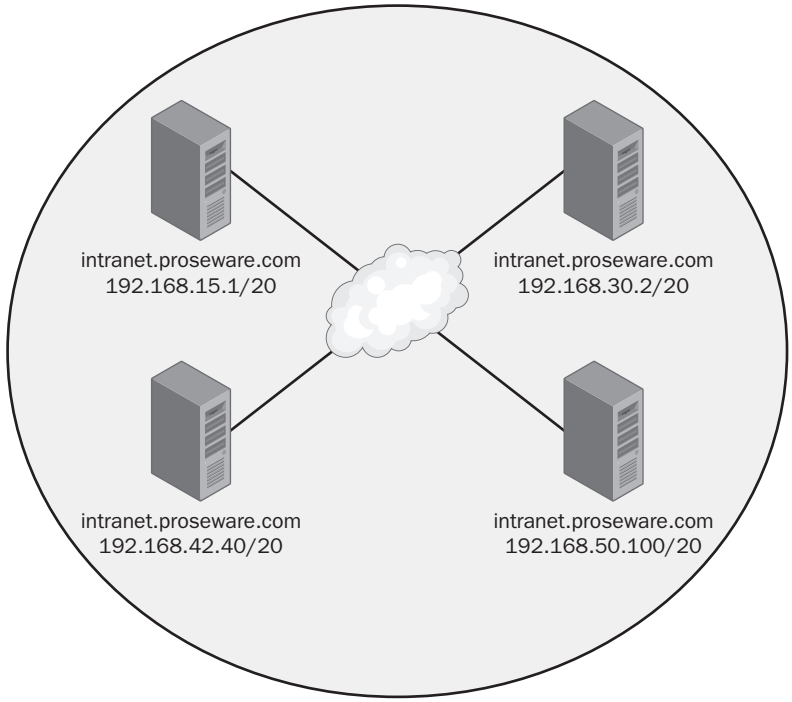


Figure 5-40 Proseware intranet servers

Within the Proseware network, a DNS client computer with the IP address 192.168.33.5 submits a query to a DNS server for the name intranet.proseware.com. Assuming that the Netmask Ordering option is enabled on the DNS server, which IP address is returned to the DNS client? (Hint: Determine which of the four Web servers shares the same subnet ID as that of the querying client computer.)

192.168.42.40

Page 5-63

Lesson 4, Practice, Exercise 3

12. Use the DNS console to answer the following question: How many A resource records does Computer1 hold for the sub.domain1.local domain?

None

Page 5-64

Lesson 4 Review

1. You are designing the DNS namespace for a company named Proseware, which has a registered domain name of proseware.com. Proseware has a central office in Rochester and one branch office each in Buffalo and Syracuse. Each office has a separate LAN and network administrator. You want to configure a single DNS server at each location, and you want the central office to host the proseware.com domain. In addition, you want the administrators in Buffalo and Syracuse to maintain responsibility for DNS names and name resolution within their networks.

Which of the following steps should you take?

a. Configure a standard primary server in Rochester to host the proseware.com zone. Delegate a subdomain to each of the branch offices. Configure a secondary server in both Buffalo and Syracuse to host each of the delegated subdomains.

b. Configure a standard primary server in Rochester to host the proseware.com zone. Configure a secondary server in both Buffalo and Syracuse to improve performance and fault tolerance to the zone.

c. Configure the DNS server in Rochester to host a standard primary zone for the proseware.com domain. Configure the DNS servers in both Buffalo and Syracuse to each host a standard primary zone for a subdomain of proseware.com. Create a delegation from the DNS server in Rochester to each of these subdomains.

d. Configure the DNS server in Rochester to host a standard primary zone for the proseware.com domain. Configure the DNS servers in both Buffalo and Syracuse to host a standard primary zone for a subdomain of proseware.com. Add secondary zones on each DNS server to pull transfers from the primary zones hosted on the other two DNS servers.

c

2. You are the administrator for your company's network, which consists of a central office LAN and three branch office LANs, all in different cities. You have decided to design a new DNS infrastructure while deploying Active Directory on your network. Your goals for the network are first to implement a single Active Directory forest across all four locations and second to minimize response times for users connecting to resources anywhere on the network. Assume that all branch offices have domain controllers running DNS servers.

Which of the following actions best meets these goals?

a. Configure a single Active Directory domain for all four locations and configure a single Active Directory–integrated DNS zone that replicates through the entire domain.

b. Configure a single Active Directory domain for all four locations, and configure a standard primary zone at the central office with zone transfers to secondary zones at each branch office.

c. Configure an Active Directory domain and a DNS domain for the central office, delegate a DNS subdomain to each branch office, and configure an Active Directory–integrated zone in each location that replicates through the entire forest.

d. Configure an Active Directory domain and a DNS domain for the central office, delegate a DNS subdomain to each branch office, and configure an Active Directory–integrated zone in each location that replicates through the entire domain.

a

3. Which resource records are added to a parent zone to delegate a given subdomain? What are the specific functions of these records?

An NS resource record and an A resource record are created in the delegated subdomain on the parent zone. The NS resource record directs queries to the DNS server, specified by name, that is authoritative for the delegated zone. The A resource record, called a glue record, allows the computer name specified in the NS resource record to be mapped to an IP address.

4. The DNS server NS1 hosts the zone lucernepublishing.com and is configured to forward all queries for which the server is not authoritative. NS1 receives a query for sub.lucernepublishing.com, a delegated subdomain. Where will the query be directed?

The query will be directed to the server authoritative for the sub.lucernepublishing.com zone, not to the configured forwarder.

Page 5-74

Lesson 5 Review

1. What is the most common use of a stub zone?

A stub zone is most frequently used as an alternative to delegation. Compared to a delegation, a stub zone provides the added benefit of enabling a parent zone to keep an updated list of authoritative name servers in the subzone.

2. Which of the following is *not* a benefit of using a stub zone?

a. Improving name resolution performance

b. Keeping foreign zone information current

c. Simplifying DNS administration

d. Increasing fault tolerance for DNS servers

d

3. When would you choose to implement a stub zone over a secondary zone? When would you choose to implement a secondary zone over a stub zone?

A stub zone is preferable to a secondary server when you want to avoid the storage demands of a full secondary zone or the network resource demands associated with zone transfers. You should implement a secondary zone instead of a stub zone when you need to provide data redundancy for your master zone and when improving query response times across WAN links is more important than minimizing zone transfer traffic.

Page 5-75

Case Scenario Exercise

1. Which of these goals are met by deploying an Active Directory–integrated zone on domain controllers in all three locations throughout the network?

All four goals are met by this solution.

2. If an Active Directory–integrated zone is deployed for the lucernepublishing.com domain, which option should you recommend be configured in the Change Zone Replication Scope dialog box shown in Figure 5-41? Assume that improving name resolution response time is more important than minimizing network traffic.

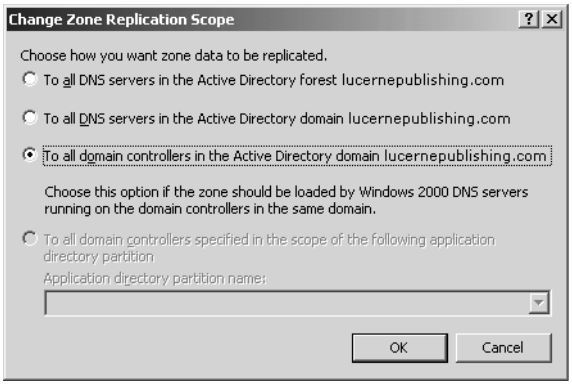


Figure 5-41 Zone replication scope settings for the lucernepublishing.com domain

To All DNS Servers In The Active Directory Forest Lucernepublishing.com

3. The Bern branch office has 200 employees, and you want to deploy DNS in a way that minimizes the administrative load for network managers at the Lucerne office. However, you also want DNS servers in headquarters to be updated on any new authoritative servers deployed in the Bern office. How can you achieve these goals?

Create a delegation for the bern.lucernepublishing.com domain, and then deploy a stub zone at headquarters that transfers NS records from the primary server of the bern .lucernepublishing.com.

4. Klaus has informed you that his network administrators have unsuccessfully attempted to deploy a test secondary DNS server in one of the branch offices. He says the administrators specified the correct IP address of a primary DNS server running Windows Server 2003 in the Lucerne office, yet the secondary server was unable to transfer data from the primary zone. Given that this test network was successfully deployed on Windows 2000 a few years ago, what is the most likely cause of the problem?

   In Windows Server 2003, zone transfers from primary servers by default are either completely disabled or restricted to servers specified on the Name Servers tab. The nature of this default restriction depends on the manner in which the DNS server has been installed. By selecting the Allow Zone Transfers check box in the zone properties dialog box, selecting Only To Servers Listed On The Name Servers Tab, and then specifying the secondary server on the Name Servers tab in zone properties, you create the necessary NS resource record and allow zone transfers.