Department of Information Technology

Lesson 6:Deploying and Configuring the DNS Service

Server Management

Zina Yaaqub

Overview

- Deploy and Configure DNS Service
- Understanding the DNS Architecture
- Designing a DNS Deployment
- Deploying a DNS Server

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.

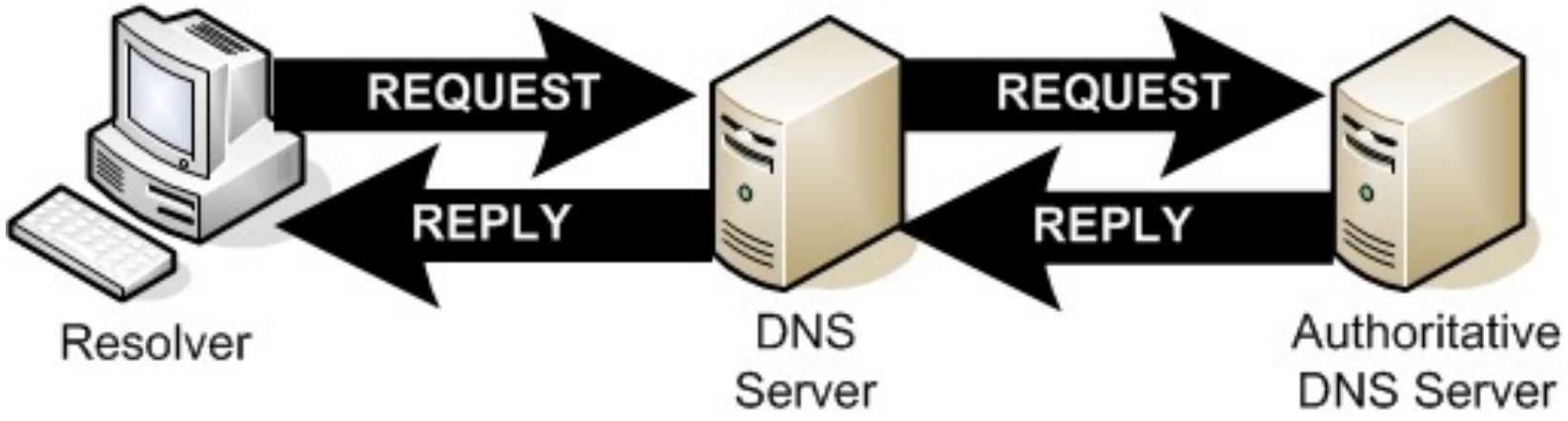
Name Servers

- 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

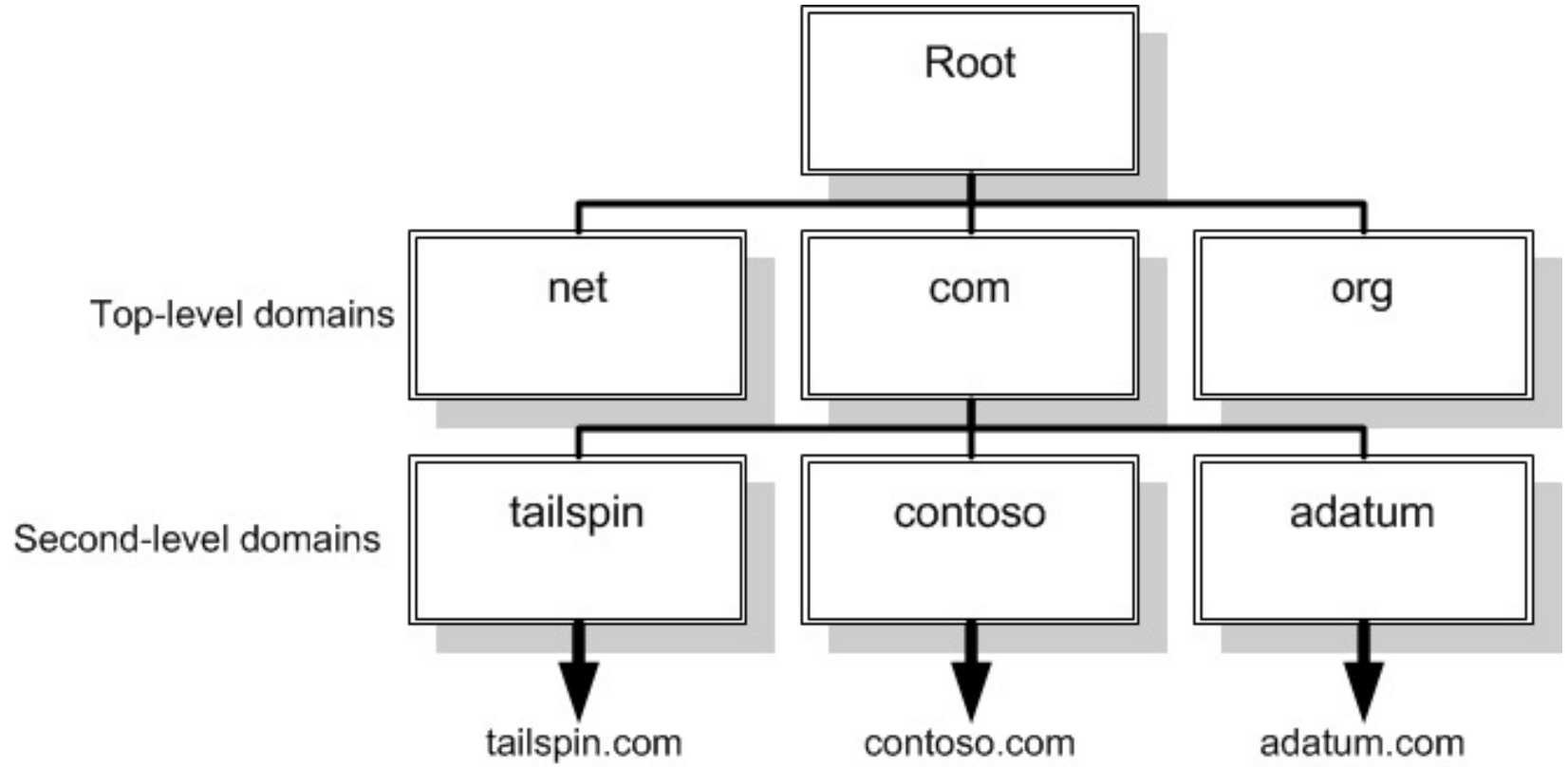
- A **resolver** is a client program that generates DNS queries and sends them to a DNS server for fulfillment.
- A resolver has direct access to at least one DNS server and can also process referrals to direct its queries to other servers when necessary.

Creating a DNS Standard



DNS servers relay requests and replies to other DNS servers

DNS Naming



The DNS domain hierarchy

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)**:

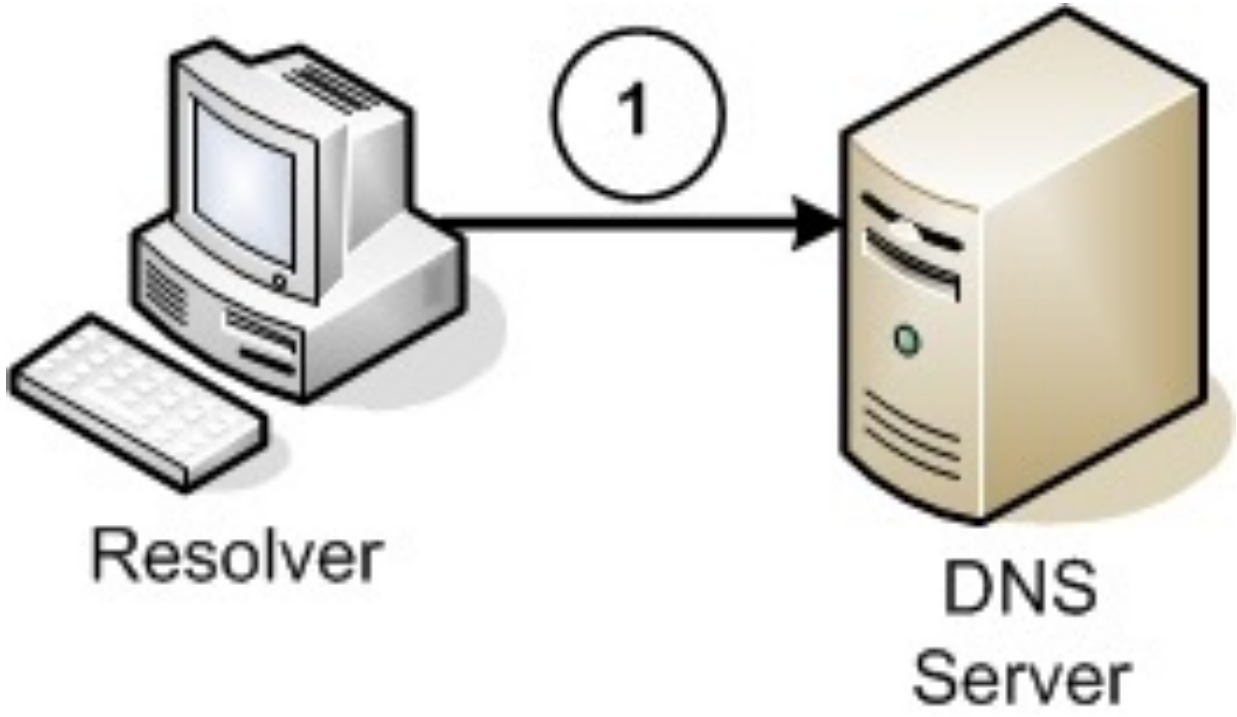
- **fr** for France
- **de** for Deutschland (Germany)
- **us** for the United States
- **ca** for Canada

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

DNS Communications

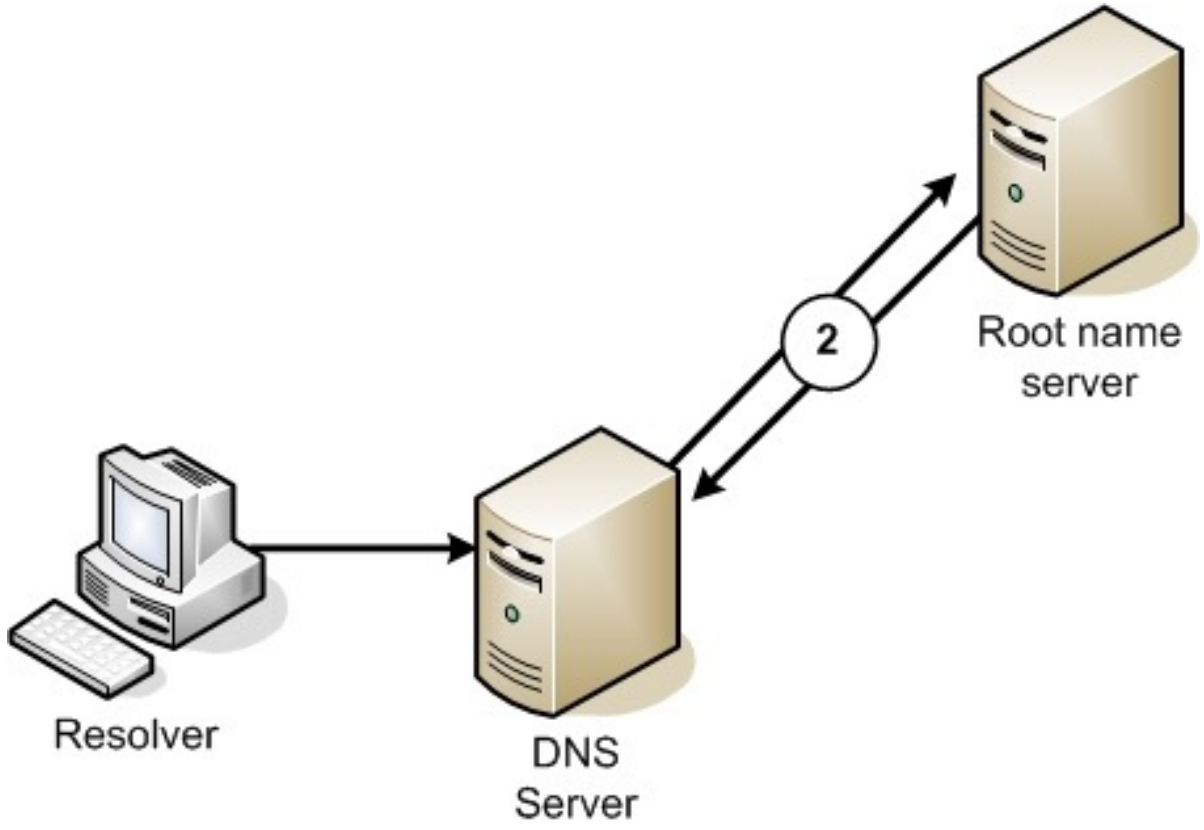
- Type a URL containing a DNS name (**www.microsoft.com**) into the browser's Address box and press Enter.
- You will see a message that says something like "**Finding Site: www.microsoft.com**."
- Then, a few seconds later, you will see a message that says "**Connecting to**," followed by an IP address.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

DNS Communications



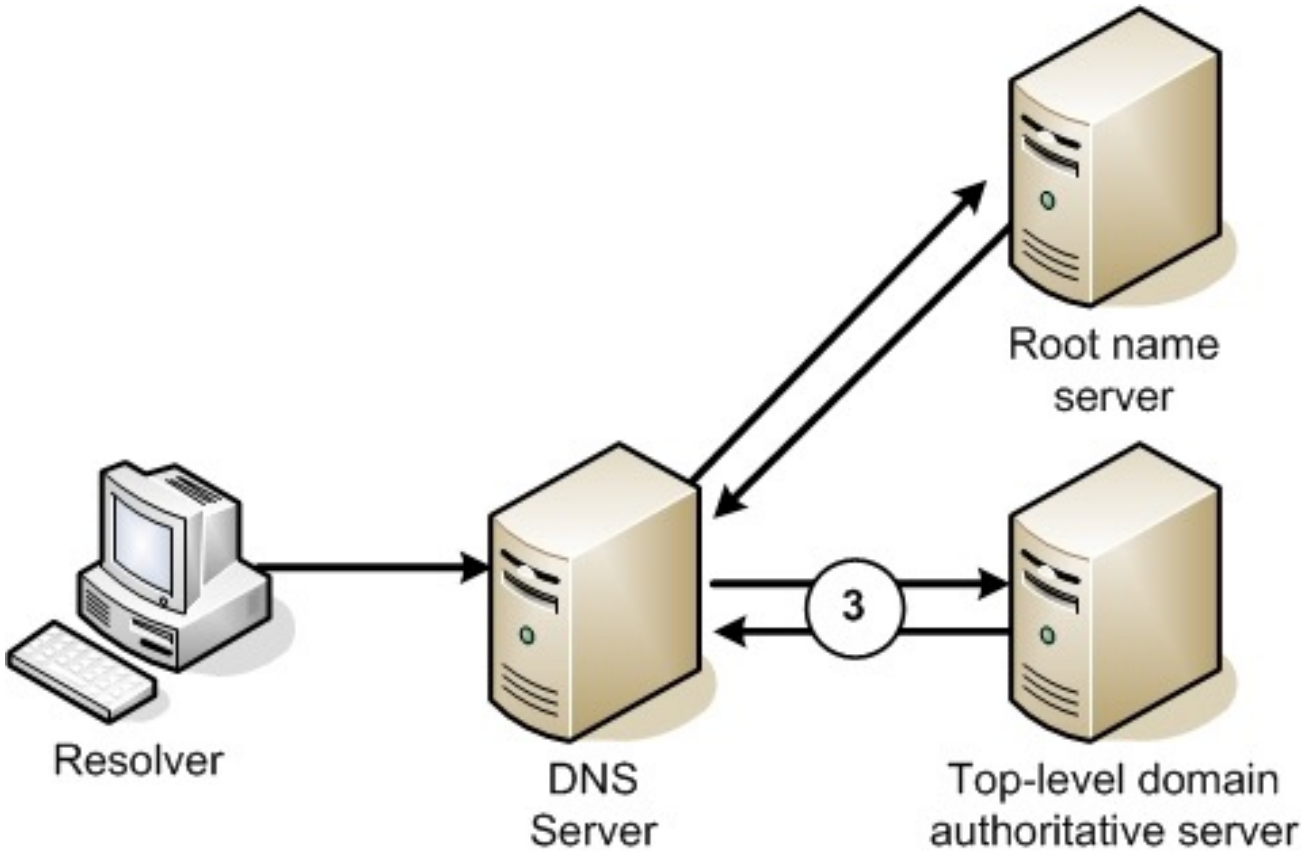
A DNS client sends a name resolution request to its designated DNS server

DNS Communications



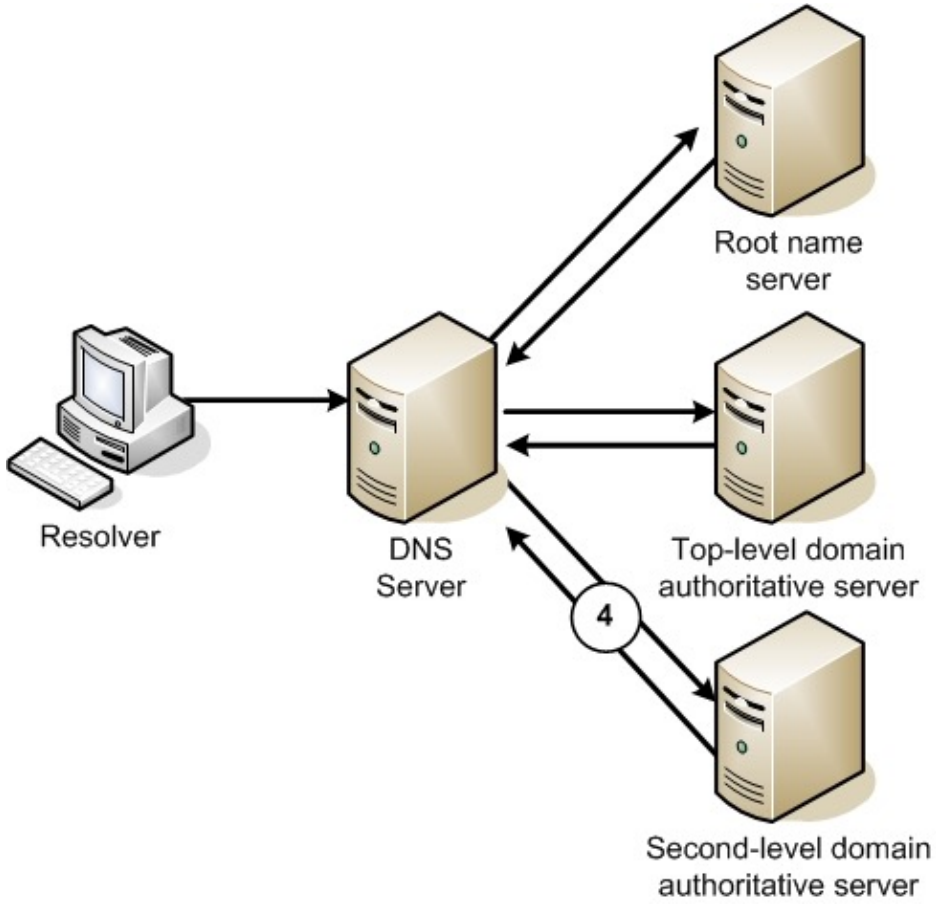
The client's DNS server forwards an iterative query to a root name server

DNS Communications



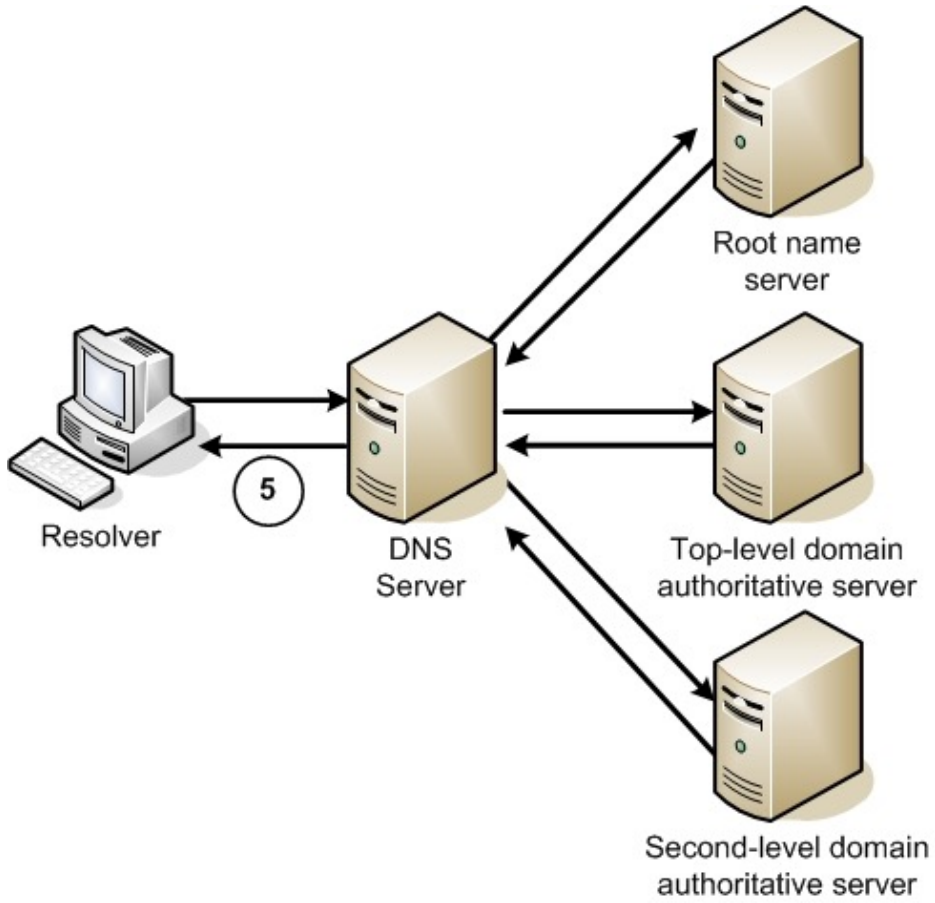
The client's DNS server forwards an iterative query to a top-level domain server

DNS Communications



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

DNS Communications

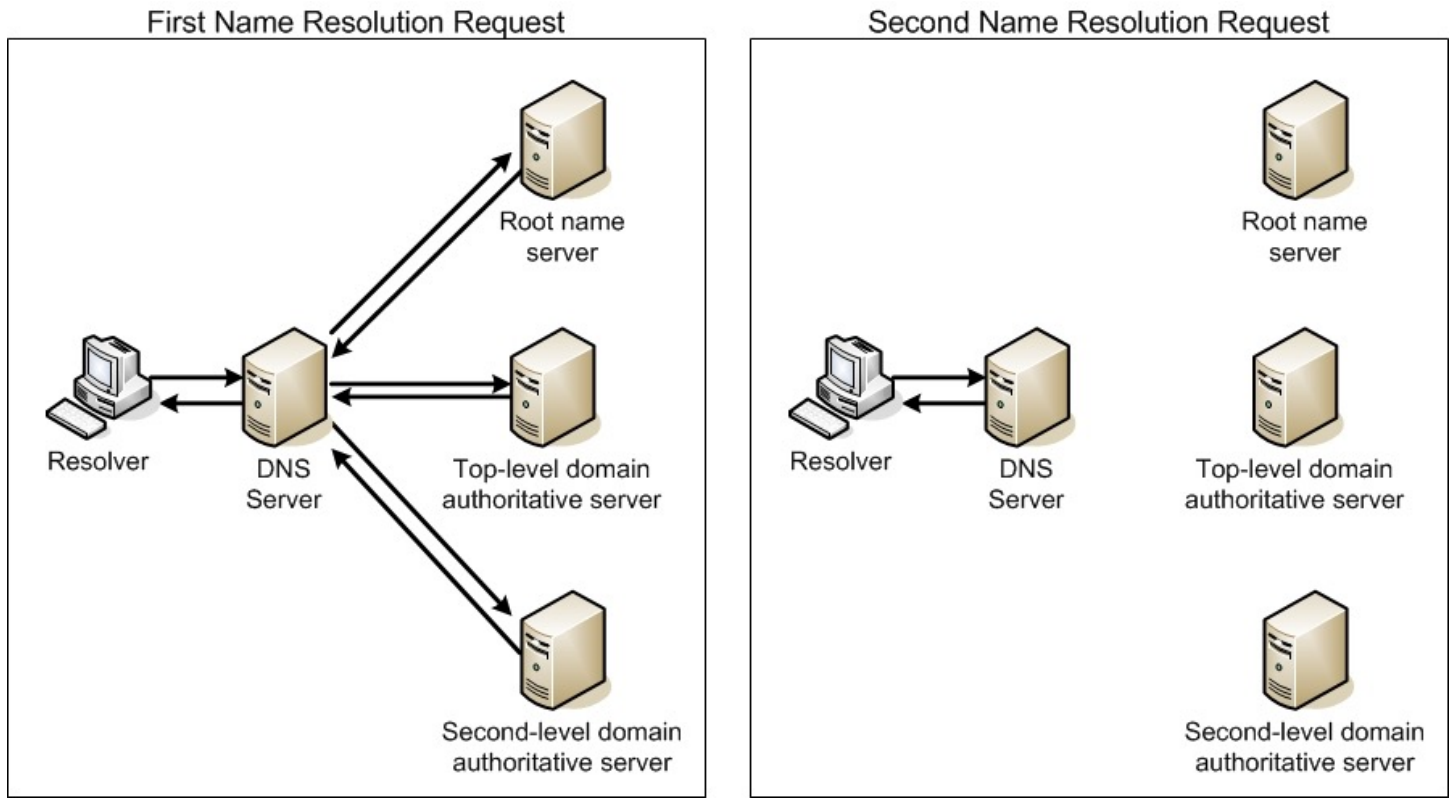


The client's DNS server returns the IP address supplied by the authoritative server to the client

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

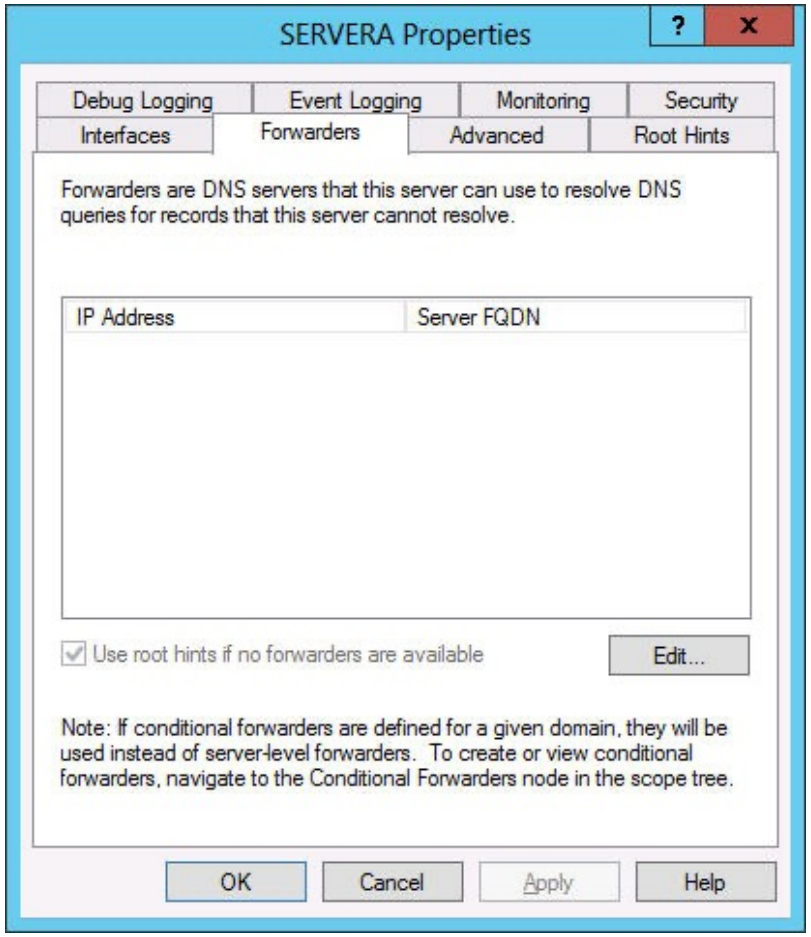
Negative Caching

- **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.

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

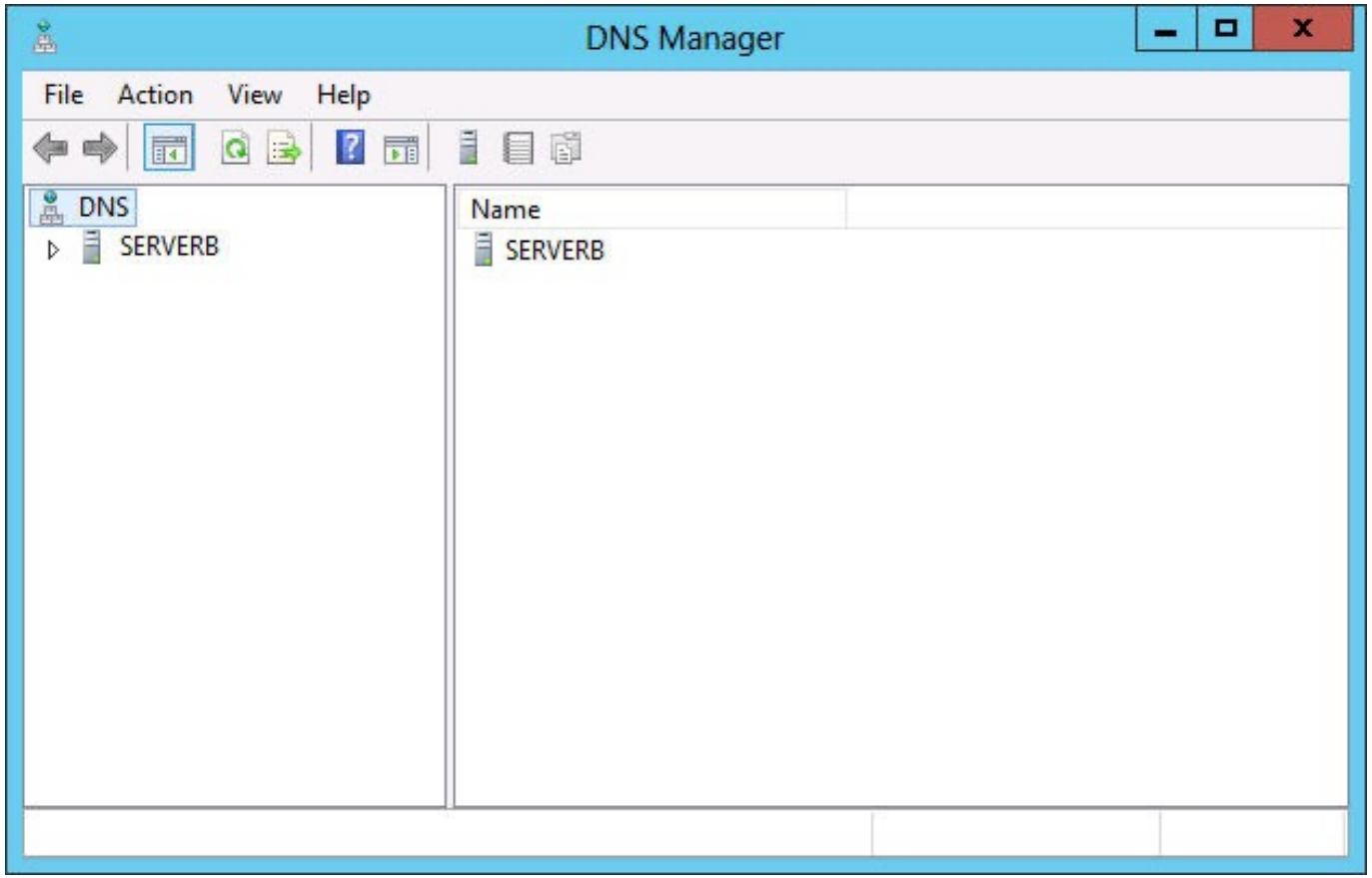
Reverse Name Resolution

- **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.

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

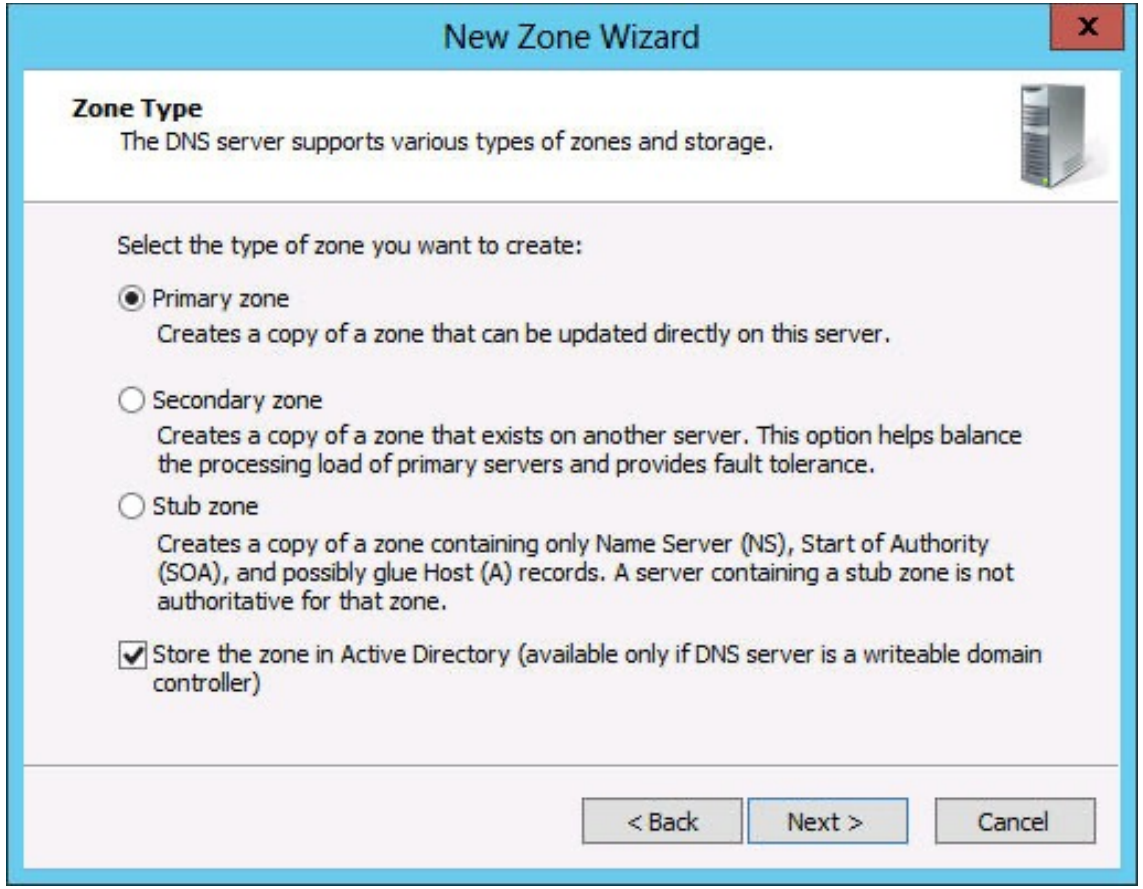
Creating Zones

- 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.

Zone Types

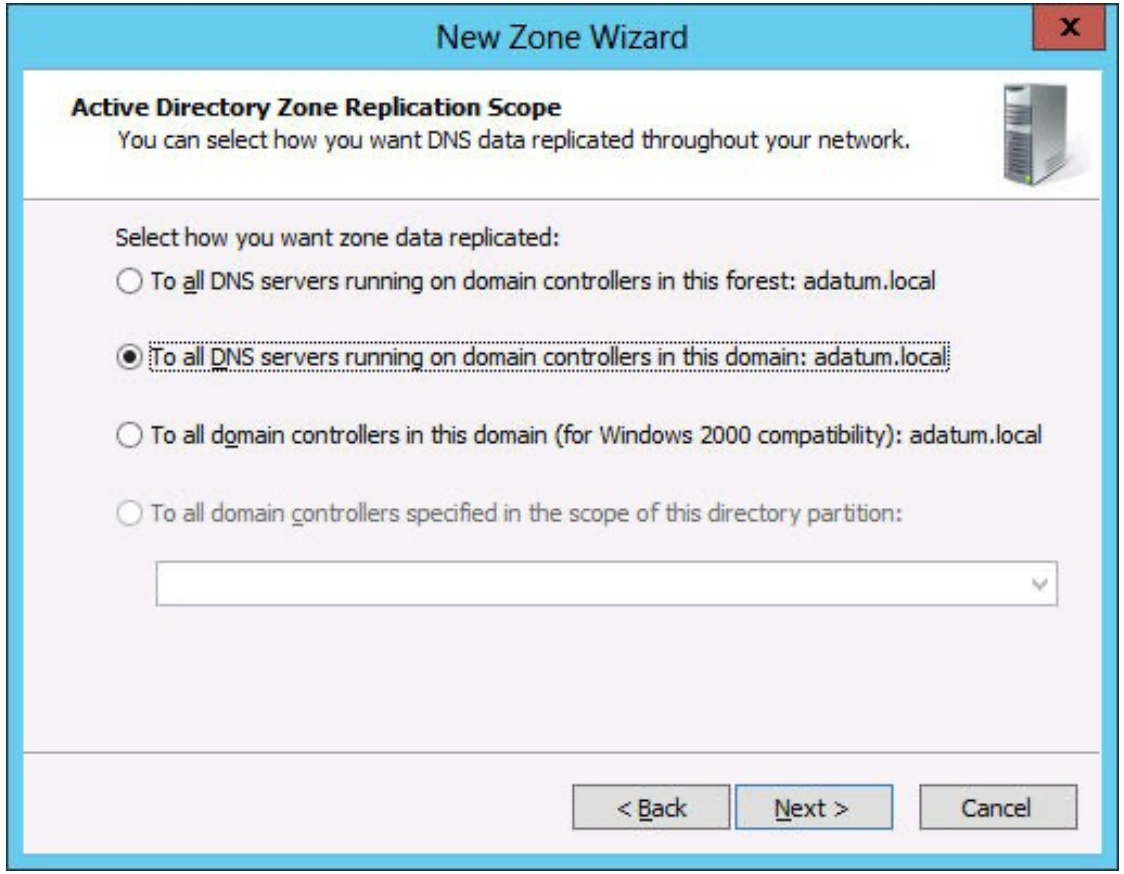
- **Primary zone:** Contains the master copy of the zone database, where administrators make all changes to the zone's resource records.
- **Secondary zone:** A duplicate of a primary zone on another server that contains a backup copy of the primary master zone database file, stored as an identical text 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.

Create an Active Directory Zone



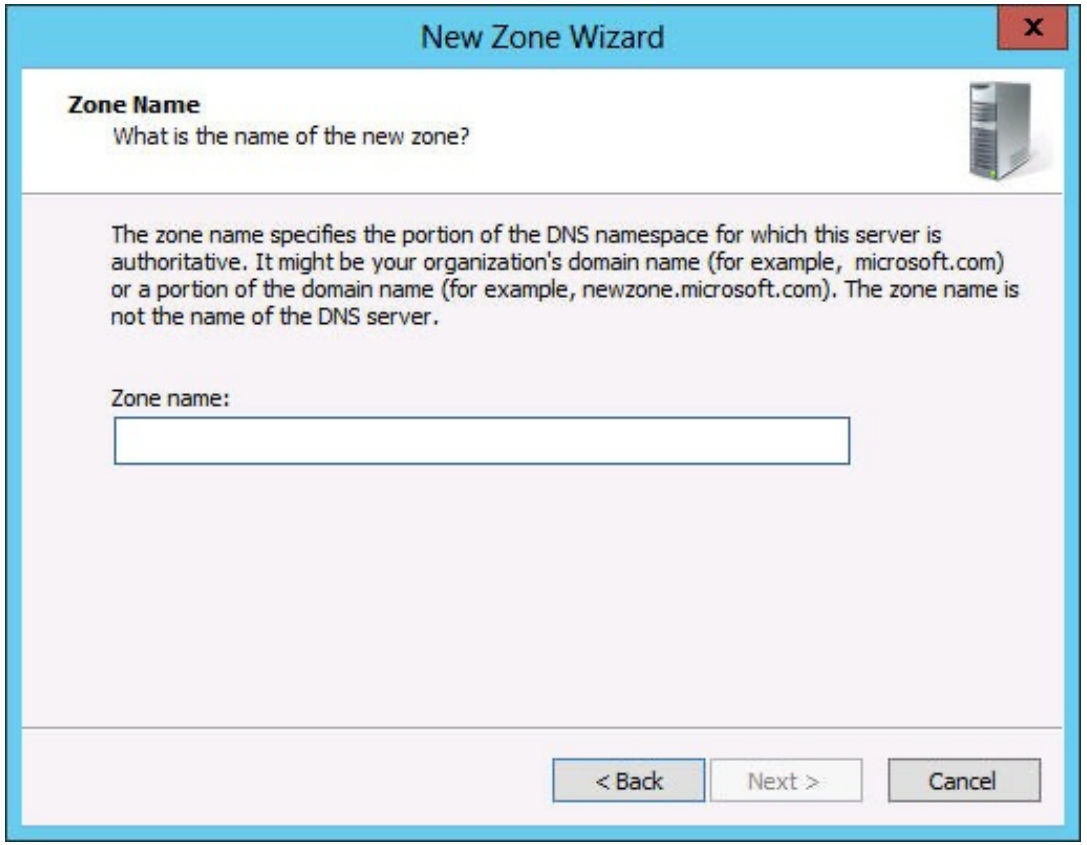
The Zone Type page of the New Zone Wizard

Create an Active Directory Zone



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

Create an Active Directory Zone



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)

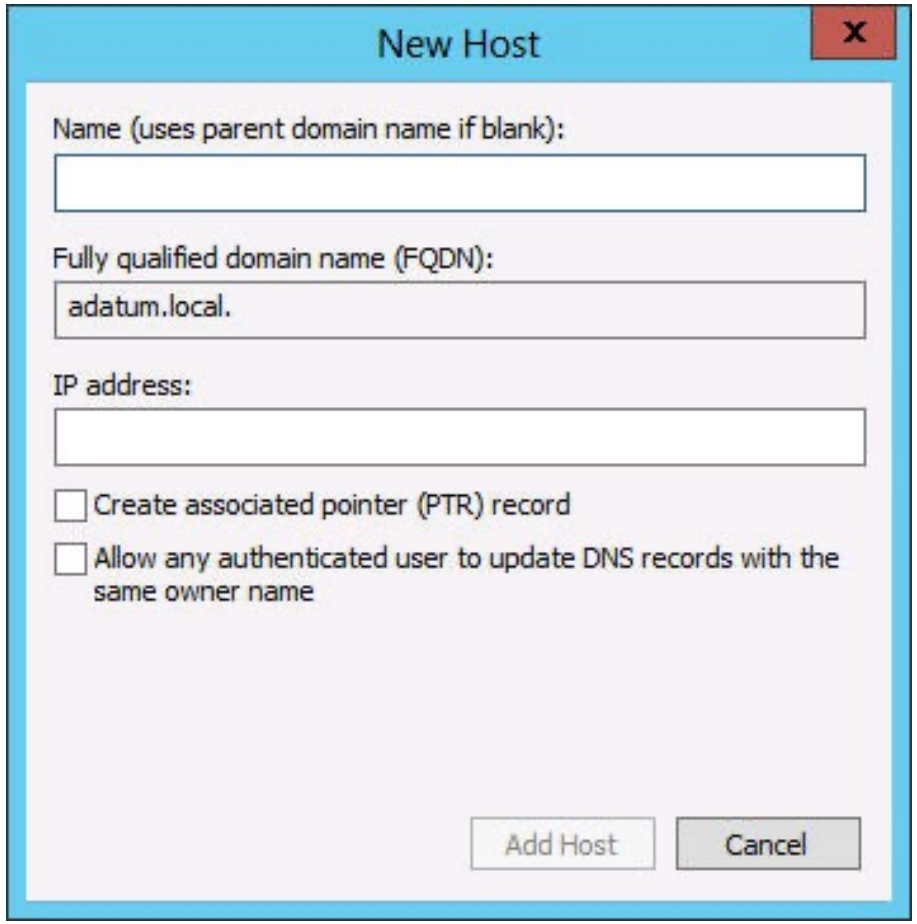
The most important types of resource record used by DNS servers:

- **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)

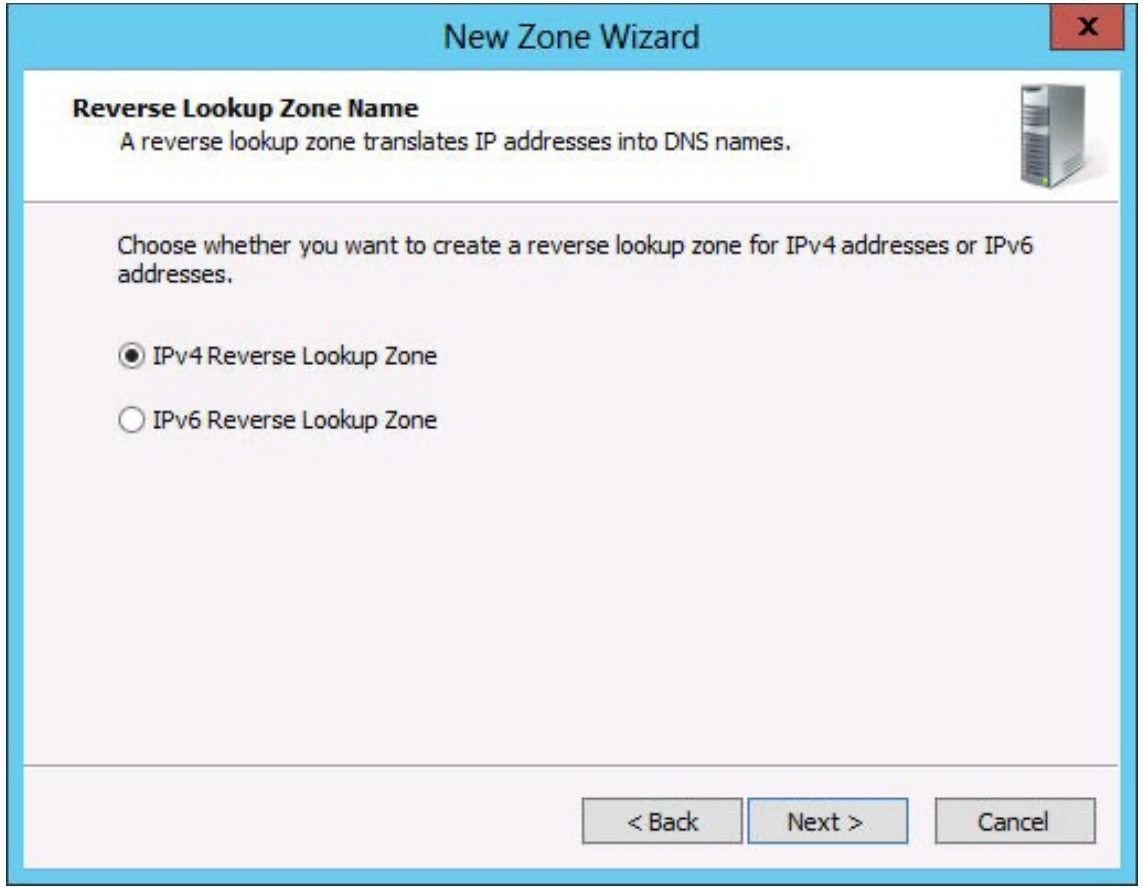
- **PTR (Pointer):** Provides an address-to-name mapping that supplies a DNS name for a specific address in the *in-addr.arpa* domain. This is the functional opposite of an A record, used for reverse lookups only.
- **CNAME (Canonical Name):** Creates an alias that points to the *canonical* name (i.e., 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



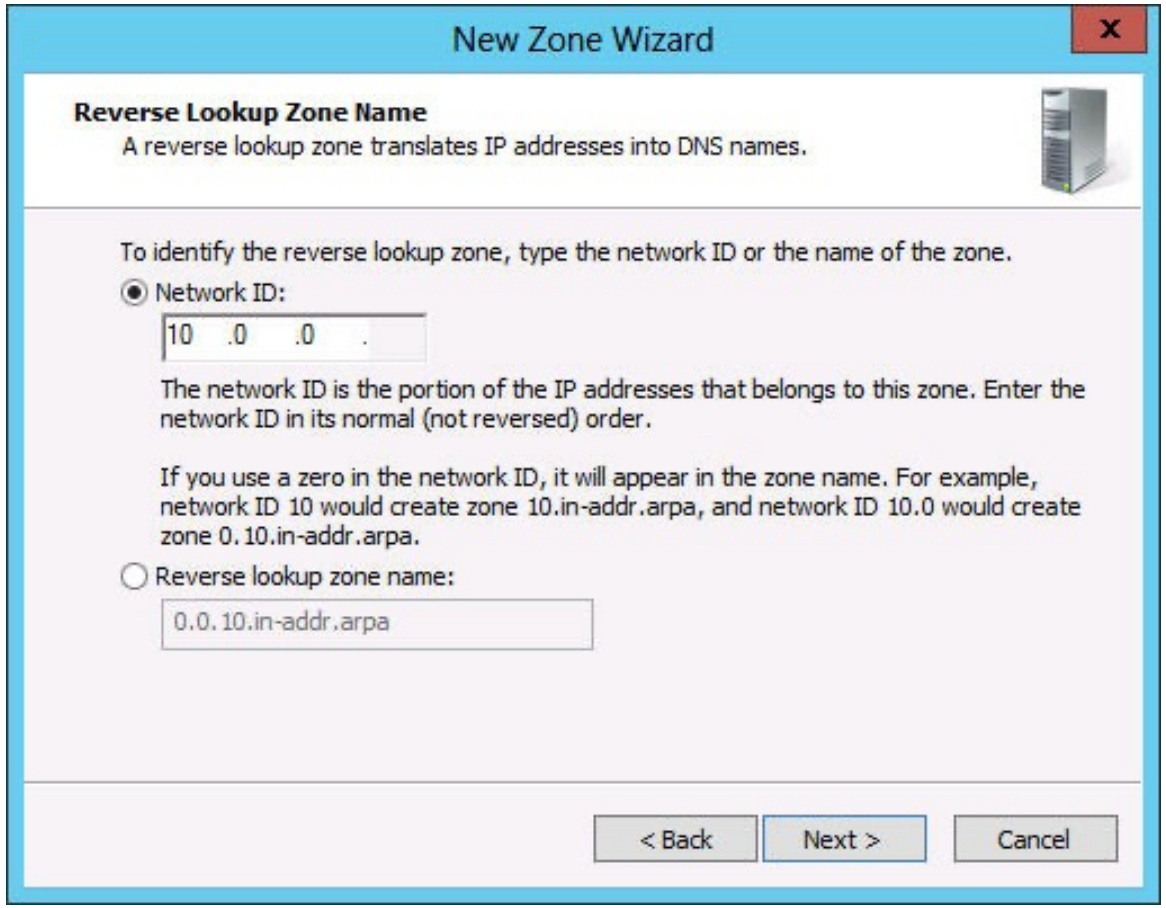
The New Host dialog box

Create an Address Resource Record



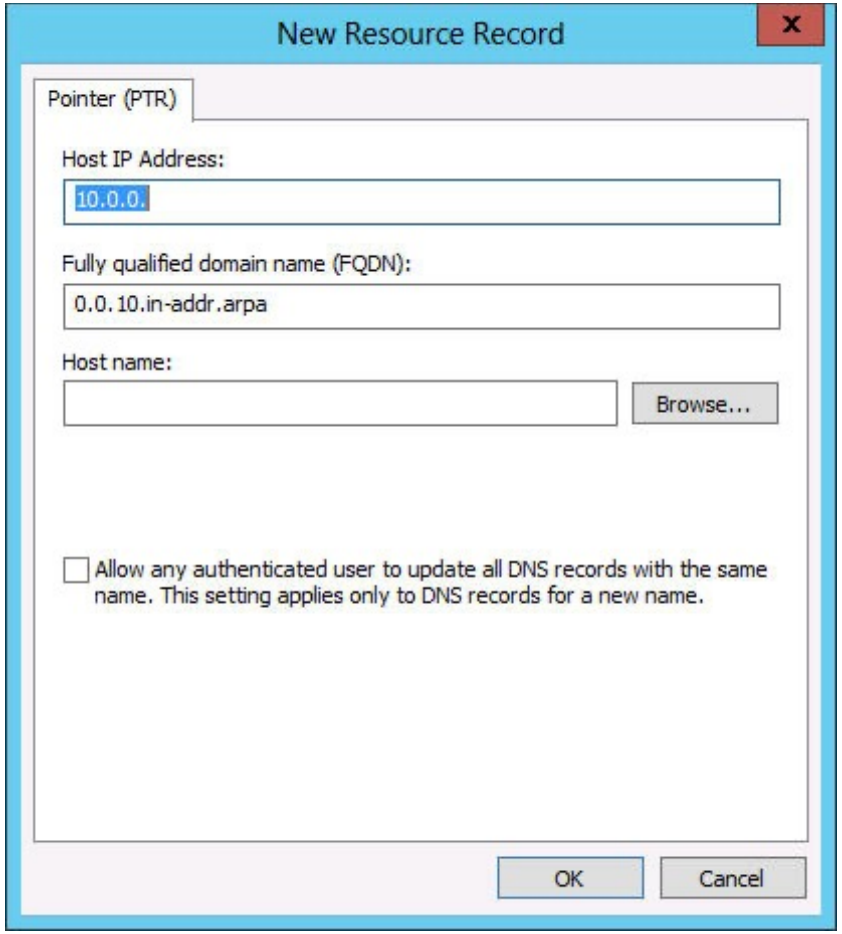
The Reverse Lookup Zone Name page in the New Zone Wizard

Create an Address Resource Record



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

Create an Address Resource Record



The New Resource Record dialog box

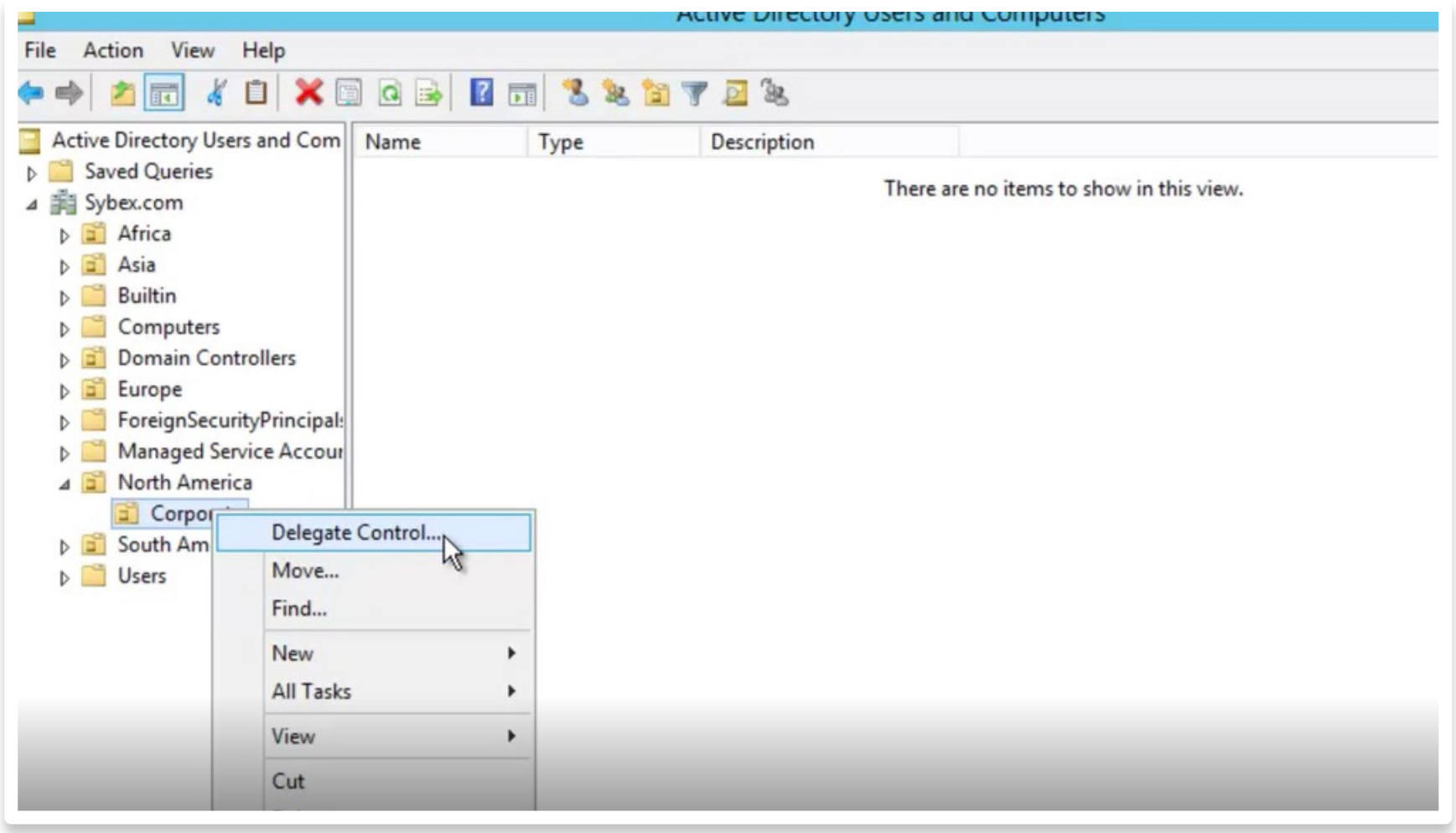
Delegation of Control

Delegation of control - a person with higher security privileges assigns authority to a person of lesser security privileges to perform certain tasks

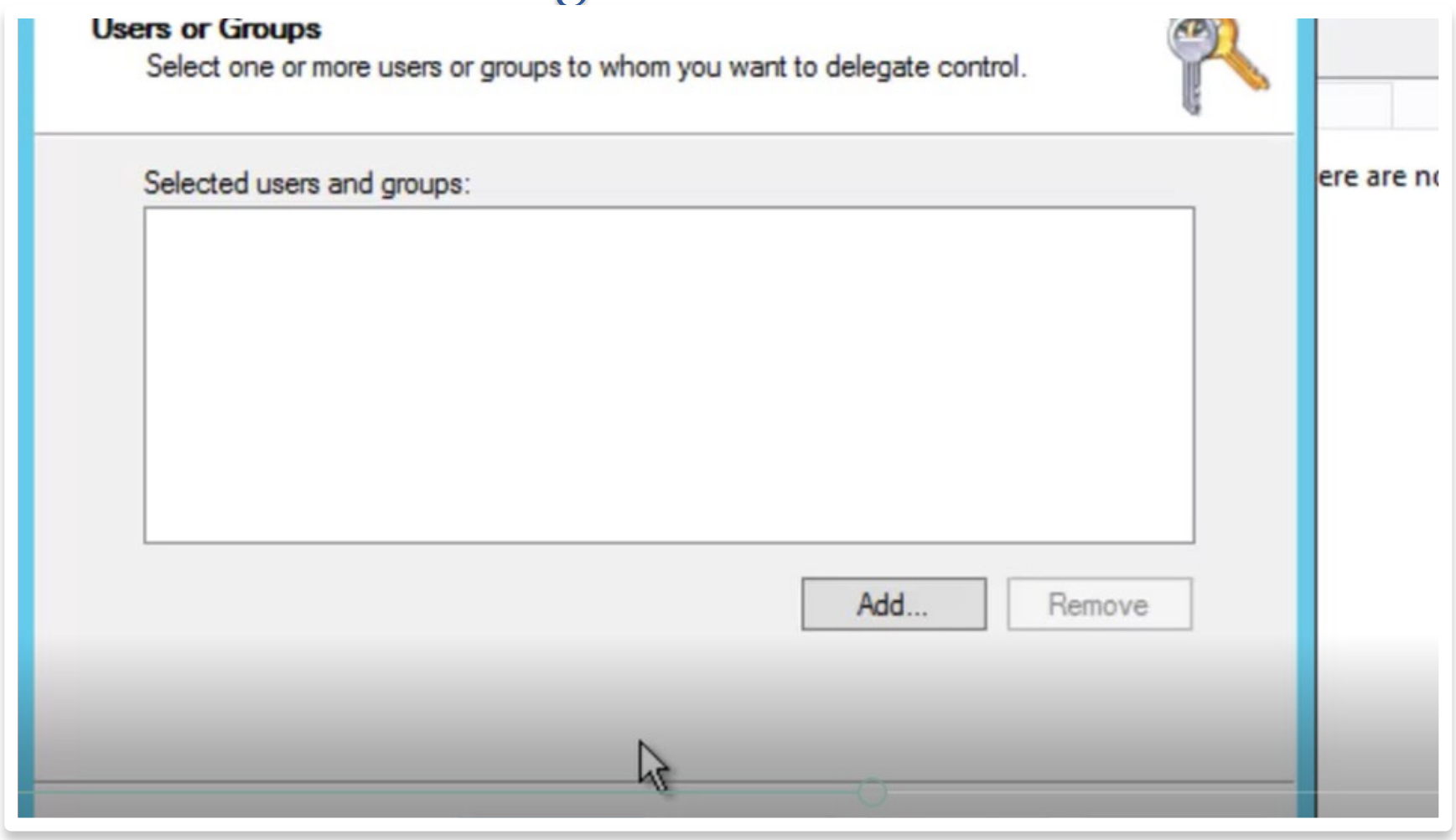
Commonly delegated tasks include

- Create, delete, and manager user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete, and manage groups
- Modify the membership of a group
- Manage group policy links
- Generate Resultant Set of Policy (Planning)
- Generate Resultant Set of Policy (Logging)

Delegation of Control

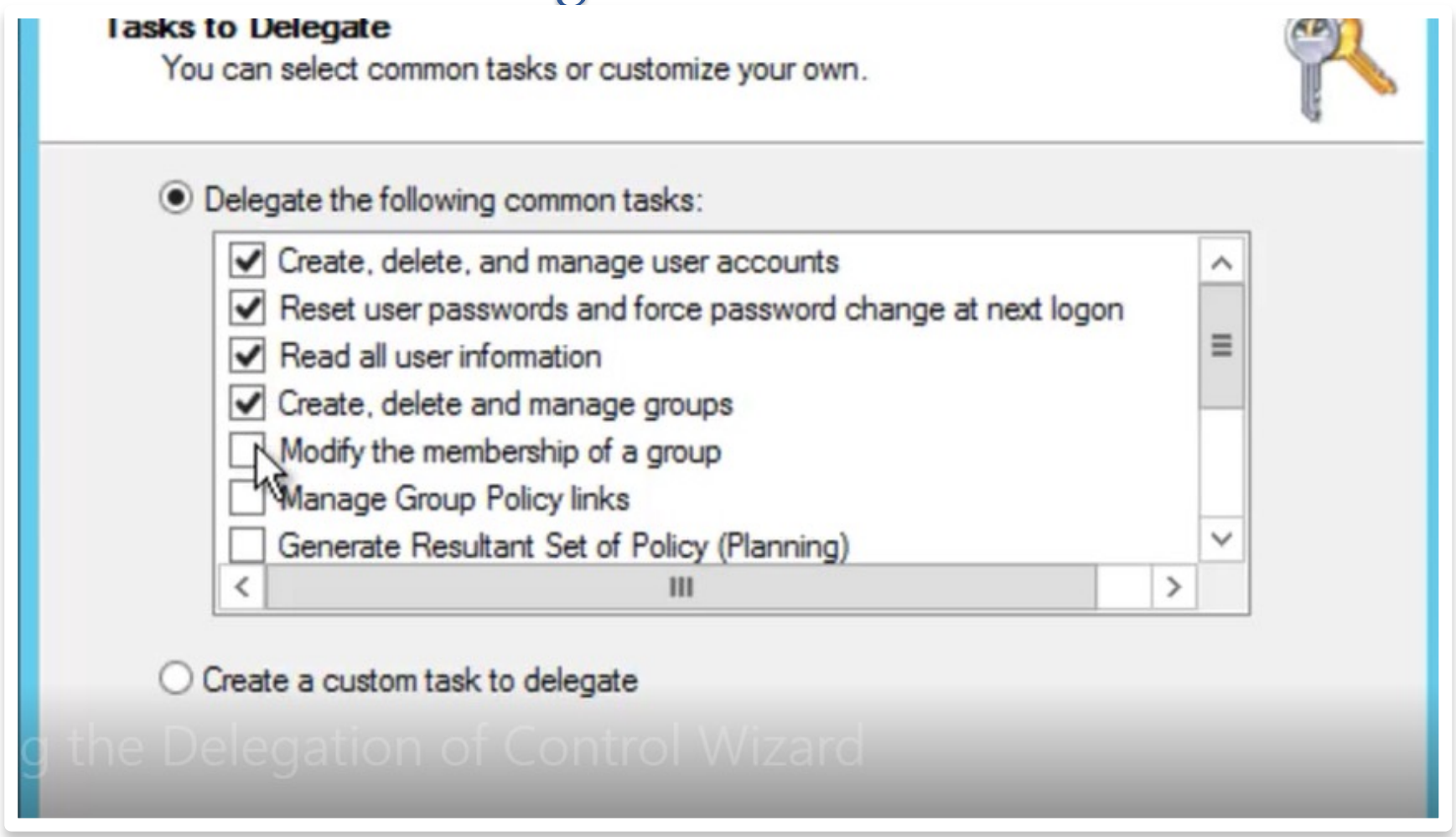


Delegation of Control



Delegation of Control

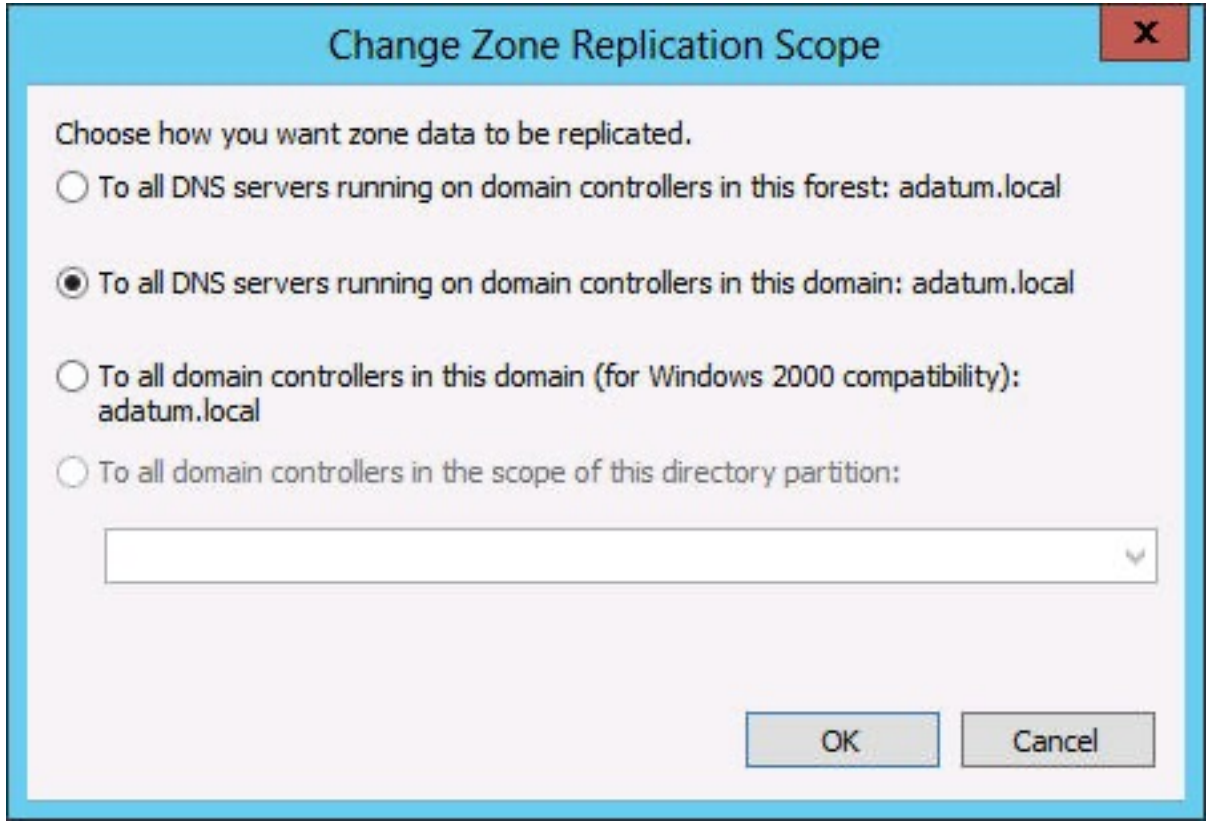
Delegation of Control



Configuring DNS Server Settings

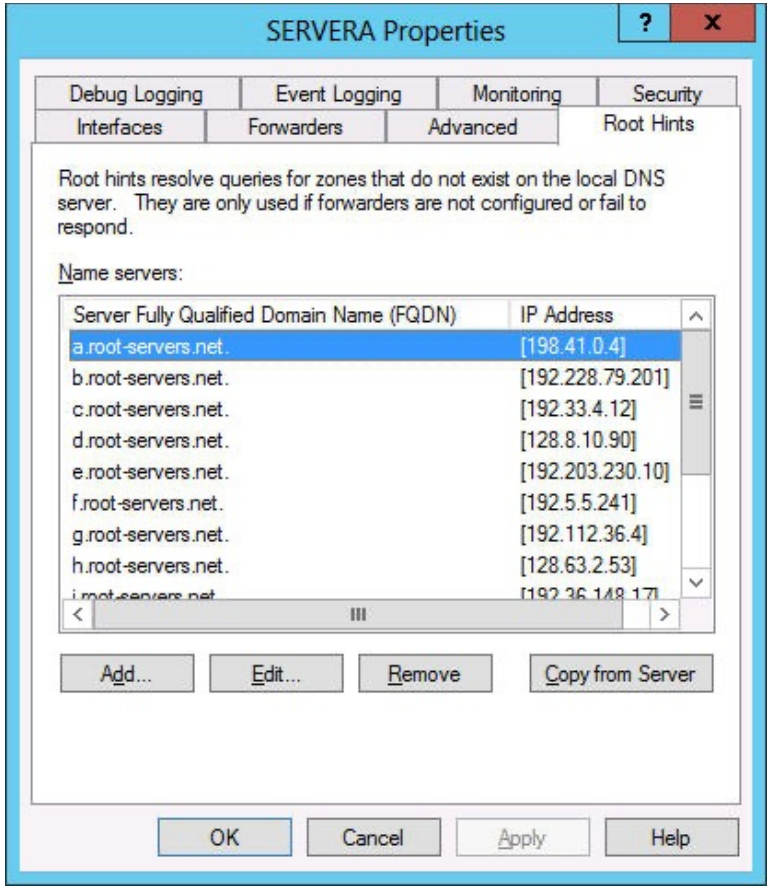
Once you have installed a DNS server and created zones and resource records on it, there are many settings you can alter to modify its behavior.

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

Deploying and Configuring the DHCP Service

Overview

- Deploy and Configure Dynamic Host Configuration Protocol (DHCP) Service
- Understanding DHCP
- Designing a DHCP Infrastructure
- Deploying a DHCP Server
- Using PXE

Understanding DHCP

The **Dynamic Host Configuration Protocol (DHCP)** service:

- Automatically configures the IP address and other TCP/IP settings on network computers by assigning addresses from a pool (called a **scope**) and reclaiming them when they are no longer in use.
- Saves time.
- Prevents configuration errors.

Understanding DHCP

DHCP consists of three components:

- **DHCP server application**: Responds to client requests for TCP/IP configuration settings.
- **DHCP client**: Issues requests to servers and applies the TCP/IP configuration settings it receives to the local computer.
- **DHCP communications protocol**: Defines the formats and sequences of the messages exchanged by DHCP clients and servers.

Understanding DHCP

Three different IP address allocation methods:

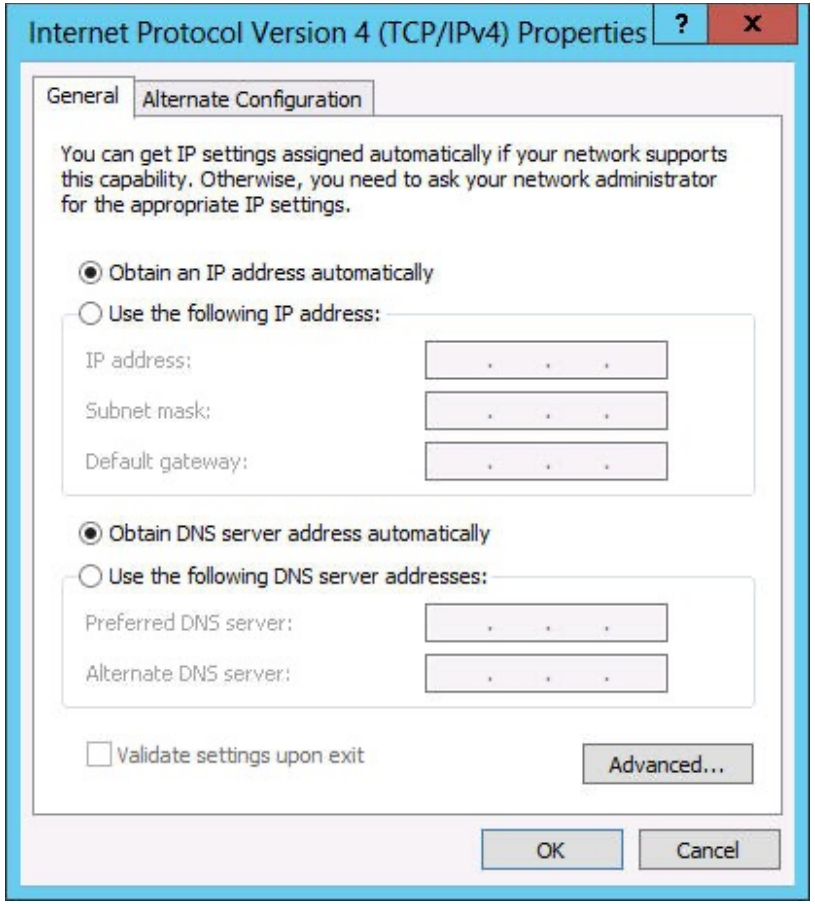
- **Dynamic allocation:** The DHCP server assigns an IP address to a client computer from a scope, for a specified length of time. DHCP servers only lease addresses to clients with this method.
- **Automatic allocation:** The DHCP server permanently assigns an IP address to a client computer from a scope. It is essentially dynamic allocation with an indefinite lease.
- **Manual allocation:** The DHCP server permanently assigns a specific IP address to a specific computer on the network. It is called a reservation. You use manually allocated addresses for computers that must have the same IP address at all times.

DHCP Options

There are many other TCP/IP parameters that can be configured by DHCP besides the IP address:

- Magic cookie
- Option format
- DHCP Message Type option
- Pad option
- Option Overload option
- Vendor-Specific Information option
- End option

DHCP Communications



The Internet Protocol Version 4 (TCP/IPv4) Properties sheet

Regulating DHCP Network Traffic

Several factors can effect network traffic and you can make configuration choices that will change the amount of traffic generated by DHCP:

- Place DHCP servers close to the clients.
- Adjust the lease duration so there are fewer renewals.
- Make the lease duration unlimited.

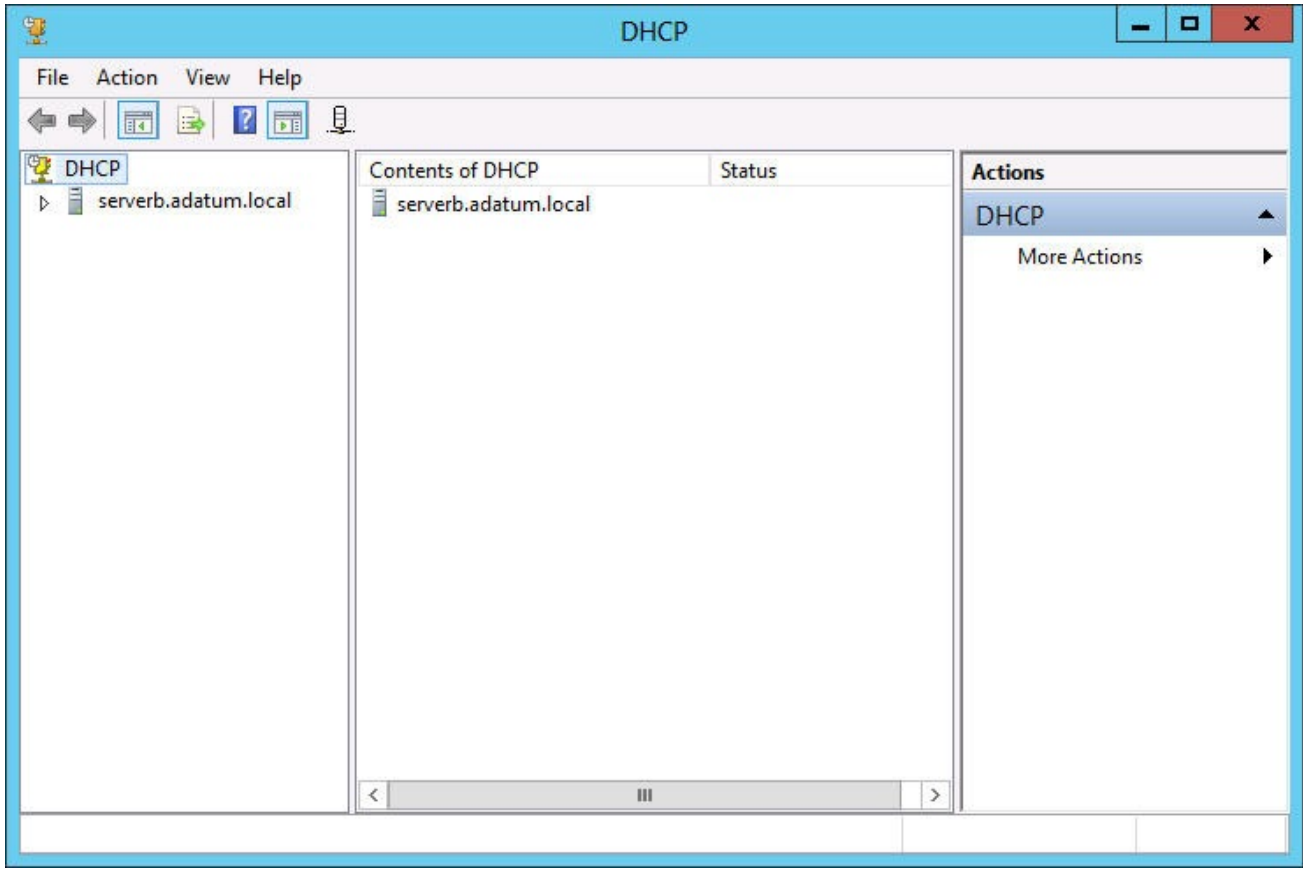
Deploying a DHCP Server

- The DHCP Server service is packaged as a role in Windows Server .
- Install the role, through the Add Roles and Features Wizard in Server Manager.
- DHCP servers operate independently, so you must install the service and configure scopes on every computer that will function as a DHCP server.

Creating a Scope

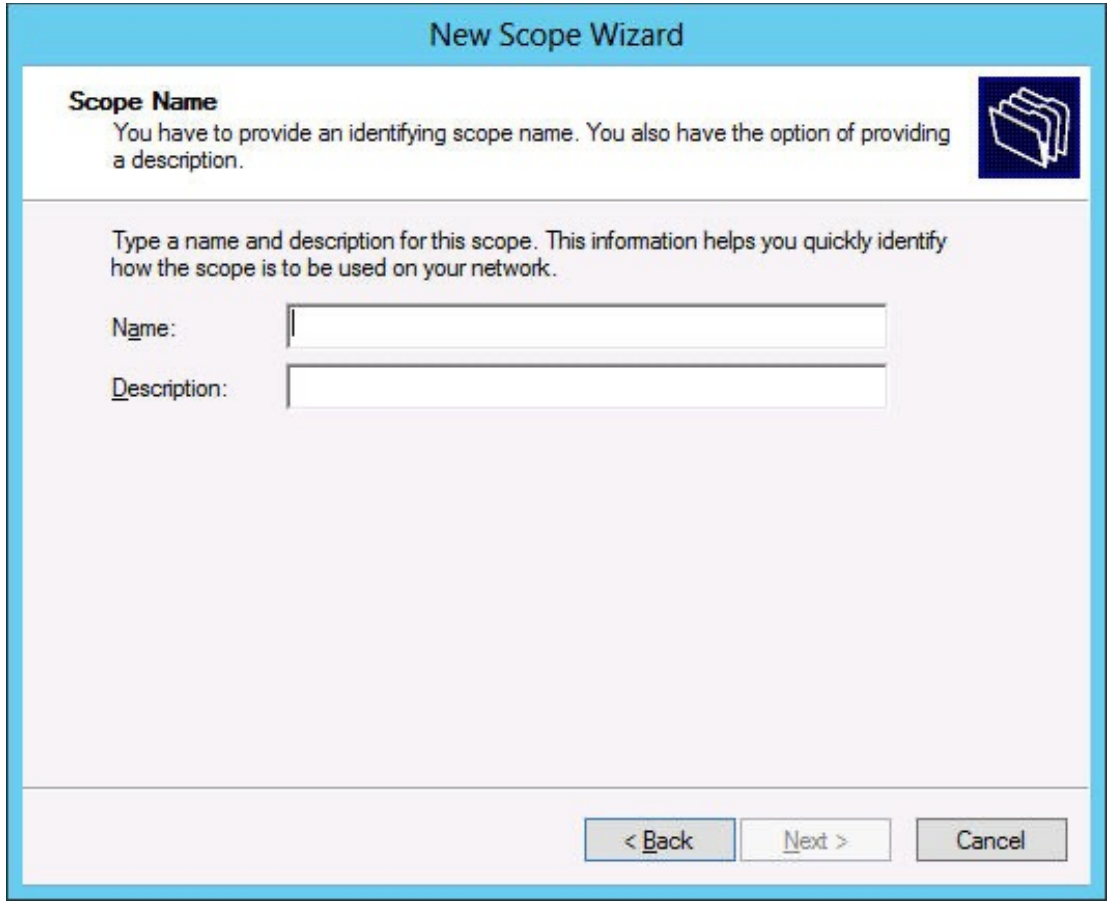
- A scope is a range of IP addresses on a particular subnet that are selected for allocation by a DHCP server.
- Create a scope using the DHCP snap-in for Microsoft Management Console (MMC).

Create a DHCP Scope



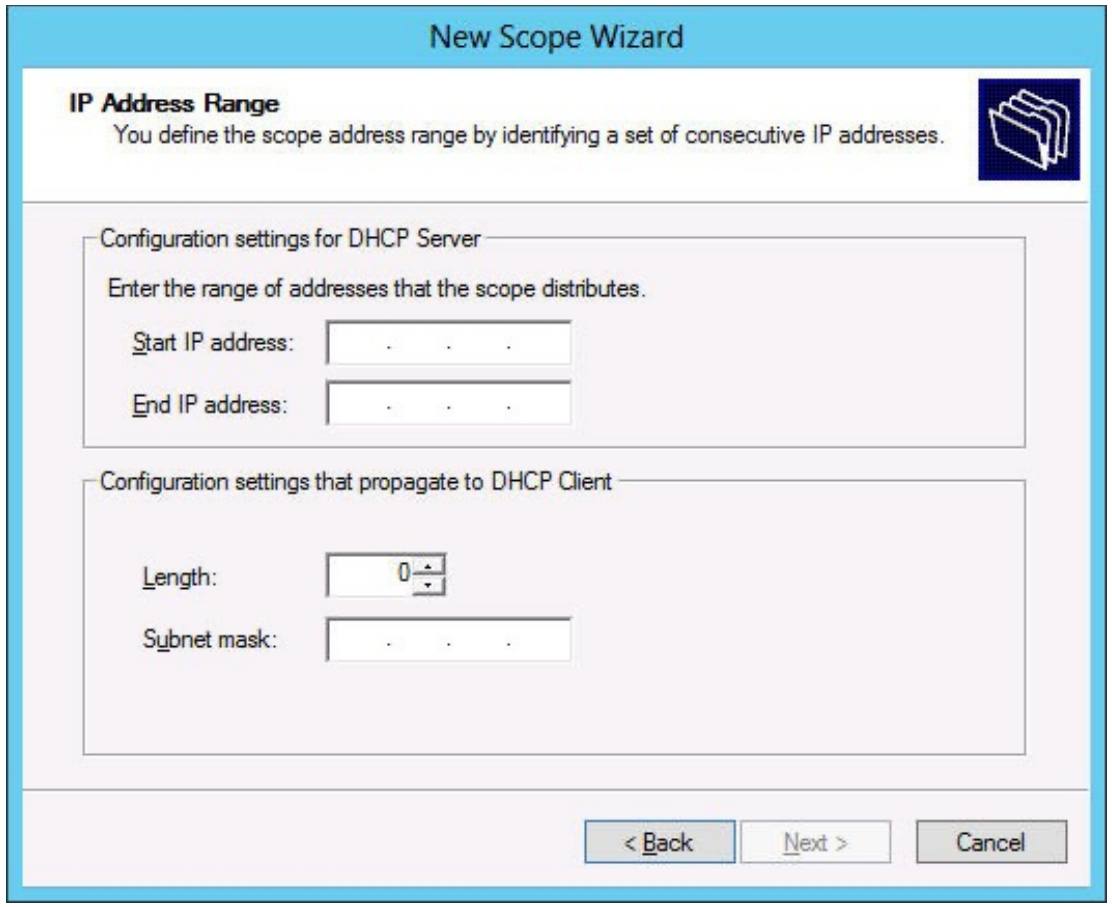
The DHCP console

Create a DHCP Scope



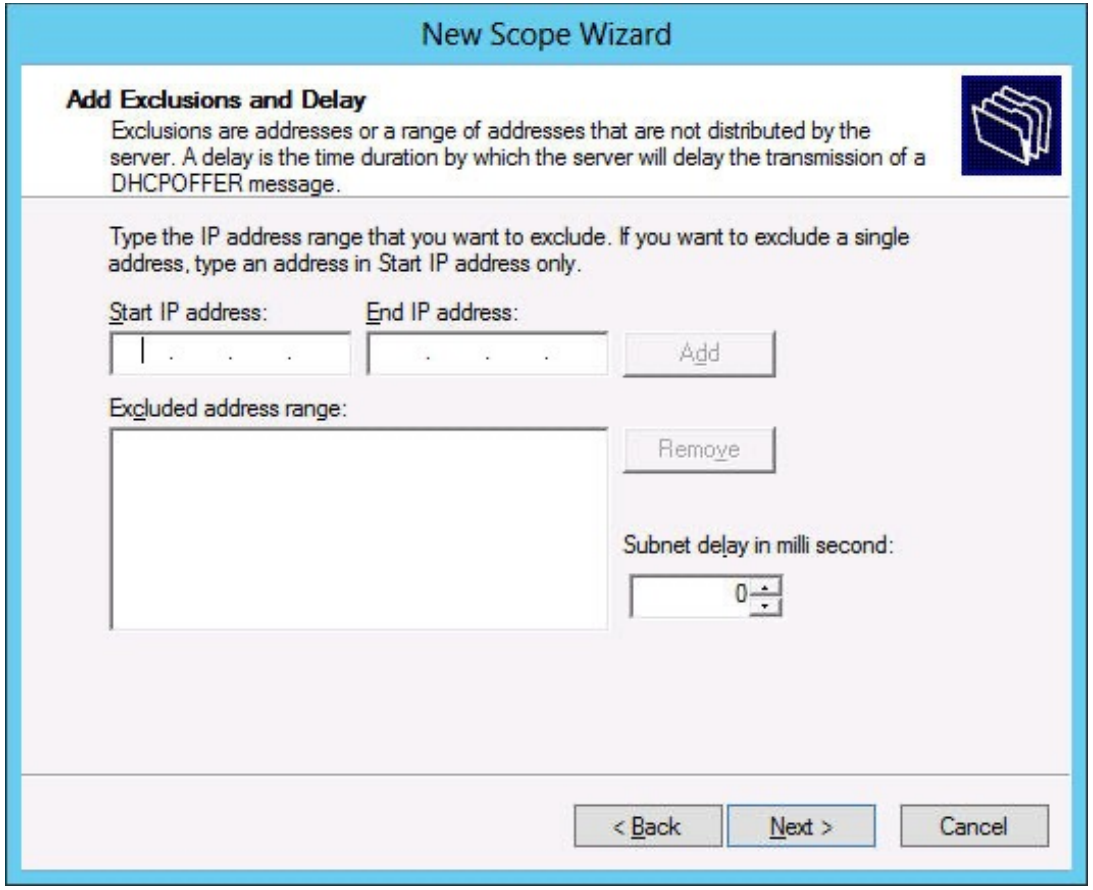
The Scope Name page in the DHCP console

Create a DHCP Scope



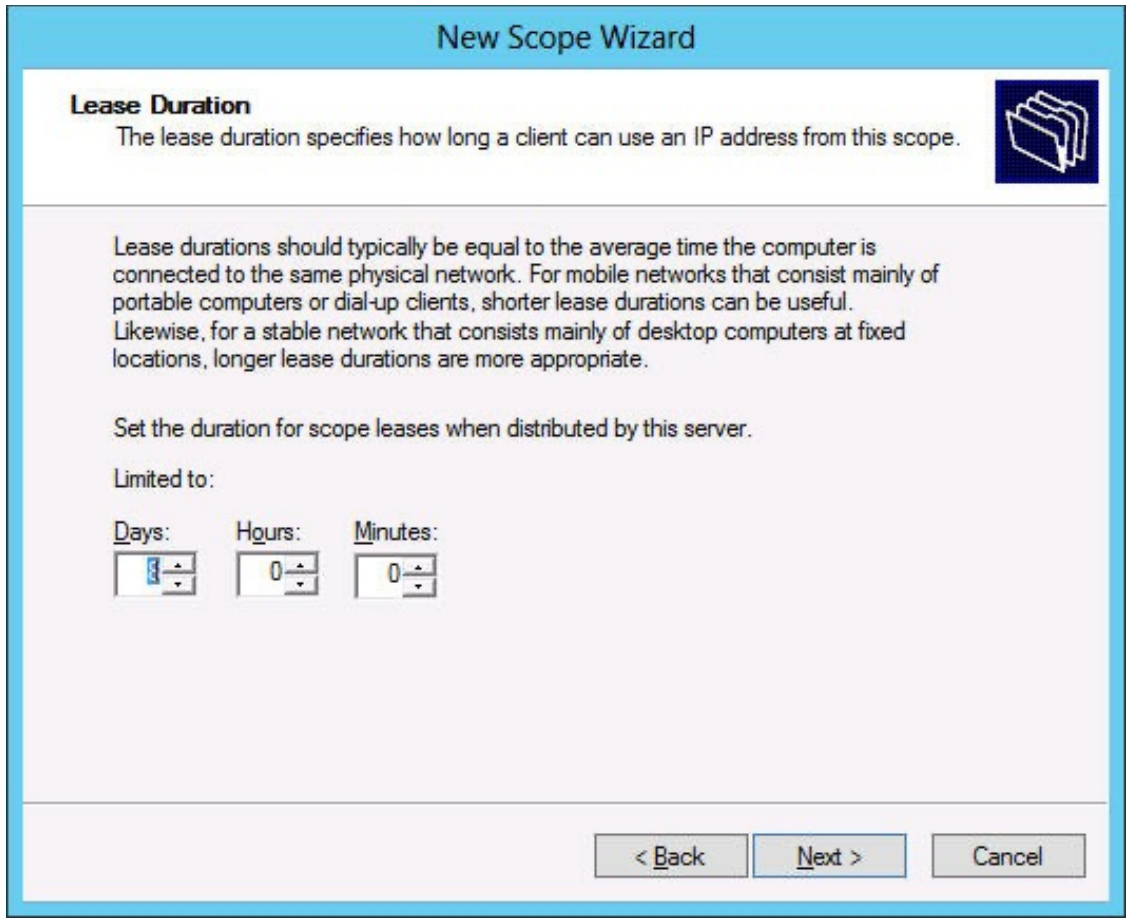
The Address Range page in the DHCP console

Create a DHCP Scope



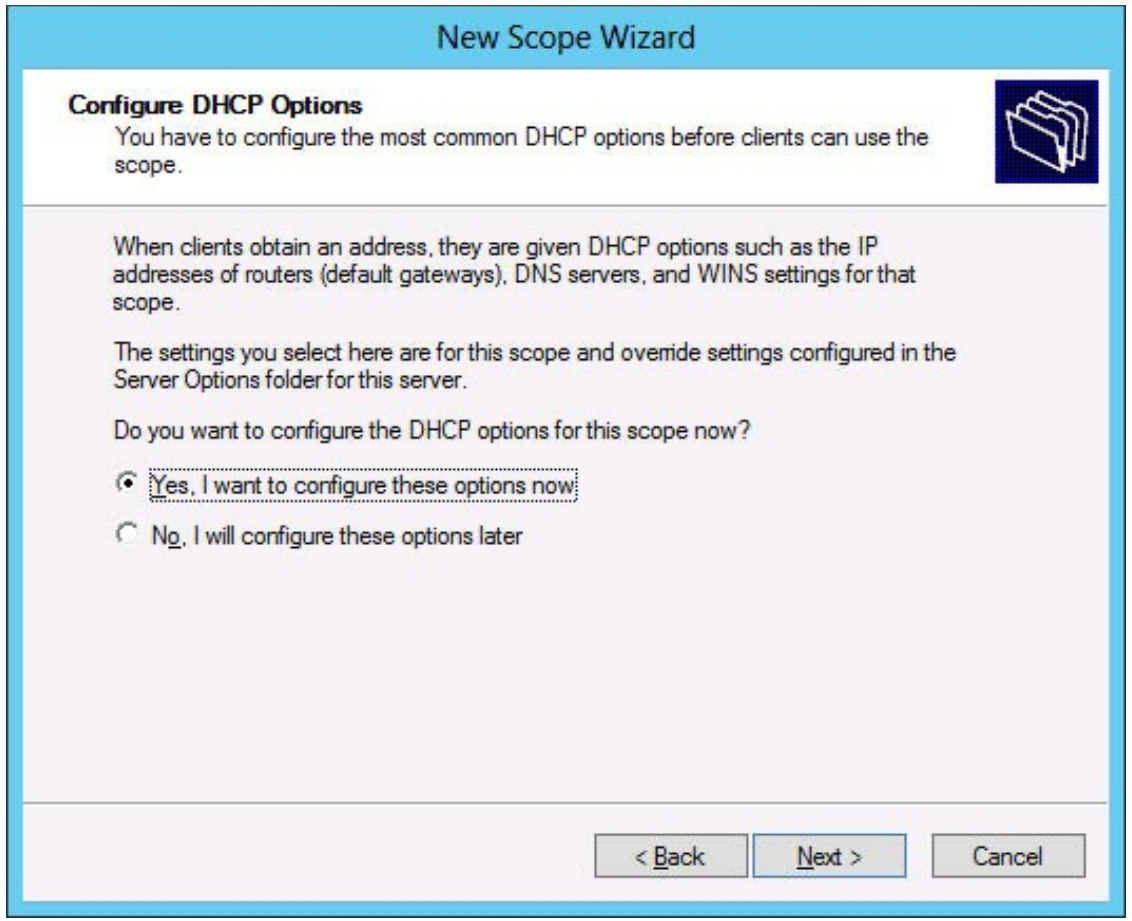
The Add Exclusions and Delay page in the DHCP console

Create a DHCP Scope



The Lease Duration page in the DHCP console

Create a DHCP Scope

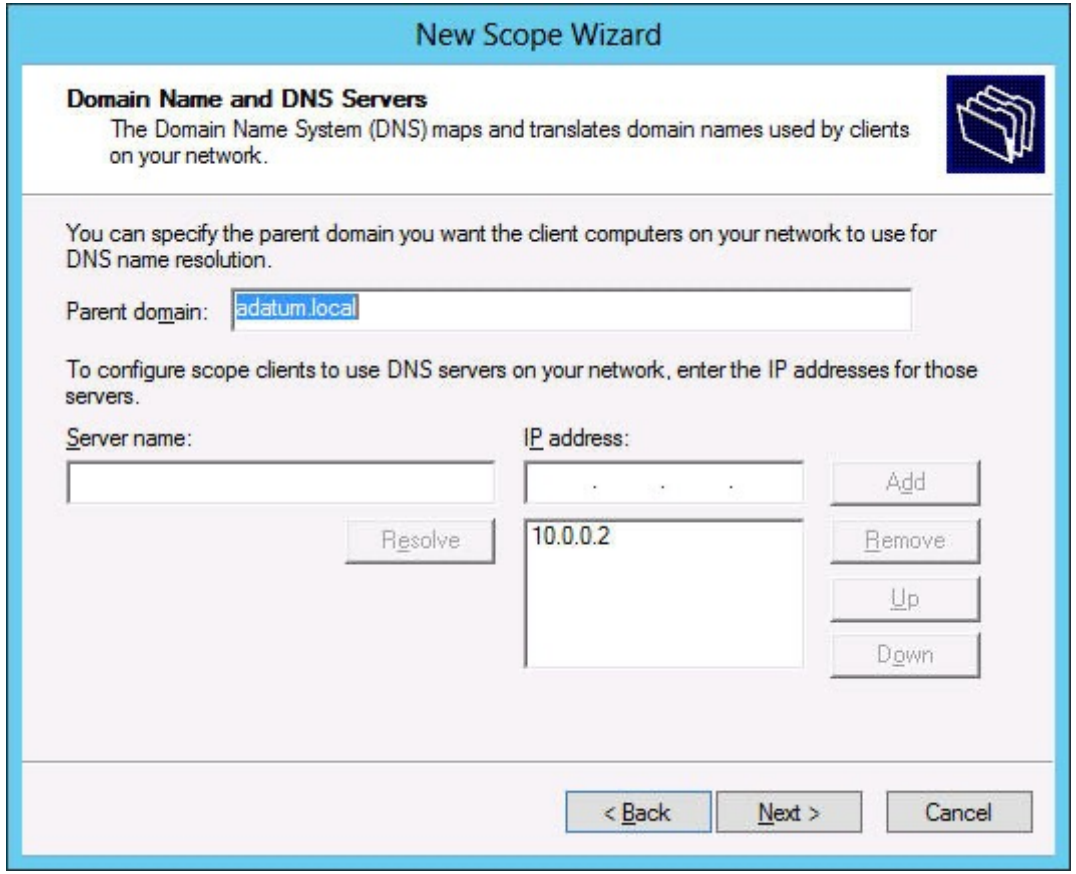


The Configure DHCP Options page in the DHCP console

Create a DHCP Scope

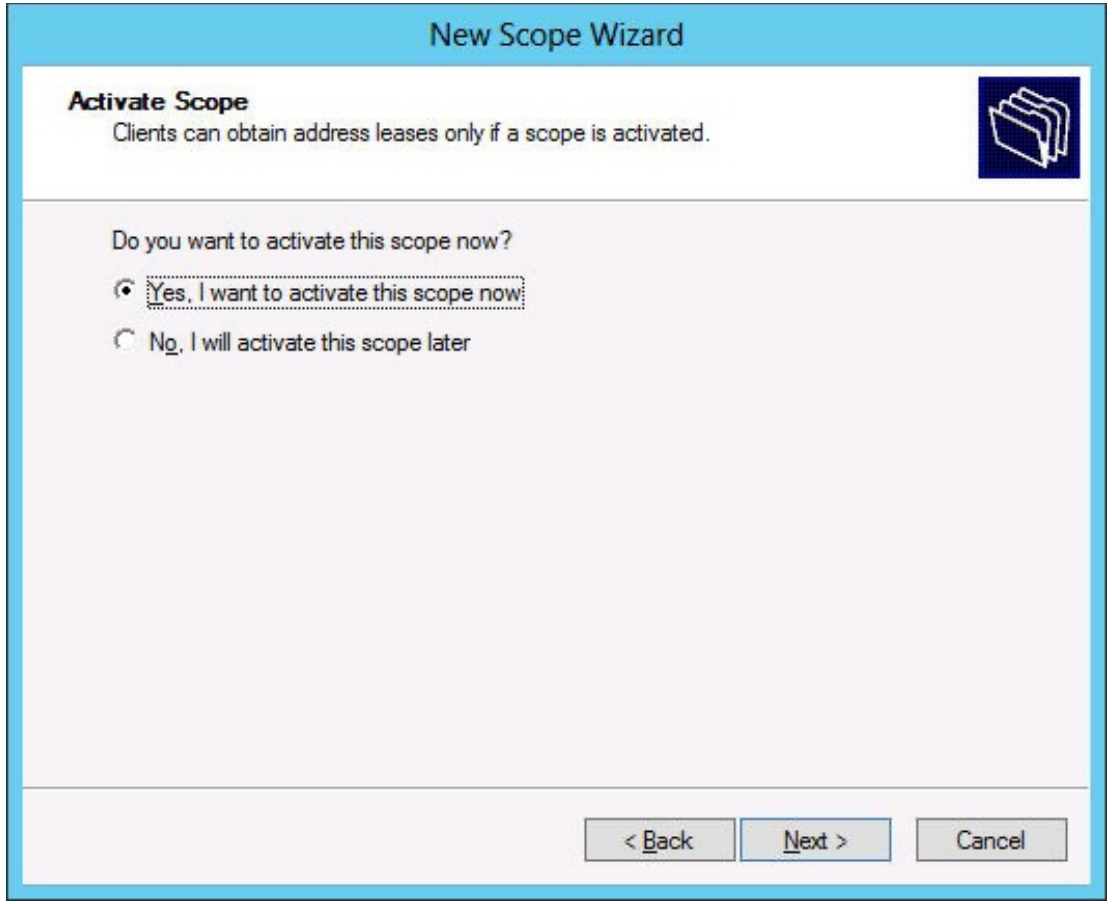
The Router (Default Gateway) page in the DHCP console

Create a DHCP Scope



The Domain Name and DNS Servers page in the DHCP console

Create a DHCP Scope



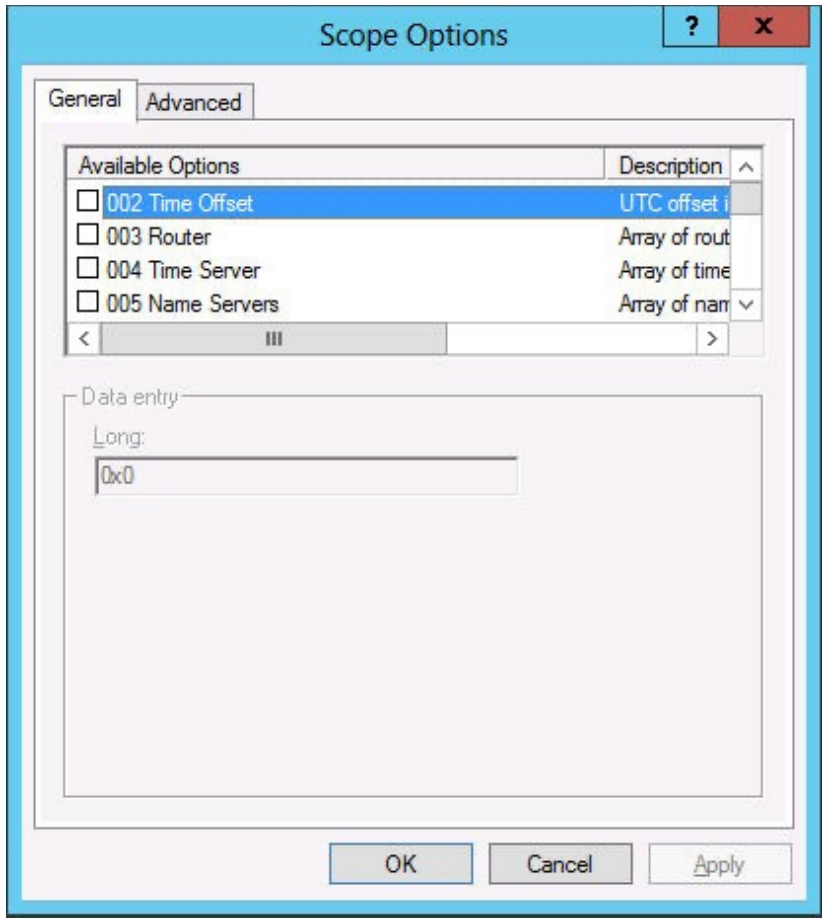
The Activate Scope page in the DHCP console

Configuring DHCP Options

The Windows DHCP server supports two kinds of options:

- **Scope options:** Supplied only to DHCP clients receiving addresses from a particular scope.
- **Server options:** Supplied to all DHCP clients receiving addresses from the server.

Configuring DHCP Options

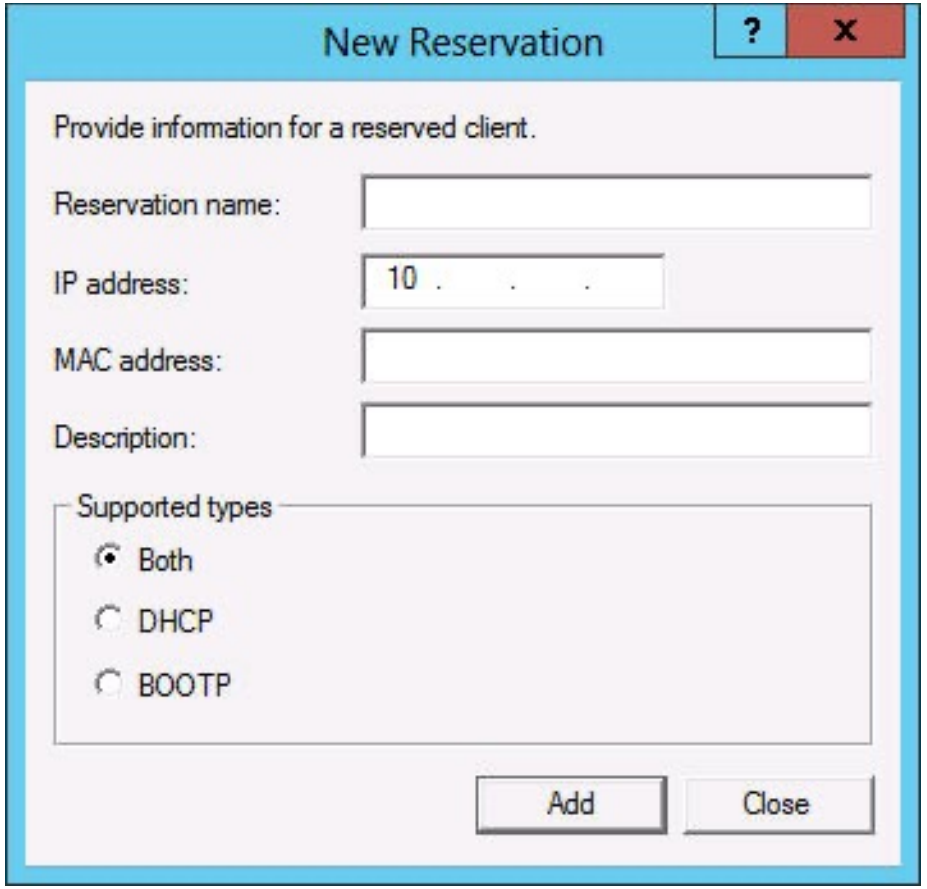


The Scope Options dialog box

Creating a Reservation

- A **reservation** is a manually allocated address.
- Used for computers whose IP addresses must remain the same (static), like domain controllers, DNS servers, and Internet web servers.
- Allows you to manage all of your IP addresses through DHCP.

Creating a Reservation



A DHCP server's New Reservation dialog box