Hunan University of Arts and Science

Networking Theory & Applications

CIS 291

2018 – 2019

Windows Server 2012

Part 3B

Chapter 4
Deploying and configuring core network services
部署和配置核心网络服务

Objectives in this chapter:　本章的目标

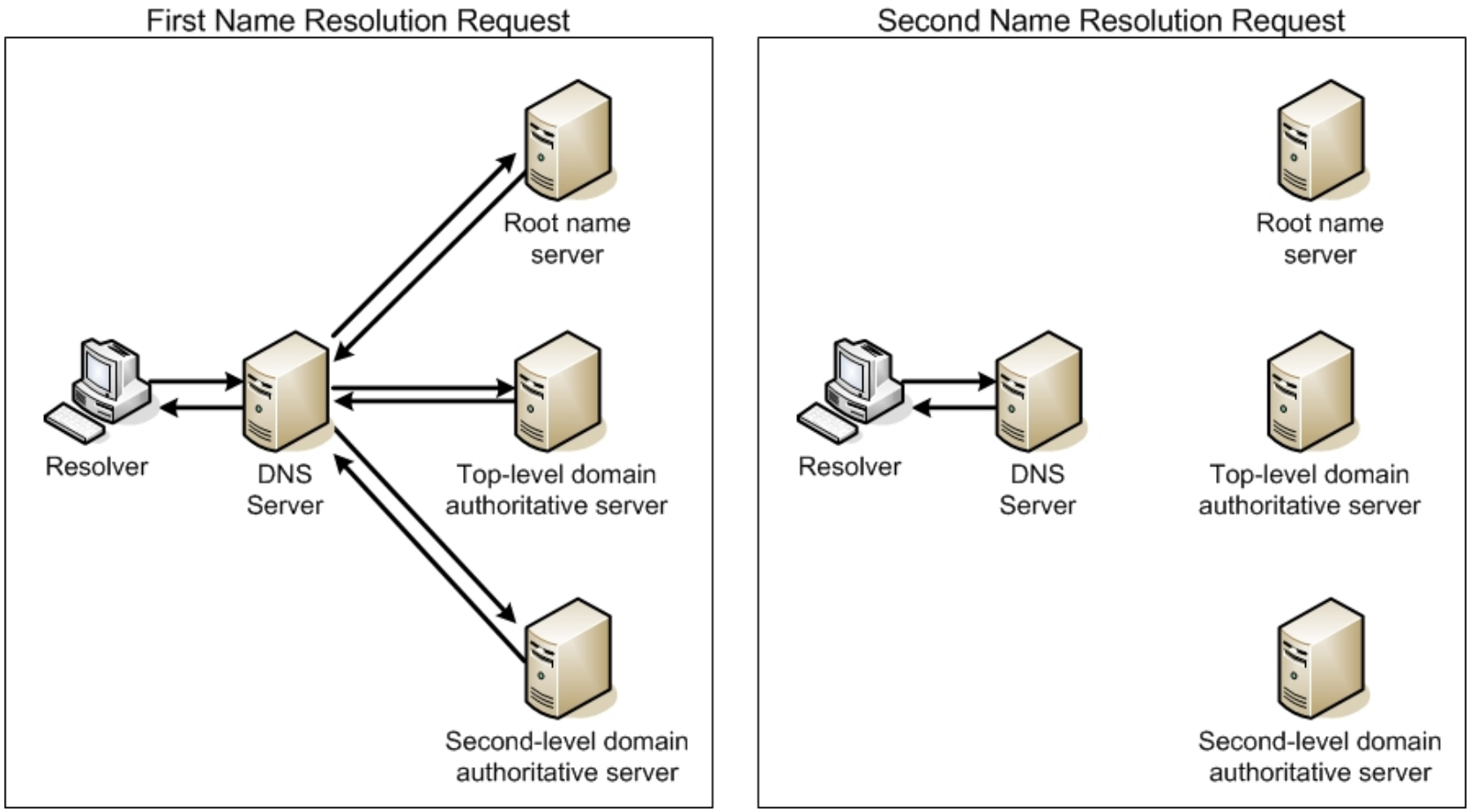
1- Configure IPv4 and IPv6 addressing

2- Configure servers

3- Deploy and configure DNS service

6- 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.



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.

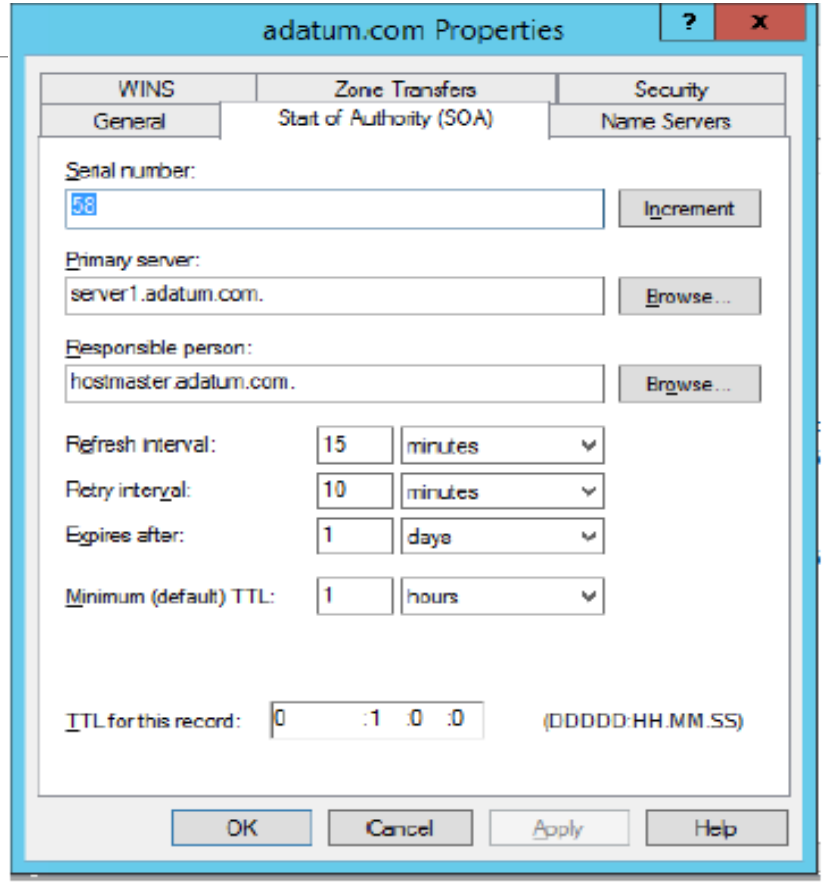
Cache Data Persistence

- 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.
- However, caches must be purged eventually, and there is a fine line between effective and ineffective caching.
- 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.
- On a network where changes in IP addresses or the addition of new resource records is frequent, a lower TTL value increases the likelihood that clients will receive current data.
- On a network that rarely changes, a longer TTL value minimizes the number of requests sent to the parent servers of your domain or zone.

- To modify the TTL value for a zone on a WS 2012 R2 DNS server, right-click the zone, open the Properties sheet, and click the Start Of Authority (SOA) tab, as shown in Figure 4-20. On this tab, you can modify the TTL for this record setting from its default value of one hour.

Client-side resolver caching

- The client resolver on Windows systems also contains a caching mechanism, which stores resolved IP addresses and also HOSTS file information on a local drive.
- When a client enounters a name that needs to be resolved into an IP address, it checks its local cache first, before sending a request to its DNS server.



Viewing the Start Of Authority (SOA) tab on a DNS server's Properties sheet

7-DNS Referrals and Queries

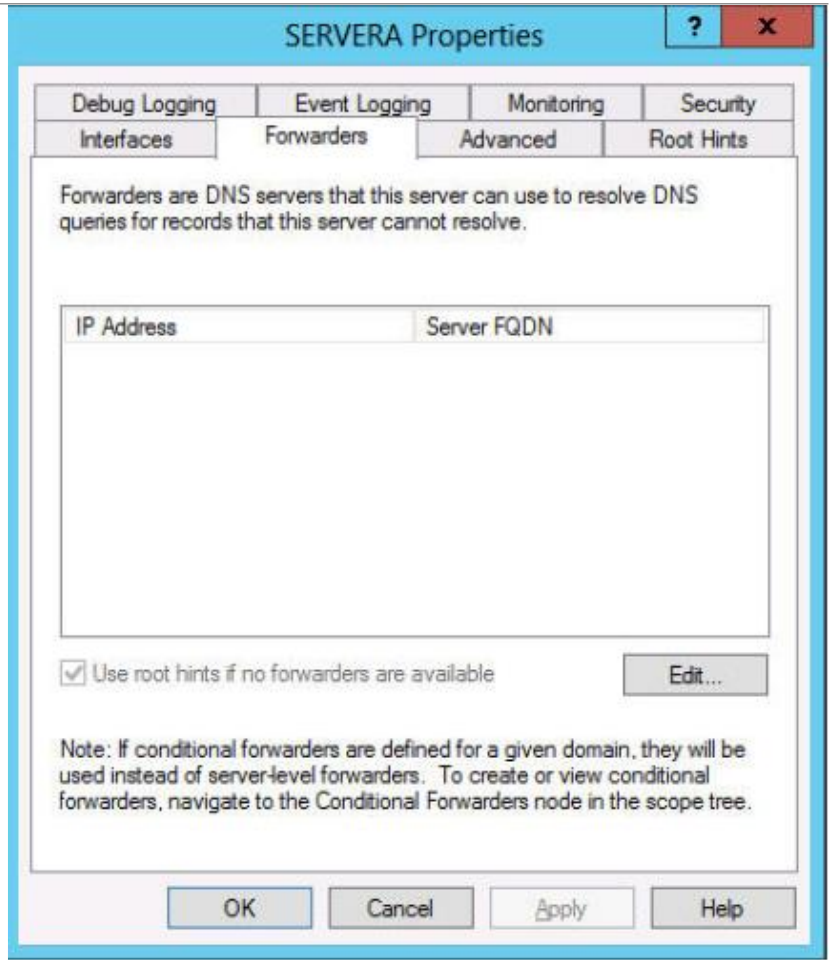
- The process by which one DNS server sends a name resolution request to another DNS server is called a referral.
- DNS servers recognize two types of name resolution requests:
  - ✓ Recursive query: The DNS server receiving the name resolution request takes full responsibility for resolving the name. If the server possesses information about the requested name, it replies immediately to the requestor. TCP/IP client resolvers always send recursive queries to their designated DNS servers.
  - ✓ 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.

8- 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.
- To prevent this, the Windows Server 2012 R2 DNS server enables you to configure one server to function as the forwarder for all Internet queries generated by the other servers on the network.
- Any time a server has to resolve the DNS name of an Internet system and fails to find the needed information in its cache, it transmits a recursive query to the forwarder, which is then responsible for sending its own iterative queries over the Internet connection.
- Once the forwarder resolves the name, it sends a reply back to the original DNS server, which relays it to the client.

- To configure forwarders on a Windows Server 2012 R2 DNS server, right-click the server node, open the Properties sheet, and click the Forwarders tab, as shown in Figure 4-21.
- On this tab, you can add the names and addresses of the servers that you want your server to use as forwarders.

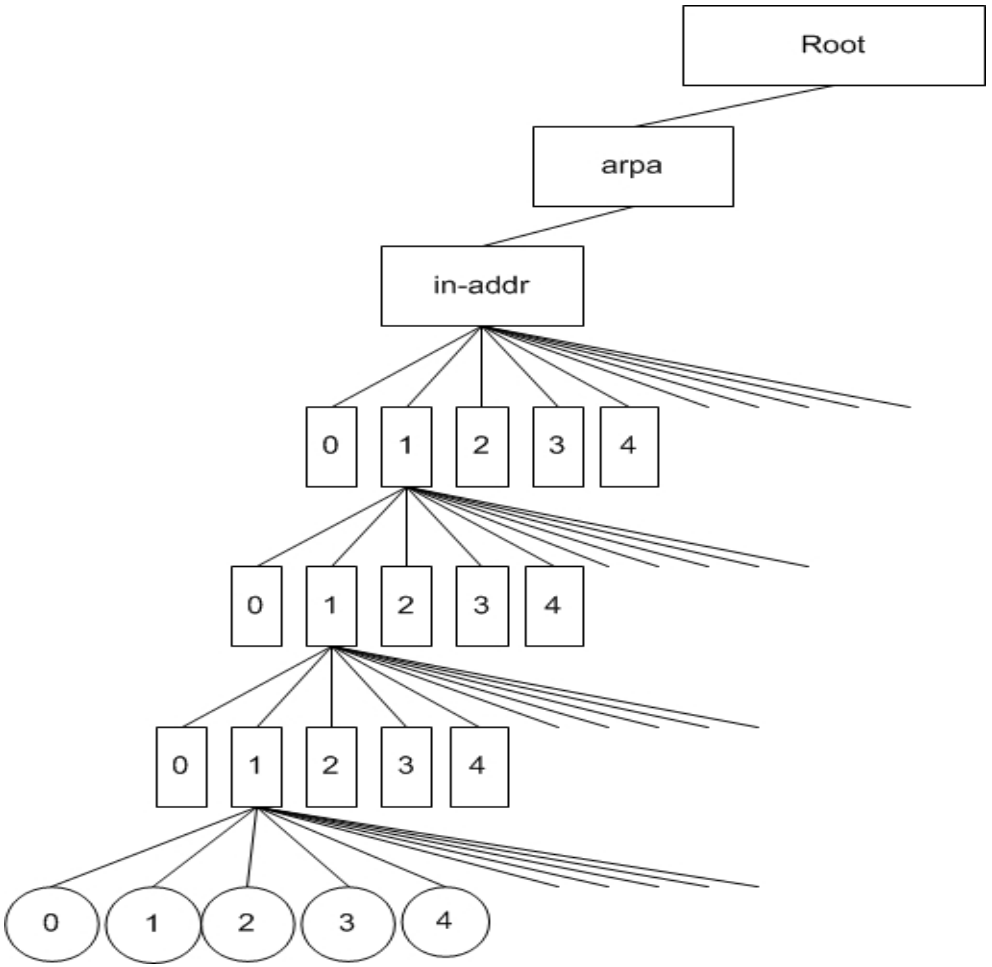
The Forwarders tab on a DNS server's Properties sheet



Break

9- 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.



The DNS reverse lookup domain

10- Deploying a DNS Server

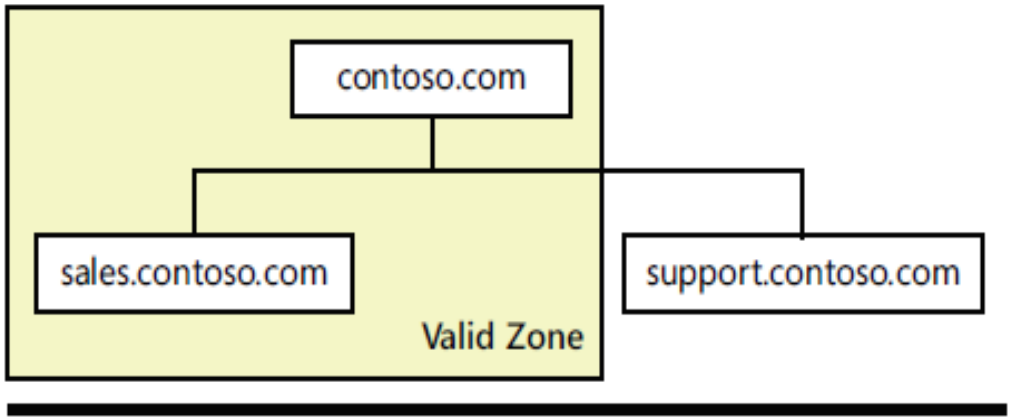
- The process of deploying a DNS server on a WS 2012 R2 computer is just a matter of installing the DNS Server role by using the Add Roles And Features Wizard in Server Manager.
- The server is ready to perform caching-only name resolution services for any clients that have access to it.
- The role also installs the DNS Manager console, which you use to configure the DNS server's other capabilities.

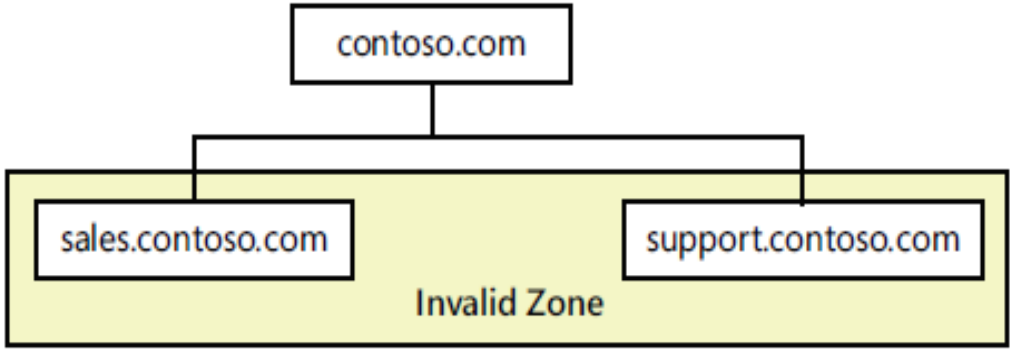
11- Creating Zones

- 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

- ✓ For example, you can create a zone containing a parent domain and its child, because they are directly connected,
- ✓ but you cannot create a zone containing two child domains without their common parent, because the two children are not directly connected, as shown in Figure 4-23.





Valid zones must consist of contiguous domains

- The DNS server in WS 2012 R2 can support as many as 200,000 zones on a single server, although it is hard to imagine a scenario that would require that many.
- Every zone consists of a zone database, which contains the resource records for the domains in that zone.

Zone Types

The DNS server in WS 2012 R2 supports three zone types, which specify where the server stores the zone database and what kind of information it contains. These zone types are as follows:

- ✓ **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.

- DNS was designed long before Active Directory, so most of the Internet relies on primary and secondary zones using text-based database files.
- However, for DNS servers supporting internal domains, especially AD DS domains, using the Windows DNS server to create a primary zone and store it in Active Directory is the recommended procedure.

12- 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.
- You can modify the DNS resource records on any writable domain controller hosting a copy of the zone data, and Active Directory will automatically update all the other domain controllers.
- You don't have to create secondary zones or manually configure zone transfers, because Active Directory performs all database replication activities.
- Creating an active directory zone- look procedures P244 lab practice

13- 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)

There are several different types of resource records used by DNS servers, the most important of which are as follows:

- **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.

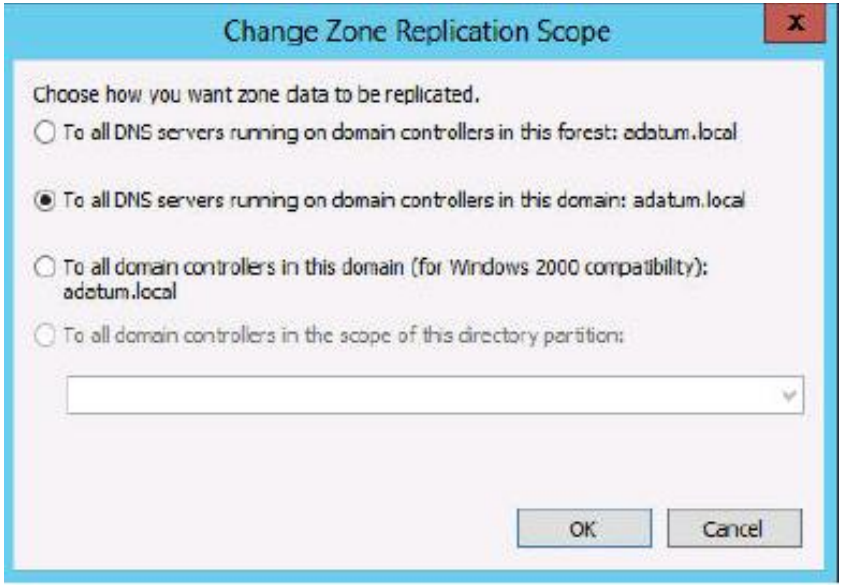
❑ To create a new Address resource record, use the following procedure. Look P246 Lab practice

14- 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. The following sections describe some of these settings.

1- CONFIGURING ACTIVE DIRECTORY DNS REPLICATION

To modify the replication scope for an Active Directory–integrated zone, open the zone's Properties sheet in the DNS Manager console and, on the General tab, click Change for Replication: All DNS Servers In The Active Directory Domain to display the Change Zone Replication Scope dialog box.



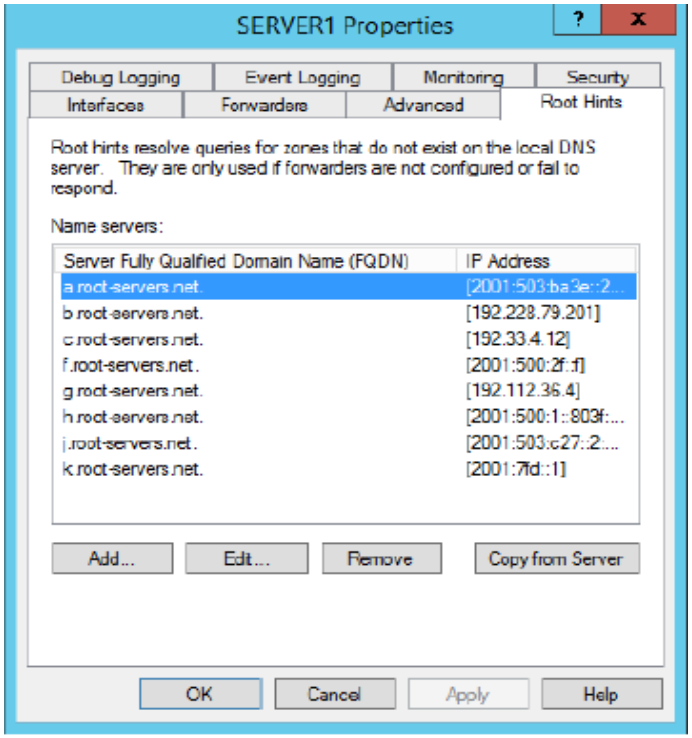
The Change Zone Replication Scope dialog box

2- CONFIGURING ROOT HINTS

- Most DNS servers must be able to contact the root name servers to initiate name resolution processes.
- Most server implementations, including Microsoft DNS Server, are preconfigured with the names and addresses of multiple root name servers. These are called *Root Hints*.
- The 13 root name server names are located in a domain called root-servers.net and are named using letters of the alphabet.

- To modify the Root Hints on a WS 2012 R2 DNS server, right-click the server node, open the Properties sheet, and click the Root Hints tab, as shown in Figure 4-27.

- On this tab, you can add, edit, or remove Root Hints from the list provided.



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