

Lesson 12: Deploying and Configuring the DNS Service

MOAC 70-410: Installing and Configuring
Windows Server 2012

Overview

- Exam Objective 4.3: Deploy and Configure DNS Service
- Understanding the DNS Architecture
- Designing a DNS Deployment
- Creating Internet Domains
- Creating Internal Domains
- Deploying a DNS Server

Understanding the DNS Architecture

Lesson 12: Deploying and Configuring the
DNS Service

Understanding the DNS Architecture

- Host names are easier for us to remember than IP addresses.
- Computers need to resolve the host names we use to IP addresses in order to communicate with other computers.
- This conversion process is referred to as **name resolution**.
- **Host tables** were used when networks were small, but are impractical today.
- Today, **Domain Name System (DNS)** servers convert host names into IP addresses.

Creating a DNS Standard

At its core, the DNS is still a list of names and their equivalent IP addresses, but the methods for creating, storing, and retrieving those names is very different from those in a host table. The DNS consists of three elements:

- The DNS name space
- Name servers
- Resolvers

The DNS Name Space

- The DNS standards define a tree-structured name space in which each branch of the tree identifies a **domain**.
- Each domain contains a collection of **resource records** that contain host names, IP addresses, and other information.
- Query operations are attempts to retrieve specific resource records from a particular domain.

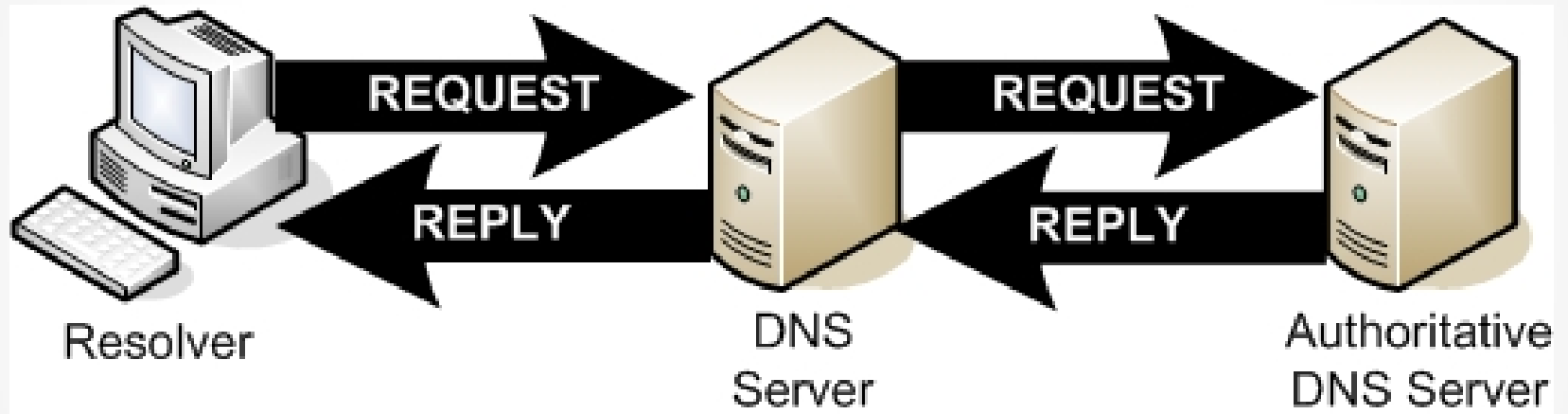
Name Servers

- A DNS server is an application running on a server computer that maintains information about the domain tree structure and (usually) contains authoritative information about one or more specific domains in that structure.
- The application responds to queries for information about the domains for which it is the authority and forwards queries about other domains to other name servers.
- This enables any DNS server to access information about any domain in the tree.

Resolvers

- A **resolver** is a client program that generates DNS queries and sends them to a DNS server for fulfillment.
- A resolver has direct access to at least one DNS server and can also process referrals to direct its queries to other servers when necessary.

Creating a DNS Standard

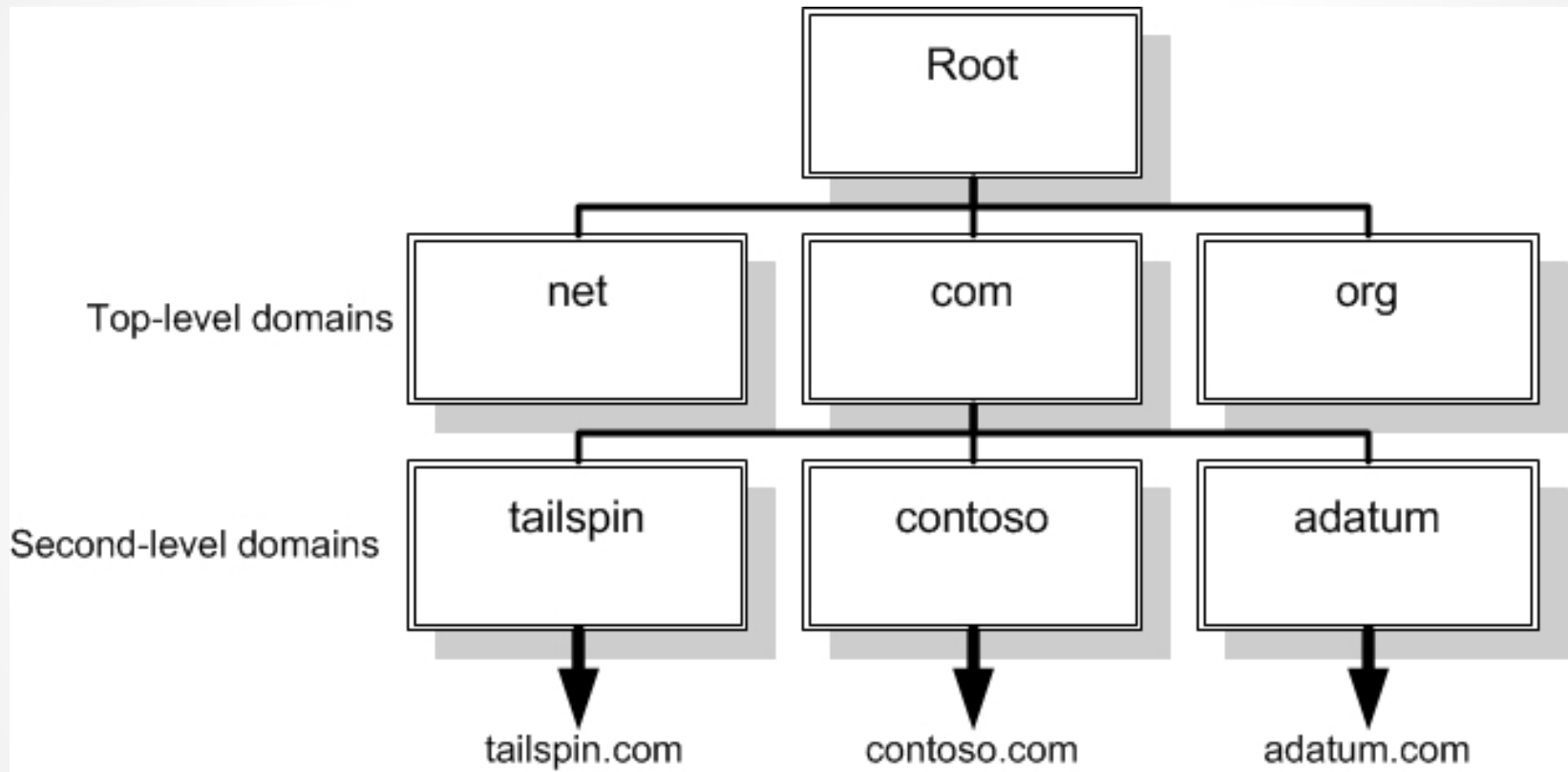


DNS servers relay requests and replies to other DNS servers

DNS Naming

- A two-tiered system, consisting of domain names and host names
- Obtain Domain names from a centralized authority, to ensure uniqueness
- Assign the host names within that domain
- Internet websites use this naming method
- We access web servers using a Uniform Resource Locator (URL), such as:
<http://www.contoso.com>

DNS Naming



The DNS domain hierarchy

The DNS Domain Hierarchy

- The authoritative source for a domain is the DNS server responsible for maintaining that domain's resource records.
- DNS servers can locate the authoritative source for any domain name, by communicating with other DNS servers.
- Domains at each level of the hierarchy are responsible for maintaining information about the domains in the next lower level.
- The **root name servers** are the highest-level DNS servers in the entire namespace.
- All DNS server implementations are preconfigured with the IP addresses of the root name servers.

Top-Level Domains

The original DNS name space called for six **generic top-level domains (gTLDs)**, dedicated to specific purposes:

- **com**: Commercial organizations
- **edu**: Four-year, degree-granting educational institutions in North America
- **gov**: United States government institutions
- **mil**: United States military applications
- **net**: Networking organizations
- **org**: Noncommercial organizations

ICANN's New Top-Level Domains

- ICANN is also responsible for the ratification of new top-level domains:
 - aero
 - biz
 - coop
 - info
 - museum
 - name
 - pro
 - asia
 - cat
 - jobs
 - mobi
 - tel
 - travel

Top-Level Domains

- The root name servers do nothing but respond to millions of requests by sending out the addresses of the authoritative servers for the top-level domains.
- The top-level domain servers do the same for the second-level domains.
- There are no hosts in the root or top-level domains.

Country Code Domains

There are hundreds of two-letter **country-code top-level domains (ccTLDs)**:

- **fr** for France
- **de** for Deutschland (Germany)
- **us** for the United States
- **ca** for Canada

Each domain is permitted to establish its own prices and requirements for registration of subdomains.

Second-Level Domains

- Each top-level domain has its own collection of second-level domains.
- Individuals and organizations can purchase these domains for their own use.
- To use the domain name, you must supply the registrar with the IP addresses of two DNS servers that you want to be the authoritative sources for information about the domain.
- The administrators of the top-level domain servers then create resource records pointing to these authoritative servers.

Subdomains

- Once you purchase the rights to a second-level domain, you can create as many hosts as you want in that domain by creating new resource records on the authoritative servers.
- You can also create as many additional domain levels as you want with only a few limitations:
 - Each individual domain name can be no more than 63 characters long.
 - The total FQDN (including the trailing period) can be no more than 255 characters long.

DNS Messaging

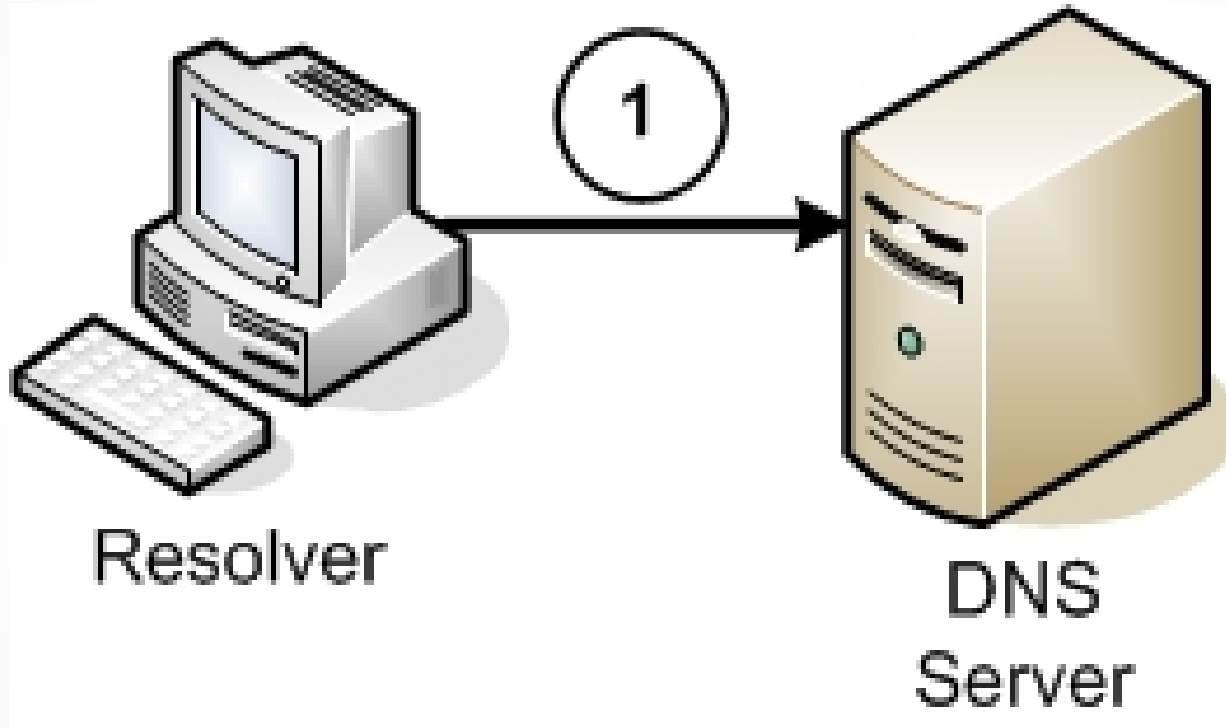
The Domain Name System uses a single message format for all communications that consists of the following five sections:

- **Header:** Contains information about the nature of the message.
- **Question:** Contains the information being requested from the destination server.
- **Answer:** Contains resource records supplying the information requested in the Question section.
- **Authority:** Contains resource records pointing to an authority for the information requested in the Question section.
- **Additional:** Contains resource records with additional information in response to the Question section.

DNS Communications

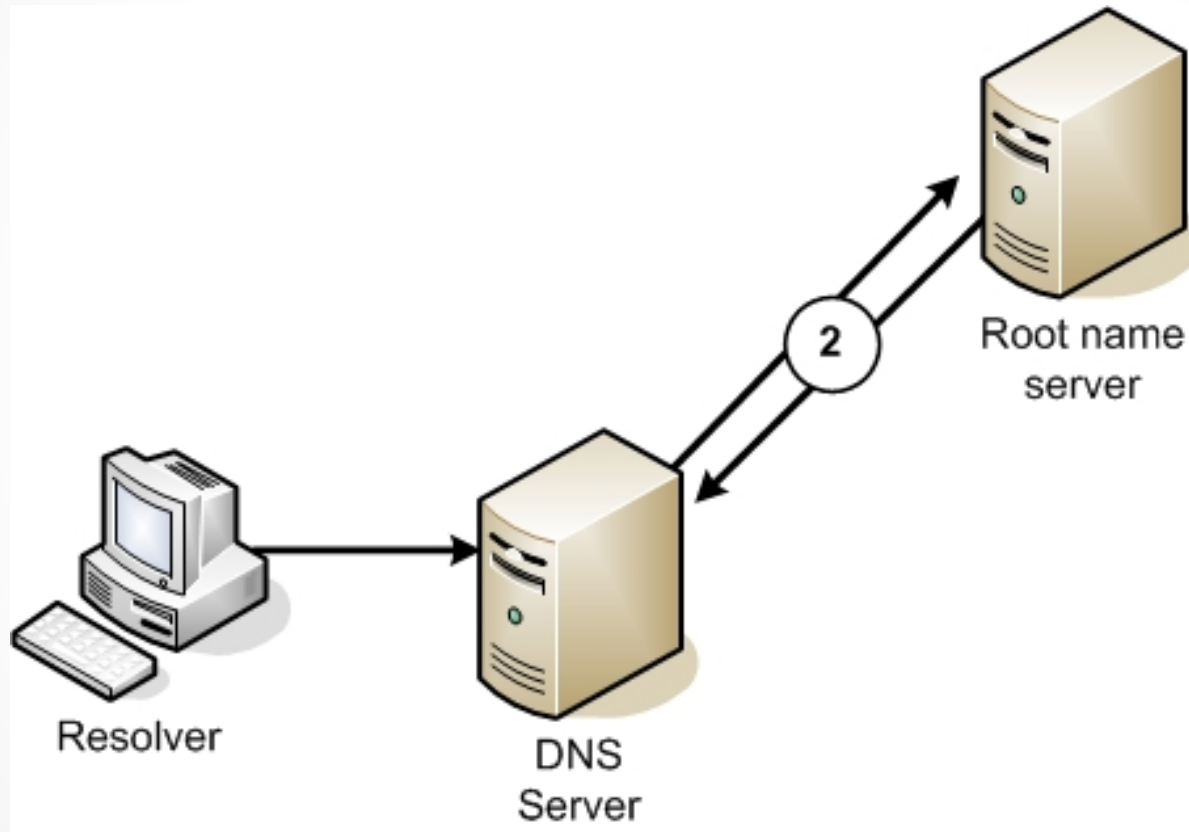
- Type a URL containing a DNS name (**www.microsoft.com**) into the browser's Address box and press Enter.
- You will see a message that says something like “**Finding Site: www.microsoft.com.**”
- Then, a few seconds later, you will see a message that says “**Connecting to,**” followed by an IP address.
- It is during this interval that the DNS name resolution process occurs.

DNS Communications



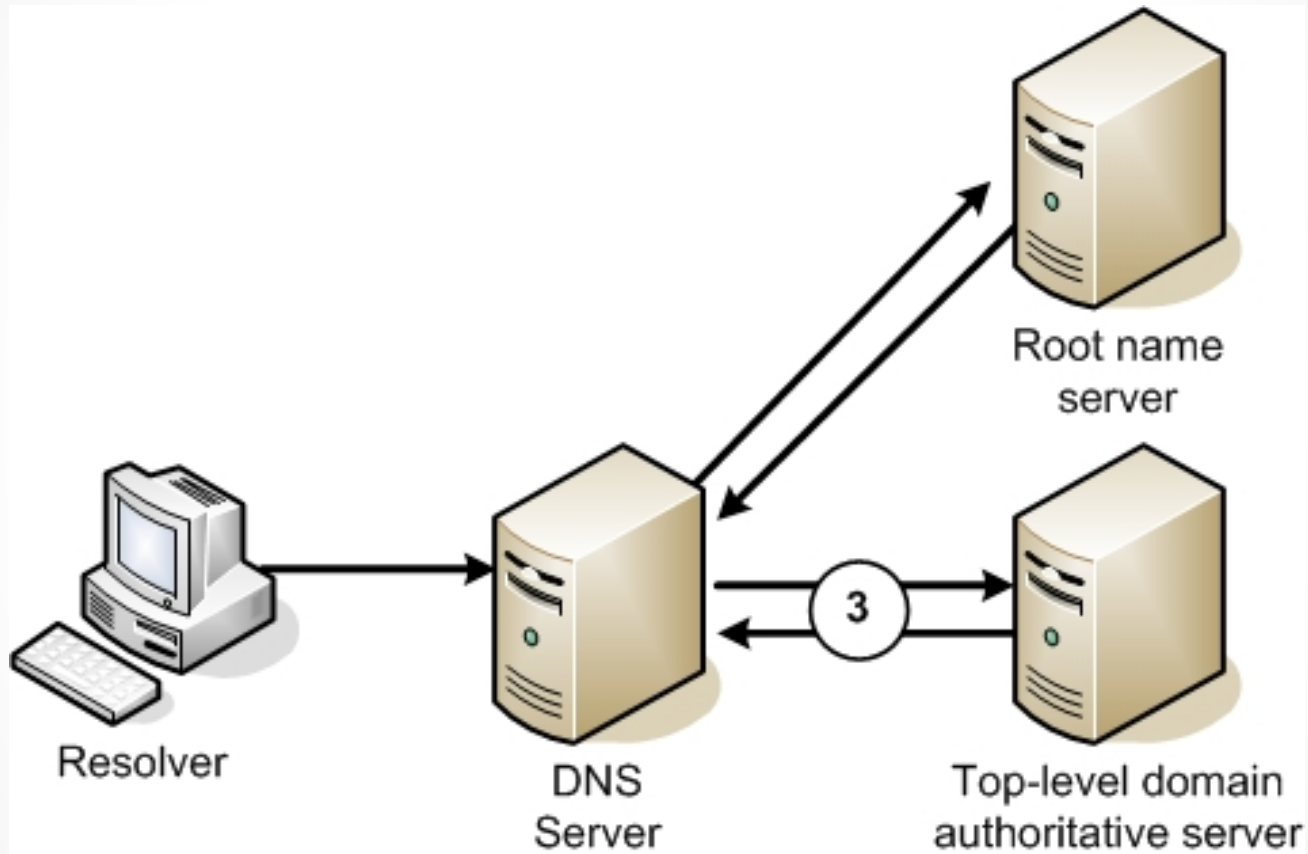
A DNS client sends a name resolution request to its designated DNS server

DNS Communications



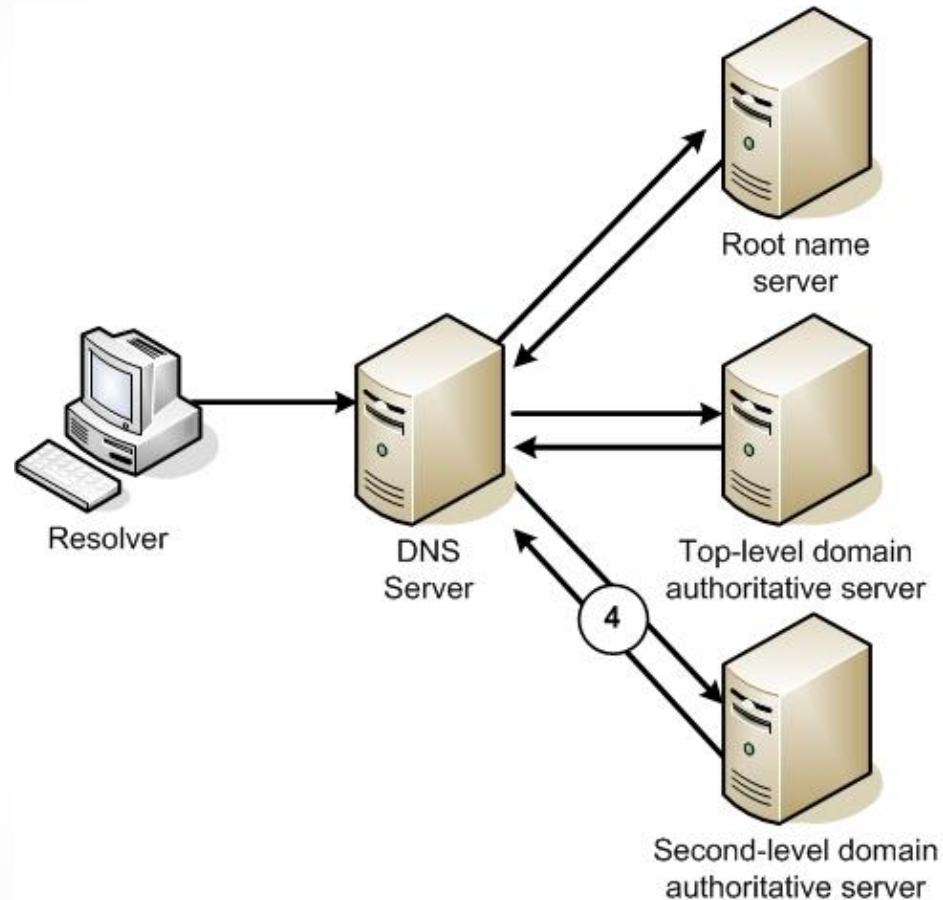
The client's DNS server forwards an iterative query to a root name server

DNS Communications



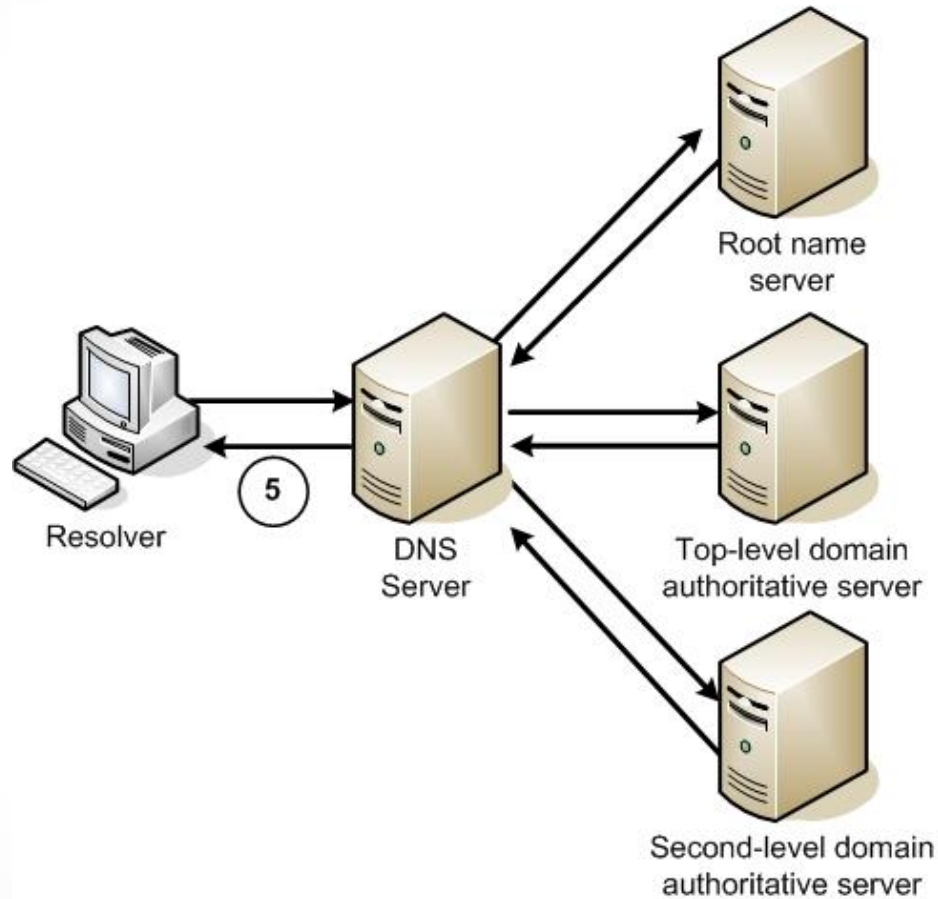
The client's DNS server forwards an iterative query to a top-level domain server

DNS Communications



The client's DNS server forwards an iterative query to a second-level domain server

DNS Communications

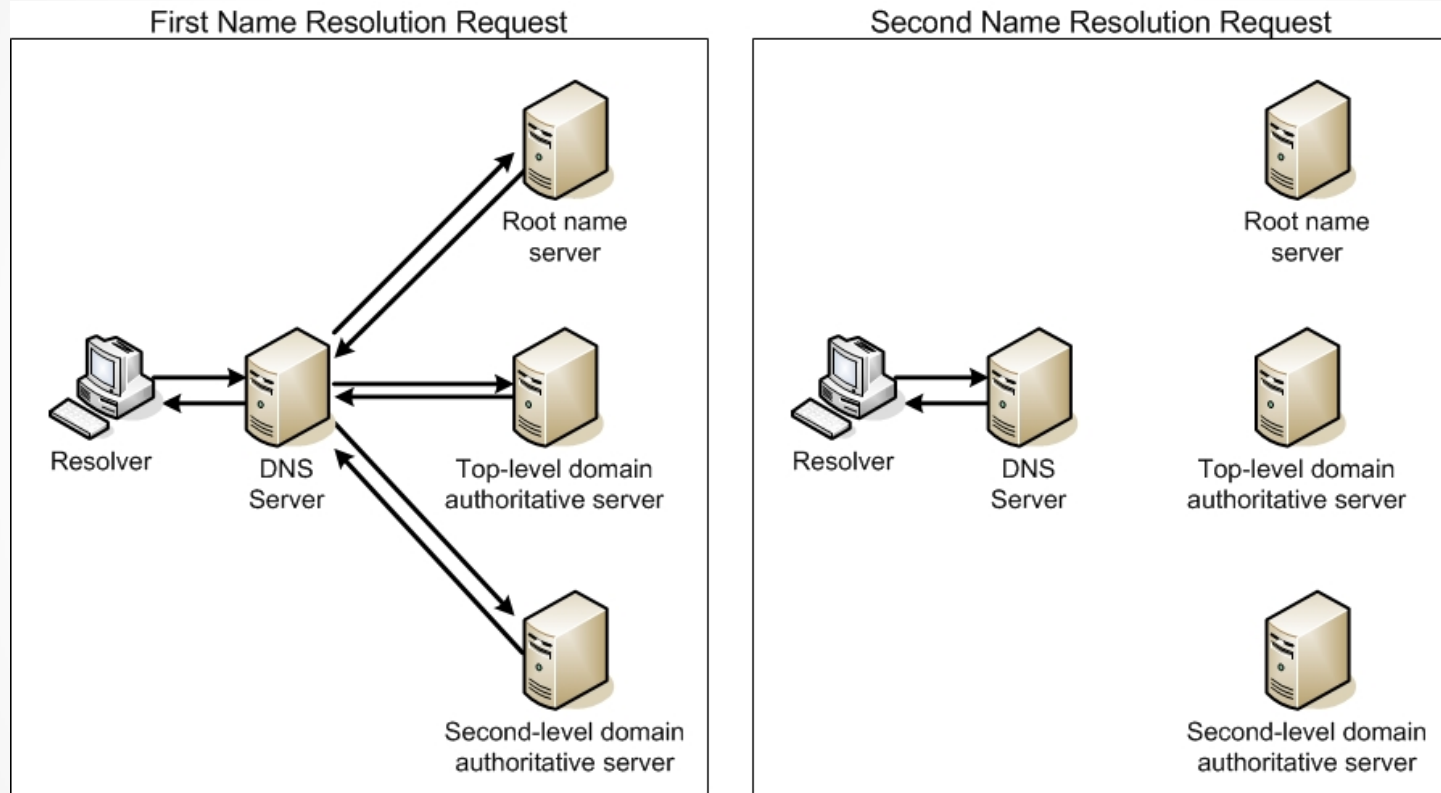


The client's DNS server returns the IP address supplied by the authoritative server to the client

DNS Server Caching

- DNS servers are capable of retaining the information they learn about the DNS name space in the course of their name resolution procedures and storing it in a cache on the local drive.
- The next time that a client requests the resolution of a previously resolved name, the server can respond immediately with the cached information.

DNS Server Caching



Name caching enables the second name resolution request for the same name to bypass the referral process

Negative Caching

- **Negative caching** occurs when a DNS server retains information about names that do not exist in a domain.
- Top-level domain server will return a reply containing an error message which will then be retained in the requesting DNS server's cache.

Cache Data Persistence

- Caching is a vital element of the DNS architecture, because it reduces the number of requests sent to the root name and top-level domain servers.
- The amount of time that DNS data remains cached on a server is called its **Time To Live (TTL)**.
- The administrators of each authoritative DNS server specify how long the data for the resource records in their domains or zones should be retained in the servers where it is cached.

Cache Data Persistence

The screenshot shows the 'adatum.local Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The dialog is divided into three main sections: 'WINS', 'Zone Transfers', and 'Security'. The 'Zone Transfers' section is further divided into 'Start of Authority (SOA)' and 'Name Servers'. The 'Start of Authority (SOA)' section contains the following fields and controls:

- Serial number:** A text box containing '48' and an 'Increment' button.
- Primary server:** A text box containing 'servera.adatum.local.' and a 'Browse...' button.
- Responsible person:** A text box containing 'hostmaster.adatum.local.' and a 'Browse...' button.
- Refresh interval:** A numeric box with '15' and a dropdown menu set to 'minutes'.
- Retry interval:** A numeric box with '10' and a dropdown menu set to 'minutes'.
- Expires after:** A numeric box with '1' and a dropdown menu set to 'days'.
- Minimum (default) TTL:** A numeric box with '1' and a dropdown menu set to 'hours'.
- TTL for this record:** A text box containing '0 :1 :0 :0' and the format '(DDDD:HH.MM.SS)'.

At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

The Start of Authority (SOA) tab on a DNS server's Properties sheet

DNS Referrals and Queries

The process by which one DNS server sends a name resolution request to another DNS server is called a **referral**.

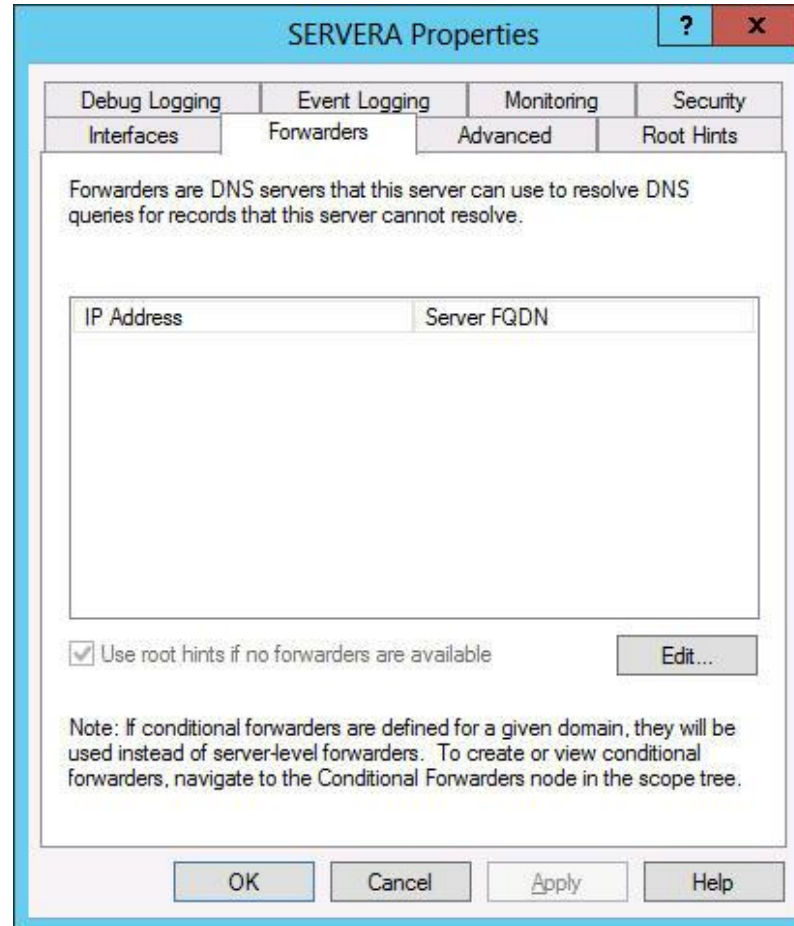
DNS servers recognize two types of name resolution requests:

- **Recursive query:** The DNS server receiving the name resolution request takes full responsibility for resolving the name. If the server possesses information about the requested name, it replies immediately to the requestor.
- **Iterative query:** The server that receives the name resolution request immediately responds with the best information it possesses at the time. This information could be cached or authoritative, and it could be a resource record containing a fully resolved name or a reference to another DNS server. DNS servers use iterative queries when communicating with each other.

DNS Forwarders

- DNS servers send recursive queries to other servers when you configure a server to function as a **forwarder**.
- On a network running several DNS servers, you may not want all the servers sending queries to other DNS servers on the Internet.

DNS Forwarders

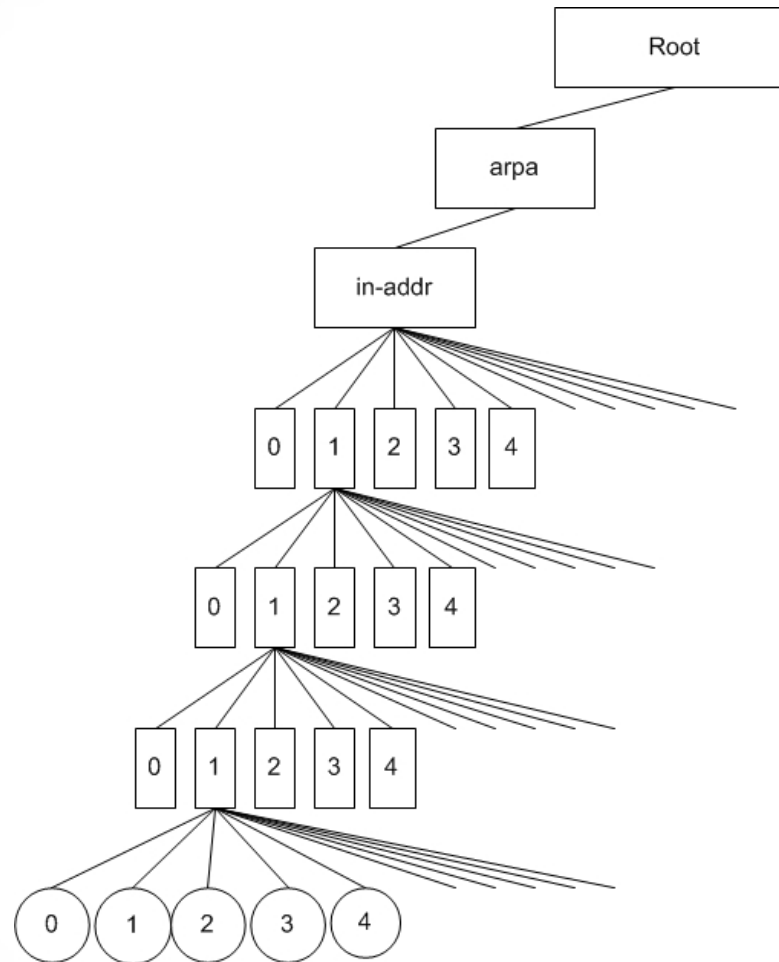


The Forwarders tab on a DNS server's Properties sheet

Reverse Name Resolution

- **Reverse name resolution** is when a computer needs to convert an IP address into a DNS name.
- A special domain called **in-addr.arpa** is specifically designed for reverse name resolution.
- For example, to resolve the IP address 192.168.89.34 into a name, a DNS server would locate a domain called 89.168.192.in-addr.arpa in the usual manner and read the contents of a resource record named 34 in that domain.

Reverse Name Resolution



The DNS reverse lookup domain

Designing a DNS Deployment

Lesson 12: Deploying and Configuring the
DNS Service

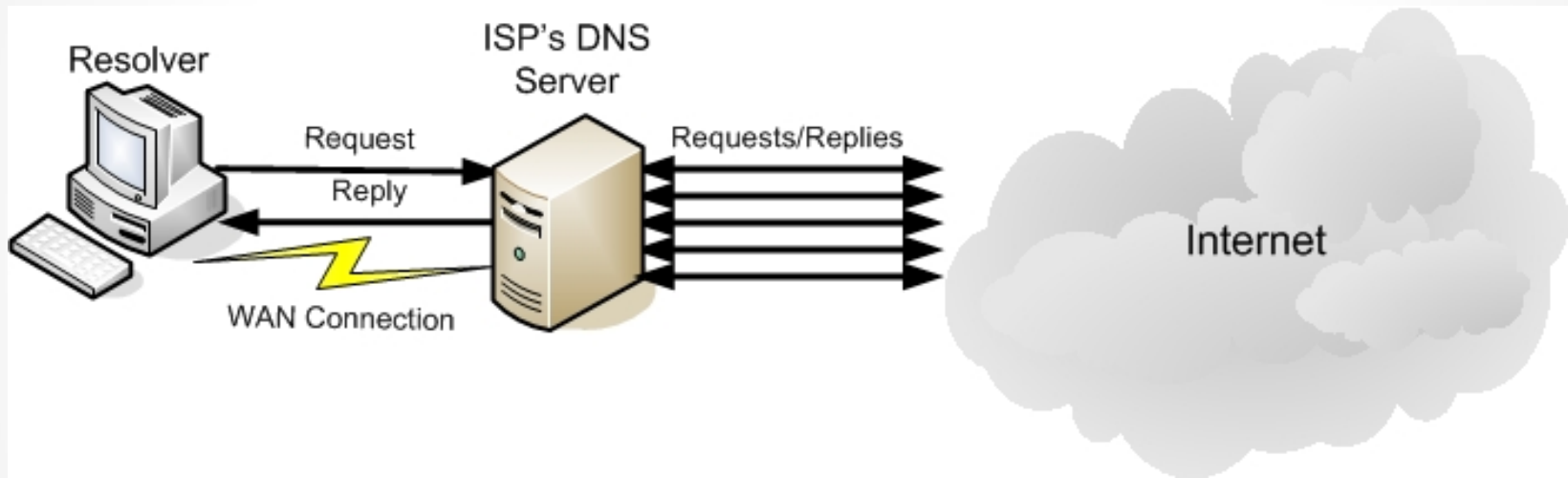
Designing a DNS Deployment

- Every computer on a TCP/IP network needs access to a DNS server.
- Internet service providers (ISPs) nearly always include the use of their DNS servers into their rates, and in some cases, it might be better to use other DNS servers, rather than run your own.
- The first factor in designing a DNS deployment is what DNS services your network requires.

Resolving Internet Names

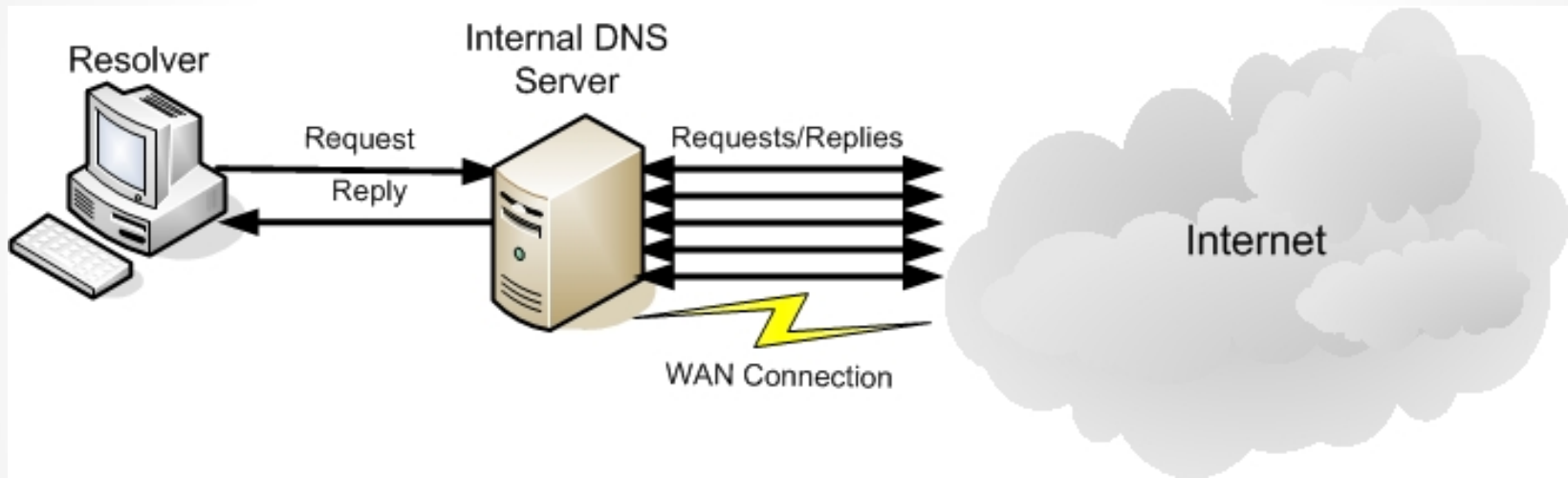
- A **caching-only server** is not the authoritative source for any domain and hosts no resource records of its own.
- It is used for Internet name resolution purposes, and it processes incoming queries from resolvers and sends its own queries to other DNS servers on the Internet.
- As a general rule, if your network requires no DNS services other than name resolution, you should consider using off-site DNS servers.

Resolving Internet Names



Using an ISP's caching-only DNS server

Resolving Internet Names



Using your own caching-only DNS server

Hosting Internet Domains

- One advantage to hosting your domain on your own DNS servers is the ability to modify your resource records at will.
- Using a commercial domain hosting service provides greater reliability, in the form of redundant servers and Internet connections, so your DNS records are always available.

Hosting Active Directory Domains

- You must have at least one DNS server on the network that supports the Service Location (SRV) resource record, in order to run Active Directory Domain Services (AD DS).
- The DNS server does not have to have a registered IP address or an Internet domain name.

Integrating DHCP and DNS

- To resolve a DNS name into an IP address, the DNS server must have a resource record containing a name and IP address.
- DHCP creates an environment where IP addresses can change.
- **Dynamic Updates in the Domain Name System (DNS UPDATE)** enables a DNS server to modify resource records at the request of DHCP servers and clients.
- When a DHCP server assigns an address to a client, it also sends the commands to the DNS server to create or update the records.

Separating DNS Services

- You do not have to choose to have your DNS servers entirely external, or entirely internal.
- It is possible to use a single DNS server to host both Internet and Active Directory domains, as well as to provide clients with name resolution services and DHCP support.
- Services are independent from each other; therefore, you might want to split these functions by using several DNS servers.
- You can use a commercial service provider to host your Internet domain while keeping your Active Directory domain hosting and dynamic update services internal.

Creating Internet Domains

Lesson 12: Deploying and Configuring the
DNS Service

Creating Internet Domains

- Most organizations register a single second-level domain and use it to host all their Internet servers.
- The name will depend on what is available.
- If your name is already taken:
 - Choose a different domain name.
 - Register the name in a different top-level domain.
 - Attempt to purchase the domain name from its current owner.

Creating Internet Domains

Some organizations maintain multiple sites on the Internet.

There are two basic ways to implement multiple sites on the Internet:

- Register a single second-level domain name and then create multiple subdomains beneath.
- Register multiple second-level domains: If your organization consists of multiple, completely unrelated brands or operations, this is often the best solution.

Creating Internal Domains

Lesson 12: Deploying and Configuring the
DNS Service

Creating Internal Domains

When you are designing a DNS namespace for a network that uses Active Directory Domain Services, the DNS domain name hierarchy is directly related to the directory service hierarchy.

Names for Your Internal Domains

- Keep domain names short
- Avoid an excessive number of domain levels
- Create a naming convention and stick to it
- Avoid obscure abbreviations
- Avoid names that are difficult to spell

Naming for a Network Connected to the Internet

- Use registered domain names
- Do not use top-level domain names or names of commonly known products or companies
- Use only characters that are compliant with the Internet standard

Creating Subdomains

- The primary reason for creating subdomains is to delegate administrative authority for parts of the namespace
- You can create subdomains based on geographical locations or logical divisions within your company, or any way you want

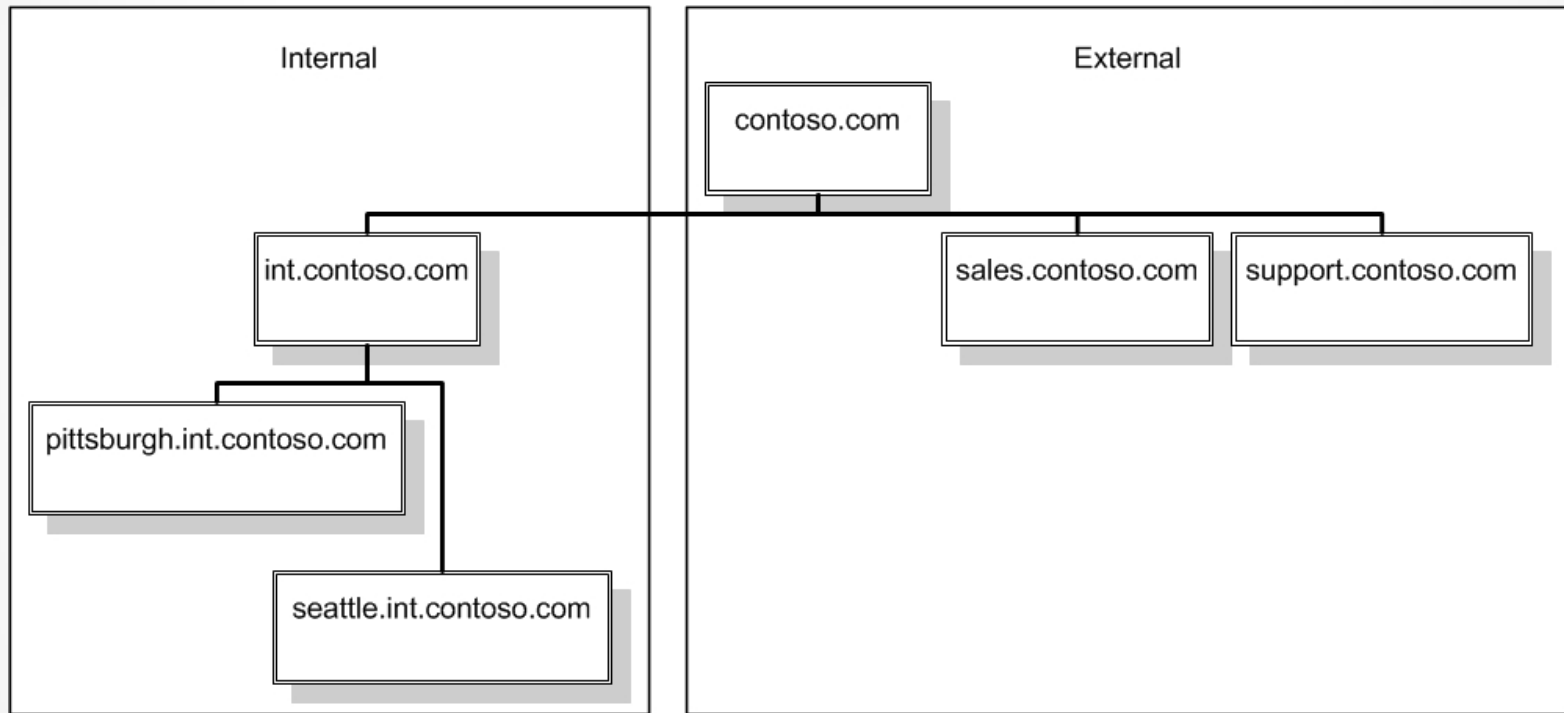
Combining Internal and External Domains

Use the same domain name internally and externally: A computer in the internal network could have the same DNS name as a computer on the external network. This duplication wreaks havoc with the name resolution process. Strongly discouraged.

Create separate and unrelated internal and external domains: By using different domain names for your internal and external networks, you eliminate the potential name resolution conflicts that come with using the same domain name for both networks.

Make the internal domain a subdomain of the external domain: Microsoft recommends combining internal and external networks by registering a single Internet domain name and using it for external resources, and then creating a subdomain beneath that domain name and using it for your internal network.

Combining Internal and External Domains



Internal and external domain names

Creating Host Names

- Create hosts the same way you create domains—devise a naming rule and then stick to it.
- In many cases, host-naming rules are based on users, geographical locations, or the function of the computer.

Creating Host Names — Best Practices

- Create easily remembered names
- Use unique names throughout the organization
- Do not use case to distinguish names
- Use only characters supported by all your DNS servers

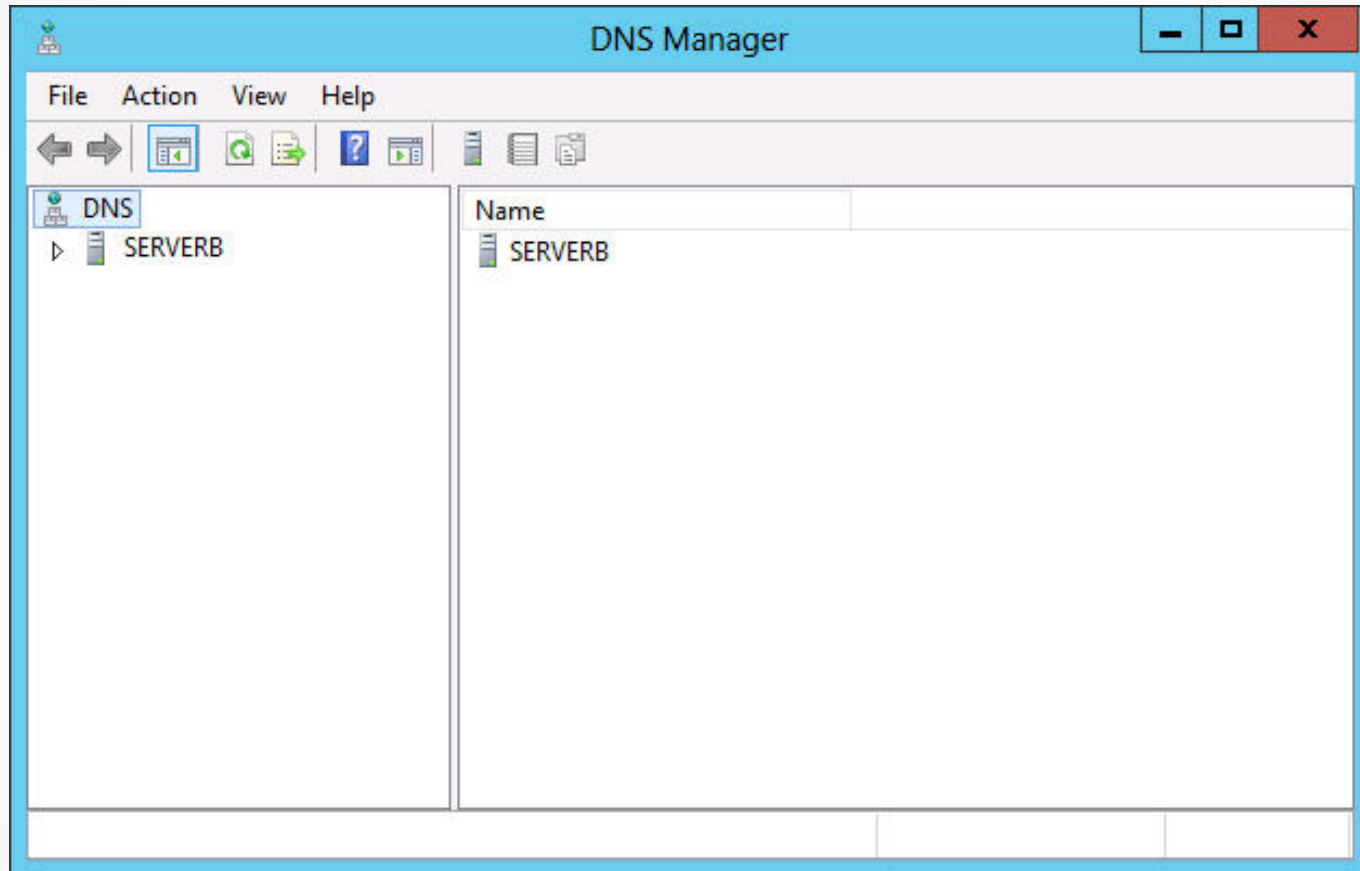
Deploying a DNS Server

Lesson 12: Deploying and Configuring the
DNS Service

Deploying a DNS Server

- Install the DNS Server role, using the Add Roles and Features Wizard in Server Manager.
- The server is ready to perform caching-only name resolution services for any clients that have access to it.
- Use the DNS Manager console to configure the DNS server's other capabilities.

Deploying a DNS Server

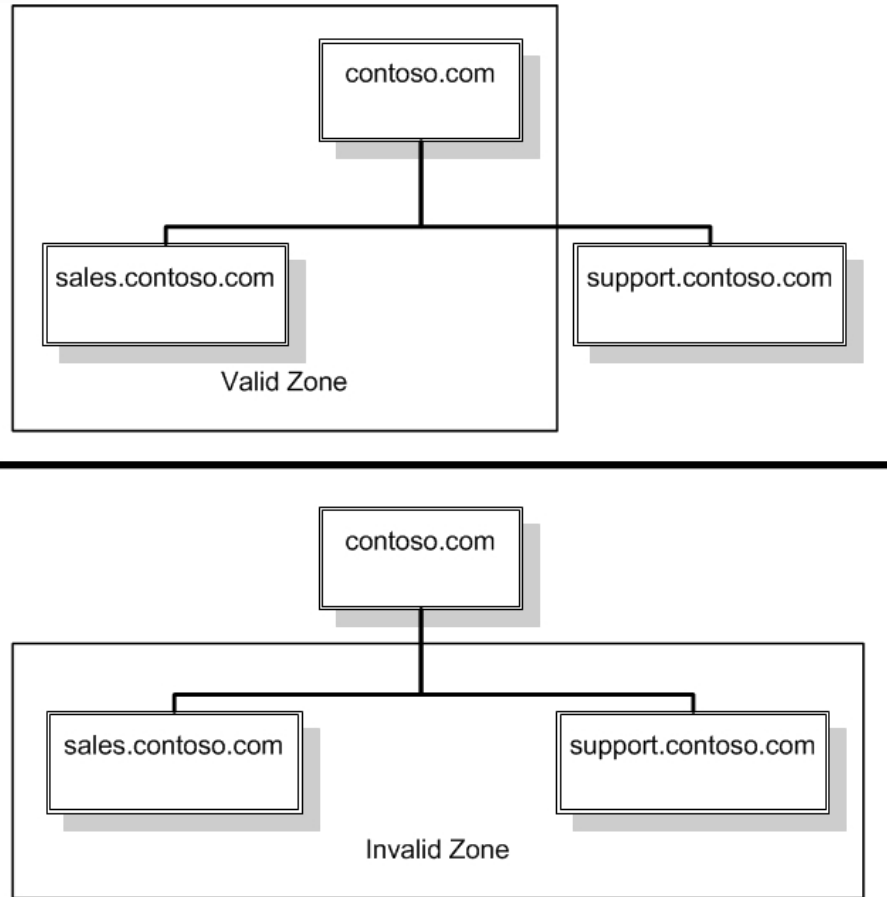


The DNS Manager console

Creating Zones

- A **zone** is an administrative entity you create on a DNS server to represent a discrete portion of the DNS namespace.
- Zones always consist of entire domains or subdomains.
- Usually, administrators create multiple zones on a server and then delegate most of them to other servers for hosting.
- Every zone consists of a zone database, which contains the resource records for the domains in that zone.

Creating Zones



Valid zones must consist of contiguous domains

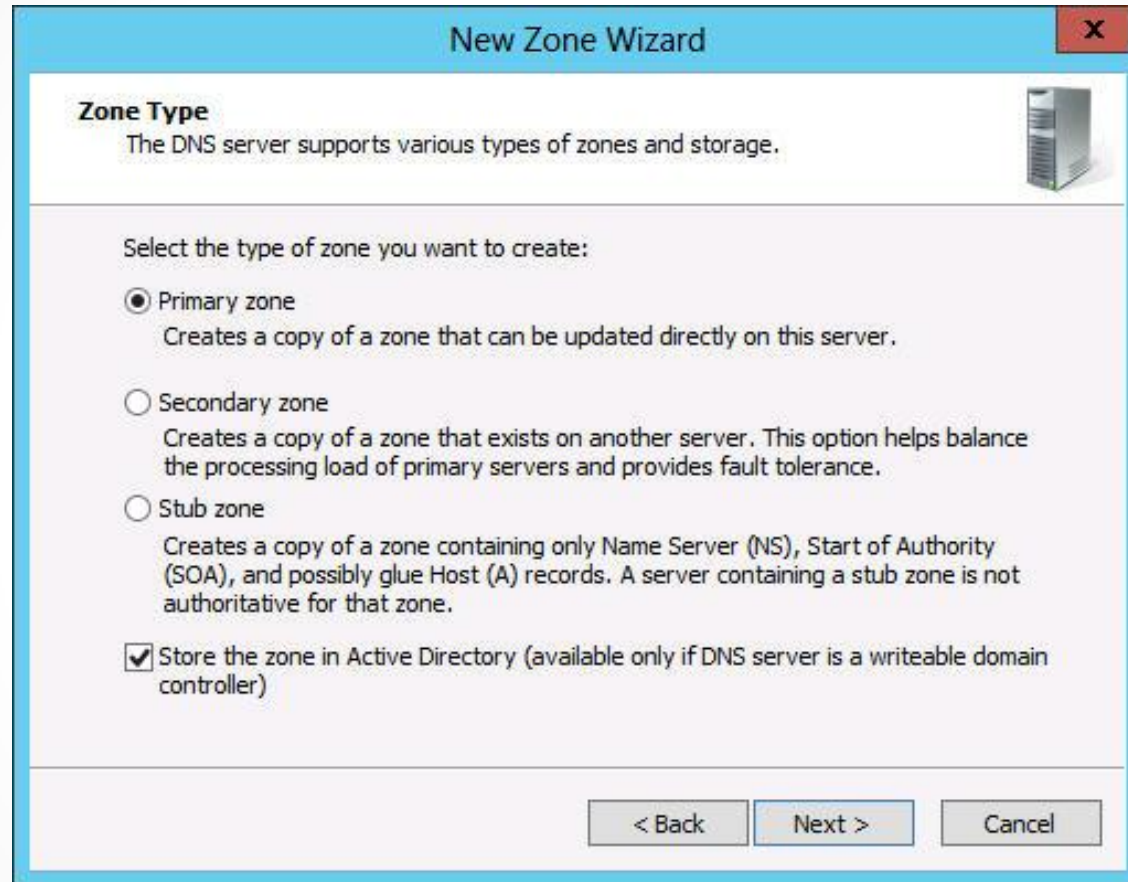
Zone Types

- **Primary zone:** Contains the master copy of the zone database, where administrators make all changes to the zone's resource records.
- **Secondary zone:** A duplicate of a primary zone on another server that contains a backup copy of the primary master zone database file, stored as an identical text file on the server's local drive.
- **Stub zone:** A copy of a primary zone that contains the key resource records that identify the authoritative servers for the zone. The stub zone forwards or refers requests.

Using Active Directory-Integrated Zones

- Storing the DNS database in Active Directory provides a number of advantages:
 - Ease of administration
 - Conservation of network bandwidth
 - Increased security
- The zone database is replicated automatically to other domain controllers, along with all other Active Directory data.

Create an Active Directory Zone



The Zone Type page of the New Zone Wizard

Create an Active Directory Zone



The screenshot shows a Windows dialog box titled "New Zone Wizard" with a close button (X) in the top right corner. The main heading is "Active Directory Zone Replication Scope" with a server icon to the right. Below the heading is the instruction: "You can select how you want DNS data replicated throughout your network." The main area contains the text "Select how you want zone data replicated:" followed by four radio button options, all with "adatum.local" as the domain name. The second option is selected. Below the last option is an empty text box with a dropdown arrow. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

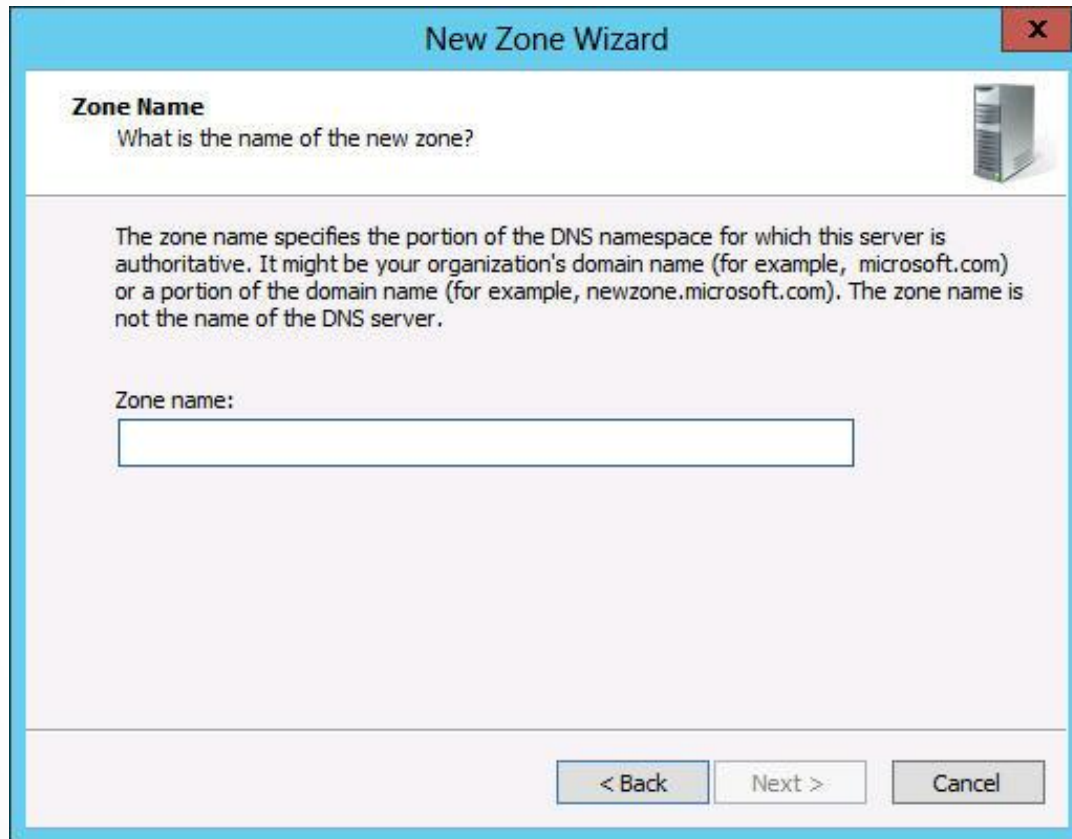
Select how you want zone data replicated:

- To all DNS servers running on domain controllers in this forest: adatum.local
- To all DNS servers running on domain controllers in this domain: adatum.local
- To all domain controllers in this domain (for Windows 2000 compatibility): adatum.local
- To all domain controllers specified in the scope of this directory partition:

< Back Next > Cancel

The Active Directory Zone Replication Scope page of the New Zone Wizard

Create an Active Directory Zone



The screenshot shows a window titled "New Zone Wizard" with a close button (X) in the top right corner. The main content area is titled "Zone Name" and contains the question "What is the name of the new zone?". To the right of this text is a small icon of a server rack. Below the question is a paragraph of explanatory text: "The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server." Underneath this text is a label "Zone name:" followed by a single-line text input field. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

The Zone Name page of the New Zone Wizard

Create an Active Directory Zone



The Dynamic Update page of the New Zone Wizard

Creating Resource Records

When you run your own DNS server, you create a resource record for each host name that you want to be accessible by the rest of the network.

Types of Resource Records (1)

The most important types of resource record used by DNS servers:

- **SOA (Start of Authority):** Indicates that the server is the best authoritative source for data concerning the zone. Each zone must have an SOA record, and only one SOA record can be in a zone.
- **NS (Name Server):** Identifies a DNS server functioning as an authority for the zone. Each DNS server in the zone (whether primary master or secondary) must be represented by an NS record.
- **A (Address):** Provides a name-to-address mapping that supplies an IPv4 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.
- **AAAA (Address):** Provides a name-to-address mapping that supplies an IPv6 address for a specific DNS name. This record type performs the primary function of the DNS, converting names to addresses.

Types of Resource Records (2)

- **PTR (Pointer):** Provides an address-to-name mapping that supplies a DNS name for a specific address in the *in-addr.arpa* domain. This is the functional opposite of an A record, used for reverse lookups only.
- **CNAME (Canonical Name):** Creates an alias that points to the *canonical* name (i.e., the “real” name) of a host identified by an A record. Used to provide alternative names by which systems can be identified.
- **MX (Mail Exchanger):** Identifies a system that will direct e-mail traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server.

Create an Address Resource Record

New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):
adatum.local.

IP address:

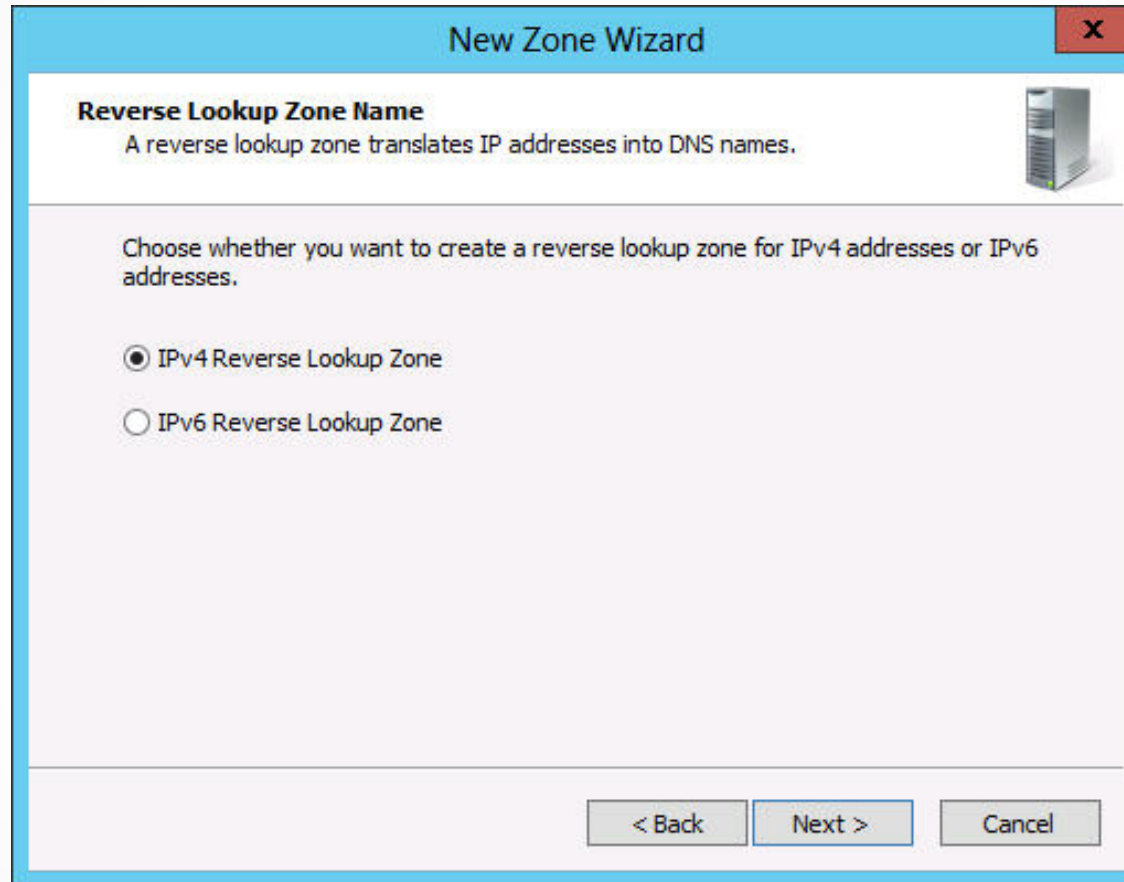
Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

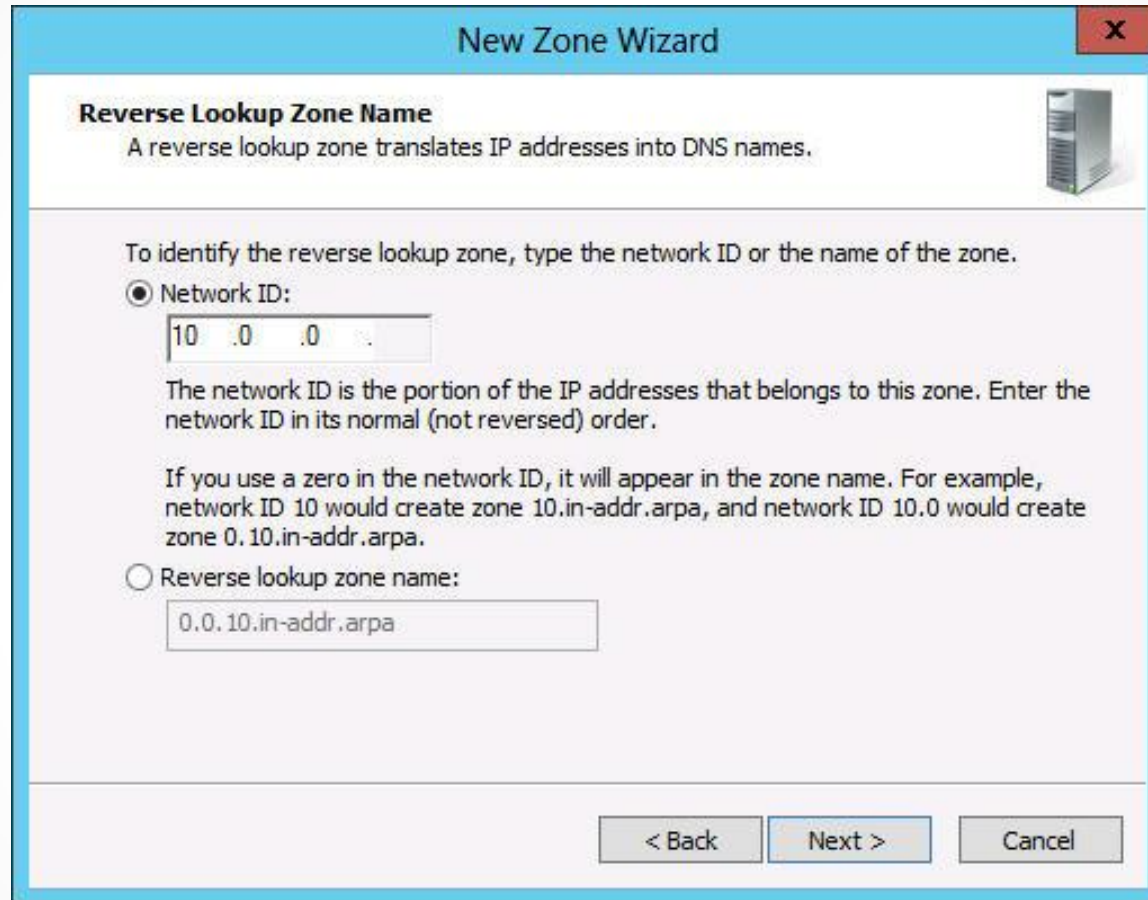
The New Host dialog box

Create an Address Resource Record



The Reverse Lookup Zone Name page in the New Zone Wizard

Create an Address Resource Record



New Zone Wizard [X]

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

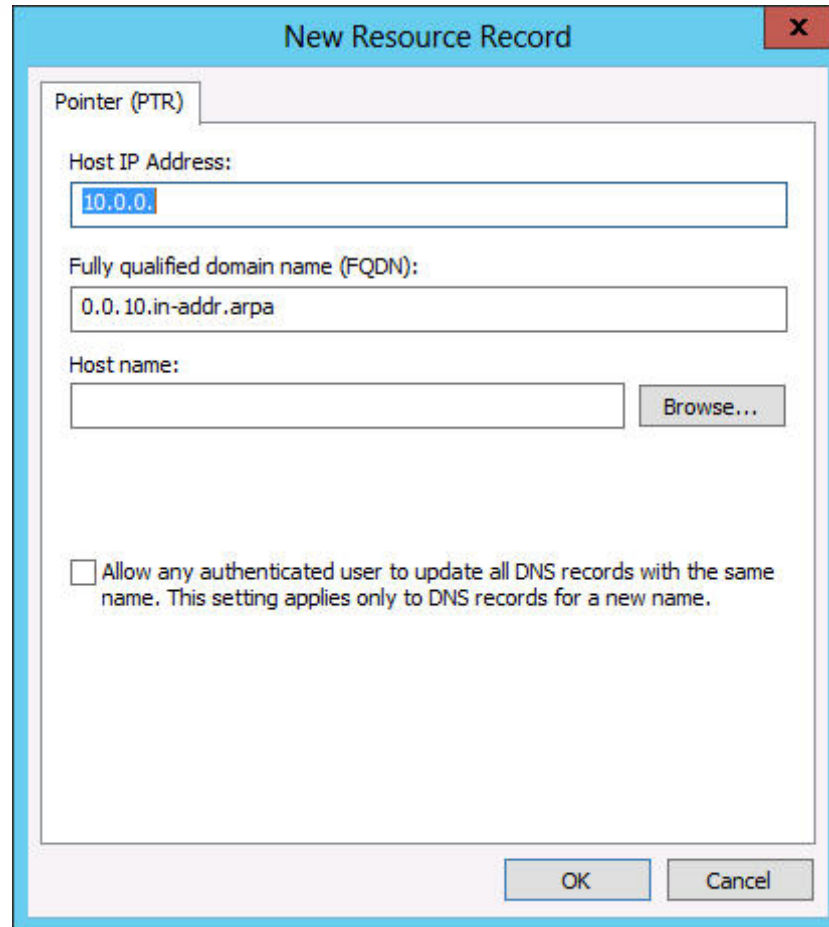
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

Reverse lookup zone name:

< Back Next > Cancel

The second Reverse Lookup Zone Name page in the New Zone Wizard

Create an Address Resource Record



The image shows a Windows-style dialog box titled "New Resource Record" with a close button (X) in the top right corner. The dialog is for creating a "Pointer (PTR)" record. It contains the following fields and controls:

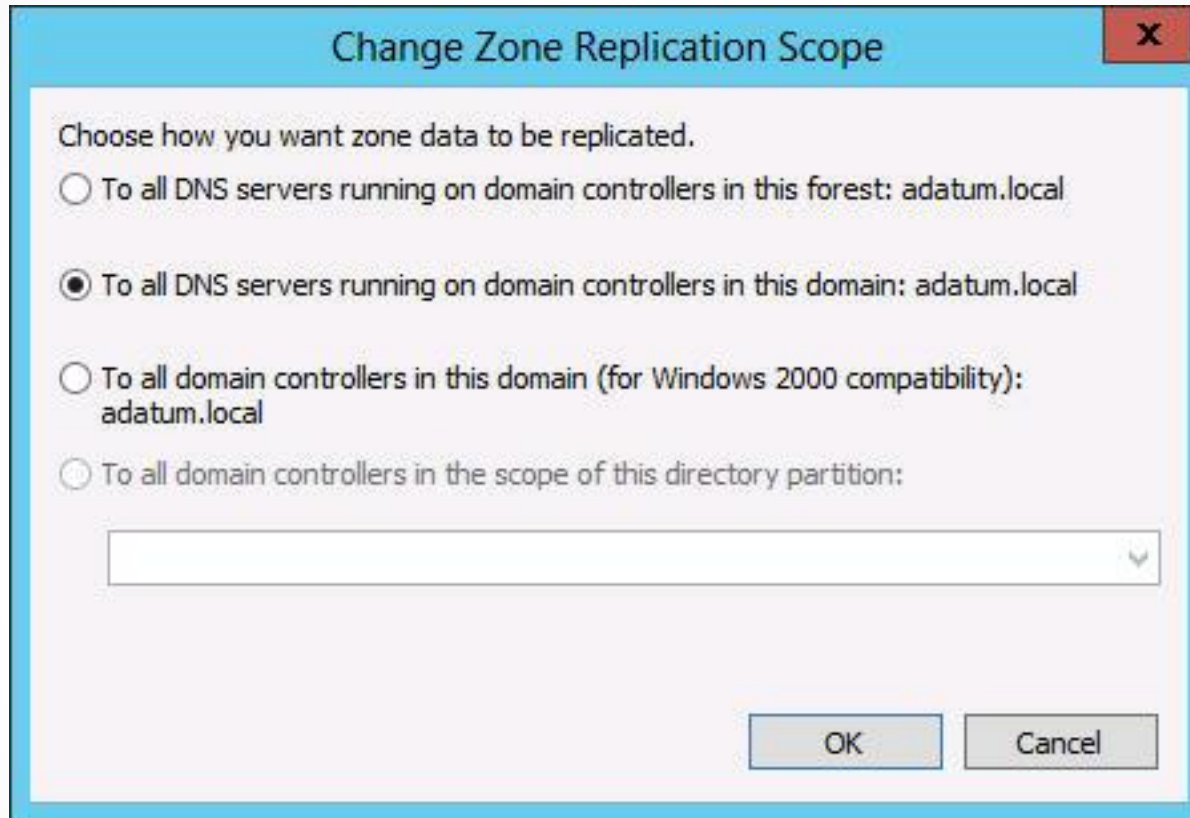
- Host IP Address:** A text box containing "10.0.0.". The text "10.0.0." is highlighted in blue.
- Fully qualified domain name (FQDN):** A text box containing "0.0.10.in-addr.arpa".
- Host name:** An empty text box next to a "Browse..." button.
- Checkboxes:** A checkbox labeled "Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name." is currently unchecked.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.

The New Resource Record dialog box

Configuring DNS Server Settings

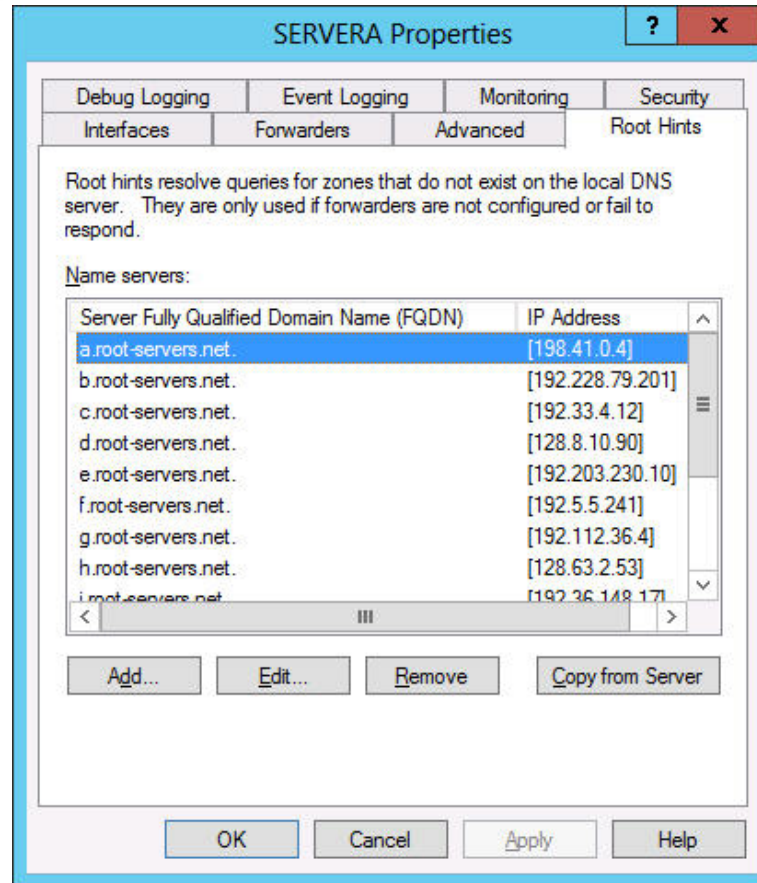
Once you have installed a DNS server and created zones and resource records on it, there are many settings you can alter to modify its behavior.

Configuring Active Directory DNS Replication



The Change Zone Replication Scope dialog box

Configuring Root Hints



The Root Hints tab on a DNS server's Properties sheet

Lesson Summary

- TCP/IP networks today use Domain Name System (DNS) servers to convert host names into IP addresses—a process called **name resolution**.
- The DNS consists of three elements: the **DNS name space**, which takes the form of a tree structure and consists of domains, containing resource records that contain host names, IP addresses, and other information; **name servers**, which are applications running on server computers that maintain information about the domain tree structure; and **resolvers**, which are client programs that generate DNS queries and send them to DNS servers for fulfillment.
- The hierarchical nature of the DNS namespace means any DNS server on the Internet can locate the authoritative source for any domain name, using a minimum number of queries. Domains at each level of the hierarchy are responsible for maintaining information about the domains at the next lower level.

Lesson Summary

- In a **recursive query**, the DNS server receiving the name resolution request takes full responsibility for resolving the name. In an **iterative query**, the server that receives the name resolution request immediately responds with the best information it possesses at the time.
- For Internet name resolution purposes, the only functions required of the DNS server are the ability to process incoming queries from resolvers and send its own queries to other DNS servers on the Internet. A DNS server that performs only these functions is known as a **caching-only server**, because it is not the authoritative source for any domain and hosts no resource records of its own.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.