# Module 7

## Implementing DNS

## Module Overview

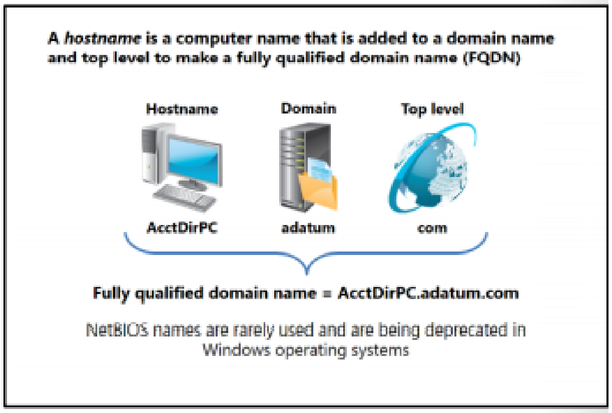
Name resolution is the process of software translating between names that users can read and understand, and numerical IP addresses, which are necessary for TCP/IP communications. Because of this, name resolution is one of the most important concepts of every network infrastructure. You can think about DNS as being like the Internet's phone book for computers. Client computers use the name resolution process when locating hosts on the Internet and when locating other hosts and services in an internal network. Doman Name System (DNS) is one of the most common technologies for name resolution. Active Directory® Domain Services (AD DS) depends heavily on DNS, as does Internet traffic. This module discusses some basic name resolution concepts, and installing and configuring a DNS Server service and its components.

## Name Resolution for Windows Clients and Servers

You can configure a computer to communicate over a network by using a name in place of an IP address. The computer then uses name resolution to find an IP address that corresponds to a name, such as a host name. This lesson focuses on different types of computer names, the methods used to resolve them, and how to troubleshoot problems with name resolution.

### What Are the Computer Names Assigned to Computers?

The TCP/IP set of protocols identifies source and destination computers by their IP addresses. However, computer users are much better at using and remembering names than numbers. Because of this, administrators usually assign names to computers. Administrators then link these names to computer IP addresses in a name resolution system such as DNS. These names are in either in *host name* format, for example *dc1.contoso.com*, which is recognized by DNS, or in *NetBIOS name* format, for example *DC1*, which is recognized by Windows Internet Name Service (WINS).



**A *hostname* is a computer name that is added to a domain name and top level to make a fully qualified domain name (FQDN)**

**Fully qualified domain name = AcctDirPC.adatum.com**

NetBIOS names are rarely used and are being deprecated in Windows operating systems

### Name Type

The type of name that an app uses, either host name or NetBIOS name, is determined by the application developer. If the application developer designs an application to request network services through Windows sockets, host names are used. If, on the other hand, the application developer designs an application to request services through NetBIOS, a NetBIOS name is used. Most current apps, including Internet apps, use Windows sockets—and thus use host names—to access network services.

### Host Names

A *host name* is a user-friendly name that is associated with a computer's IP address to identify it as a TCP/IP host. The host name can be up to 255 characters long, and can contain alphabetic and numeric characters, periods, and hyphens.

You can use host names in various forms. The two most common forms are:

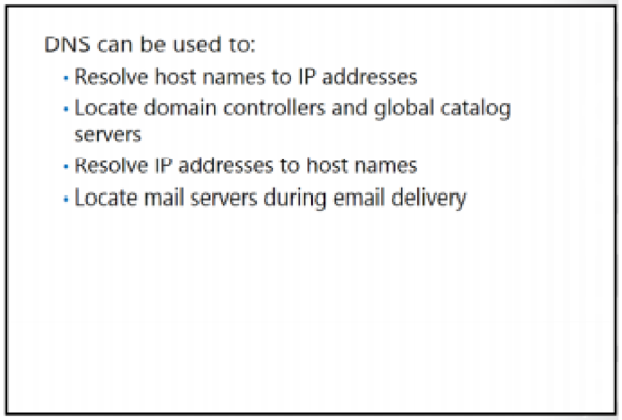
- An alias
- A fully qualified domain name (FQDN)

An alias is a single name that is associated with an IP address, such as *payroll*. You can combine an alias with a domain name to create an FQDN. An FQDN is structured for use on the Internet, and includes periods as separators. An example of an FQDN is *payroll.contoso.com*.

## What Is DNS?

*DNS* is a service that resolves FQDNs and other host names to IP addresses. All Windows Server operating systems include a DNS Server service.

When you use DNS, users on your network can locate network resources by typing in user-friendly names (for example, www.microsoft.com), which the computer then resolves to an IP address. The benefit is that IPv4 addresses may be difficult to remember (for example, 131.107.0.32), while a domain name typically is easier to remember. In addition, you can use host names that do not change while the underlying IP addresses can be changed to suit your organizational needs.



DNS can be used to:

- Resolve host names to IP addresses
- Locate domain controllers and global catalog servers
- Resolve IP addresses to host names
- Locate mail servers during email delivery

DNS uses a database of names and IP addresses, stored in a file or in AD DS, to provide this service. DNS client software performs queries on and updates to the DNS database. For example, within an organization, a user who is trying to locate a print server can use the DNS name printserver.contoso.com, and the DNS client software resolves the name to a printer's IP address, such as 172.16.23.55. Even if the printer's IP address changes, the user-friendly name can remain the same.

The representation of the entire hierarchical domain structure as shown in the following illustration is known as a DNS namespace.

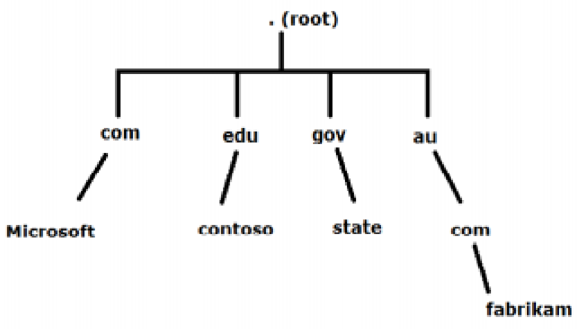


**FIGURE 7.1: DNS NAMESPACE**

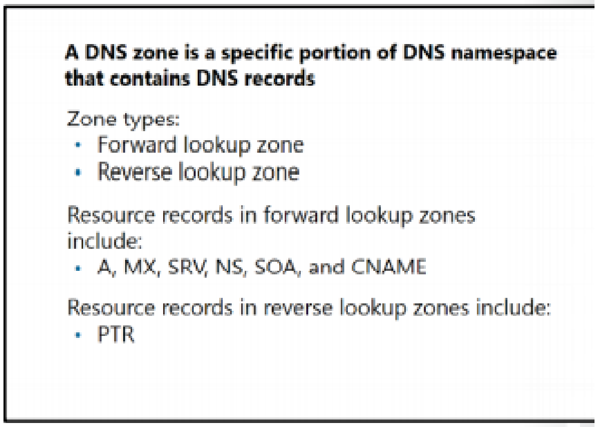
The Internet uses a single DNS namespace with multiple root servers. To participate in the Internet DNS namespace, a domain name must be registered with a DNS registrar. This ensures that no two organizations attempt to use the same domain name.

If hosts that are located on the Internet do not need to resolve names in your domain, you can host a domain internally, without registering it. However, you must still ensure that the domain name is unique from Internet domain names, or connectivity to Internet resources might be affected. A common way to ensure uniqueness is to create an internal domain in the .local domain. The .local domain is reserved for internal use in much the same way that private IP addresses are reserved for internal use.

In addition to resolving host names to IP addresses, DNS can be used to:

- Locate domain controllers and global catalog servers. This is used when logging on to AD DS.
- Resolve IP addresses to host names. This is useful when a log file contains only the IP address of a host.
- Locate a mail server for email delivery. This is used for the delivery of all Internet email.

## DNS Zones and Records



**A DNS zone is a specific portion of DNS namespace that contains DNS records**

Zone types:

- Forward lookup zone
- Reverse lookup zone

Resource records in forward lookup zones include:

- A, MX, SRV, NS, SOA, and CNAME

Resource records in reverse lookup zones include:

- PTR

A *DNS zone* is the specific portion of a DNS namespace (such as adatum.com) that contains DNS records. A DNS zone is hosted on a DNS server that is responsible for responding to queries for records in a specific domain. For example, the DNS server that is responsible for resolving www.contoso.com to an IP address would contain the contoso.com zone.

You can store DNS zone content in a file or in the AD DS database. When the DNS server stores the zone in a file, that file is located in a local folder on the server. When the zone is not stored in AD DS, only one copy of the zone is a writable copy, and all the other copies are read-only.

The most commonly used types of zones in Windows Server DNS are forward lookup zones and reverse lookup zones.

### Forward Lookup Zones

*Forward lookup zones* resolve host names to IP addresses and host common resource records, including:

- Host (A) records
- Alias (CNAME) records
- Service (SRV) records
- Mail exchanger (MX) records
- Start of authority (SOA) records
- Name server (NS) records

The most common record type is the host (A) resource record.

### Reverse Lookup Zones

*Reverse lookup zones* resolve IP addresses to domain names. A reverse lookup zone functions in the same manner as a forward lookup zone, but the IP address is part of the query and the host name is the returned information. Reverse lookup zones are not always configured, but you should configure them to reduce warning and error messages. Reverse lookup zones host SOA, NS, and pointer (PTR) resource records.

### *PTR Records*

When you create host records in the DNS console, you also have the option to make a PTR record at the same time, if an appropriate reverse lookup zone exists. PTR records can be created automatically and added to a reverse lookup zone when an A record is created in a forward lookup zone. These PTR records are automatically deleted if the corresponding A resource record is deleted. You only need to manually create a PTR record once. Since it is not tied to an A resource record, it is not deleted if the A resource record is deleted. Client computers can create their PTR records when they dynamically update. A PTR record is in the format of IP Address, type of record (PTR) and hostname.

Many standard Internet protocols rely on reverse lookup zone lookup data to validate forward lookup zone information. For example, if the forward lookup indicates that training.contoso.com is resolved to 192.168.2.45, you can use a reverse lookup to confirm that 192.168.2.45 is associated with training.contoso.com.

### Resource Records

The DNS zone file stores resource records. *Resource records* specify a resource type and the IP address to locate the resource. The most common resource record is a host (A) resource record. This is a simple record that resolves a host name to an IP address. The host can be a workstation, server, or another network device, such as a router.

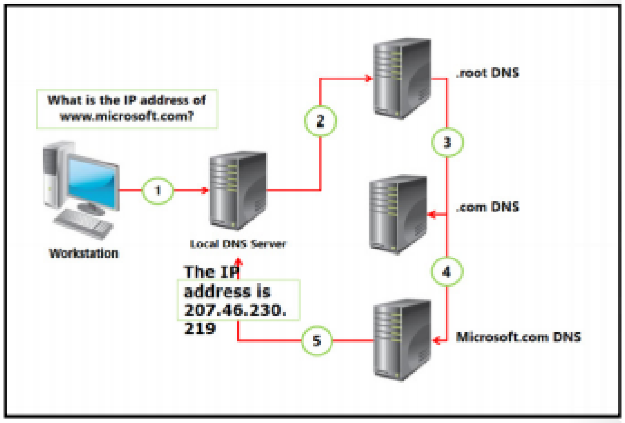
Resource records also help find resources for a particular domain. For instance, when a Microsoft Exchange Server needs to find the server that is responsible for delivering mail for another domain, it requests the mail exchanger (MX) resource record for that domain. This record points to the host (A) resource record of the host that is running the SMTP mail service.

Resource records also can contain custom attributes. MX records, for instance, have a Preference attribute, which is useful if an organization has multiple mail servers. The MX record tells the sending server which mail server the receiving organization prefers. SRV records also contain information about the port the service is listening to, and the protocol that you should use to communicate with the service.

## How Internet DNS Names Are Resolved

When resolving DNS names on the Internet, an entire system of computers is used rather than just a single server. There are hundreds of servers on the Internet, called *root servers*, which manage the overall practice of DNS resolution. These servers are represented by 13 FQDNs. A list of these 13 servers is preloaded on each DNS server. When you register a domain name on the Internet, you are paying to become part of this system.

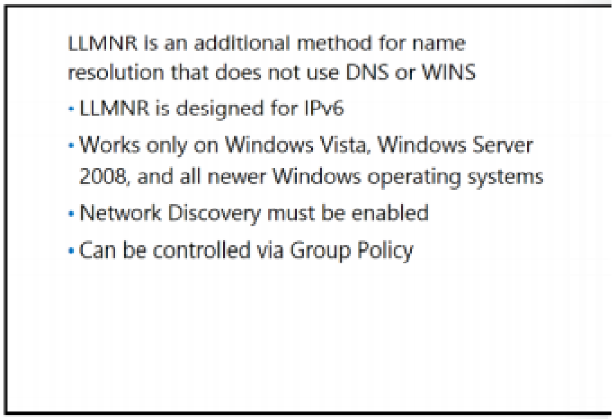
To see how these servers work together to resolve a DNS name, look at the following name resolution process for the name www.microsoft.com:


What is the IP address of www.microsoft.com?
Workstation
1
Local DNS Server
2
.root DNS
3
.com DNS
4
Microsoft.com DNS
5
The IP address is 207.46.230.219

1. A workstation queries the local DNS server for the IP address www.microsoft.com.
2. If the local DNS server does not have the information, it queries a root DNS server for the location of the .com DNS servers.
3. The local DNS server queries a .com DNS server for the location of the microsoft.com DNS servers.
4. The local DNS server queries the microsoft.com DNS server for the IP address of www.microsoft.com.
5. The IP address of www.microsoft.com is returned to the workstation.

## What Is Link-local Multicast Name Resolution?

In Windows Server 2012, a new method for resolving names to IP addresses is Link-local Multicast Name Resolution (LLMNR). Because of various limitations that are beyond the scope of this lesson, LLMNR typically is used only on localized networks. Although LLMNR is able to resolve IPv4 addresses, it has been designed specifically for IPv6; therefore, if you want to use it, you must have IPv6 supported and enabled on your hosts.



LLMNR is an additional method for name resolution that does not use DNS or WINS

- LLMNR is designed for IPv6
- Works only on Windows Vista, Windows Server 2008, and all newer Windows operating systems
- Network Discovery must be enabled
- Can be controlled via Group Policy

LLMNR is commonly used in networks where:

- There are no DNS or NetBIOS services for name resolution.
- Implementation of these services is not practical for any reason.
- These services are not available.

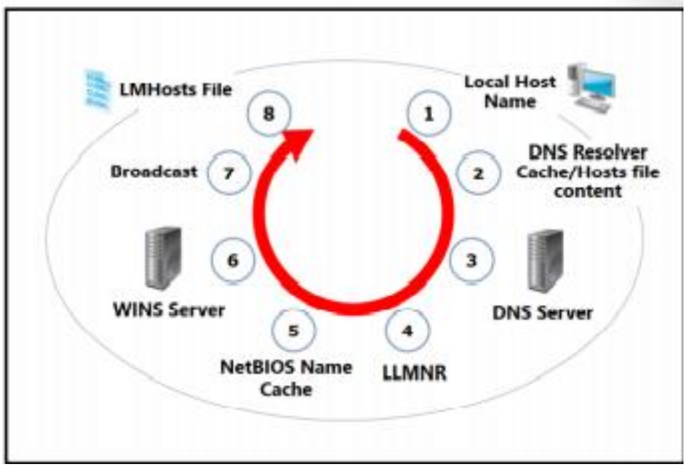
For example, you might want to set up a temporary network for testing purposes without a server infrastructure.

## How a Client Resolves a Name

Windows operating systems support a number of different methods for resolving computer names, such as DNS, WINS, and the host name resolution process.

### DNS

As previously discussed, DNS is the Microsoft standard for resolving host names to IP Addresses. For more information on DNS, refer back to second topic of this Lesson, *What is DNS*.

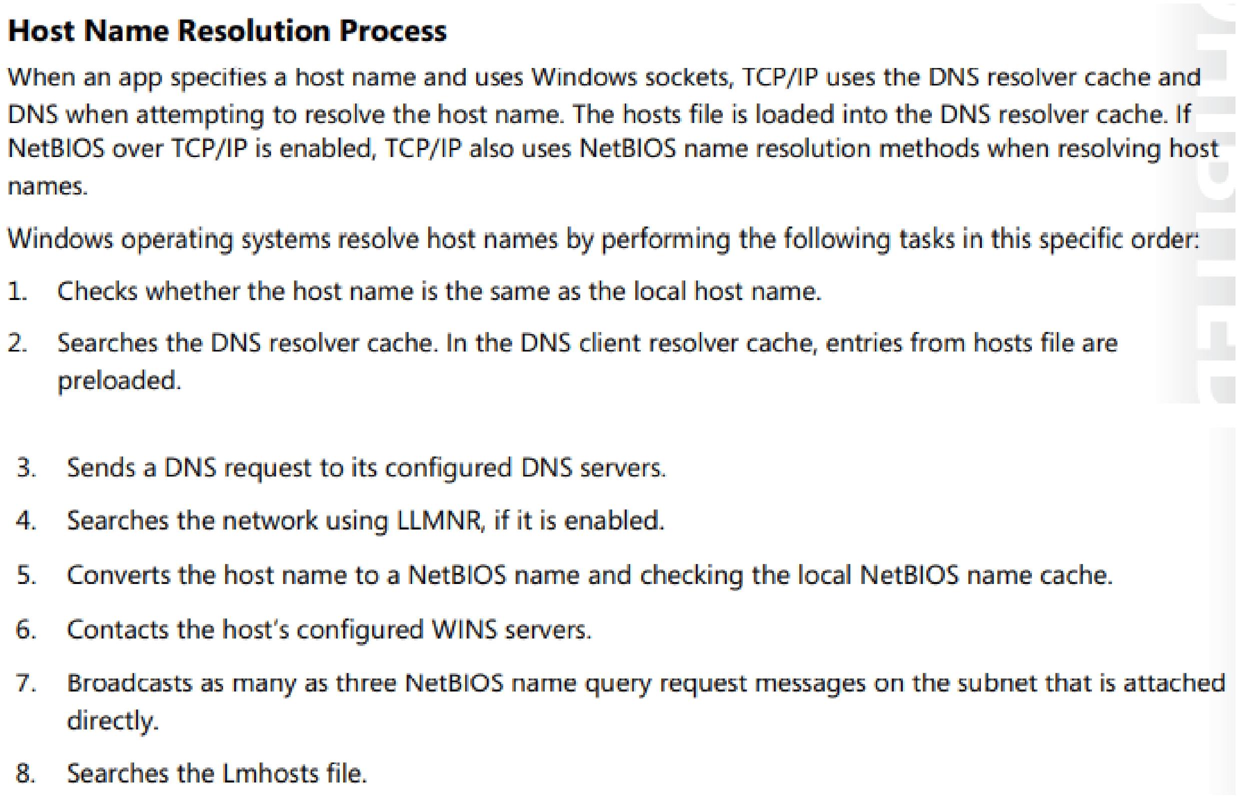


### WINS

WINS provides a centralized database for registering dynamic mappings of a network's NetBIOS names. Windows operating systems retain support for WINS to provide backward compatibility.

You can resolve NetBIOS names by using:

- Broadcast messages. Broadcast messages, however, do not work well on large networks because routers do not propagate broadcasts.
- Lmhosts file on all computers. Using an Lmhosts file for NetBIOS name resolution is a high maintenance solution, because you must maintain the file manually on all computers.
- Hosts file on all computers. Similar to an Lmhosts file, you can also use a hosts file for NETBIOS name resolution. This file is also stored locally on each machine, and it is used for fixed mappings of names to IP addresses, on local network segment.



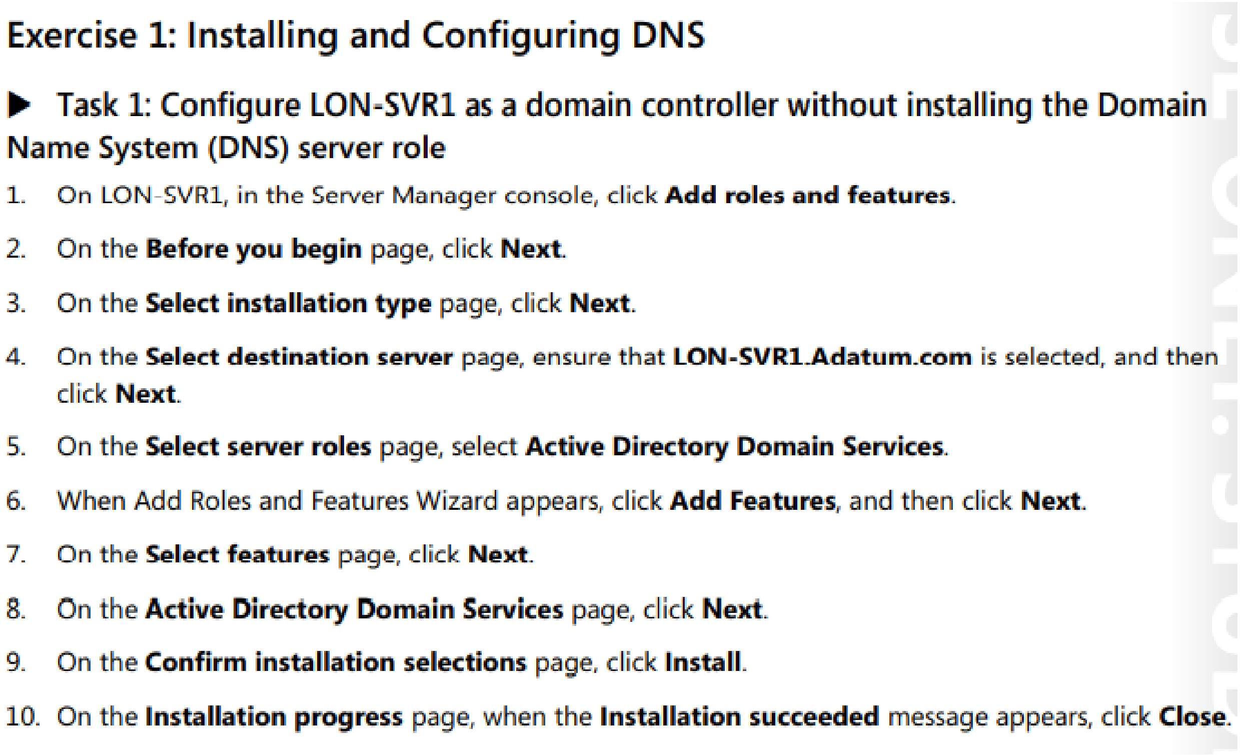
## Host Name Resolution Process

When an app specifies a host name and uses Windows sockets, TCP/IP uses the DNS resolver cache and DNS when attempting to resolve the host name. The hosts file is loaded into the DNS resolver cache. If NetBIOS over TCP/IP is enabled, TCP/IP also uses NetBIOS name resolution methods when resolving host names.

Windows operating systems resolve host names by performing the following tasks in this specific order:

1. Checks whether the host name is the same as the local host name.
2. Searches the DNS resolver cache. In the DNS client resolver cache, entries from hosts file are preloaded.
3. Sends a DNS request to its configured DNS servers.
4. Searches the network using LLMNR, if it is enabled.
5. Converts the host name to a NetBIOS name and checking the local NetBIOS name cache.
6. Contacts the host's configured WINS servers.
7. Broadcasts as many as three NetBIOS name query request messages on the subnet that is attached directly.
8. Searches the Lmhosts file.

# Module 7



## Exercise 1: Installing and Configuring DNS

### ▶ Task 1: Configure LON-SVR1 as a domain controller without installing the Domain Name System (DNS) server role

1. On LON-SVR1, in the Server Manager console, click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, select **Active Directory Domain Services**.
6. When Add Roles and Features Wizard appears, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, when the **Installation succeeded** message appears, click **Close**.

11. In the Server Manager console, on the navigation page, click **AD DS**.
12. On the title bar where **Configuration required for Active Directory Domain Services at LON-SVR1** is visible, click **More**.
13. On the **All Server Task Details and Notifications** page, click **Promote this server to a domain controller**.
14. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then click **Next**.
15. On the **Domain Controller Options** page, deselect the **Domain Name System (DNS) server** check box, and leave the **Global Catalog (GC)** check box selected.
16. Type **Pa$$w0rd** in both text fields, and then click **Next**.
17. On the **Additional Options** page, click **Next**.
18. On the **Paths** page, click **Next**.
19. On the **Review Options** page, click **Next**.
20. On the **Prerequisites Check** page, click **Install**.
21. On the **You're about to be signed out** blue bar, click **Close**.

**Note:** The LON-SVR1 server automatically restarts as part of the procedure.

22. After LON-SVR1 restarts, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

### ▶ Task 2: Create and configure Contoso.com zone on LON-DC1

1. On the LON-DC1 virtual machine, in the Server Manager console, click **Tools**, and then click **DNS**.
2. Expand **LON-DC1**, right-click **Forward Lookup Zones**, and then select **New Zone**.
3. In the New Zone Wizard, on the **Welcome to the New Zone Wizard** page, click **Next**.
4. On the **Zone Type** page, deselect the **Store the zone in Active Directory** check box, and then click **Next**.
5. On the **Zone Name** page, type **Contoso.com**, and then click **Next**.
6. On the **Zone File** page, click **Next**.
7. On the **Dynamic Update** page, click **Next**.
8. On the **Completing the New Zone Wizard** page, click **Finish**.
9. Expand **Forward Lookup Zones**, and then select and right-click **contoso.com** zone and click **New Host (A or AAAA)**
10. In the New Host window, in the **Name** textbox type **www**.

11. In the **IP address** box type **172.16.0.100**.

12. Click **Add Host**.

13. Click **OK** and then click **Done**.

14. Leave **DNS Manager** console open.

### ▶ Task 3: Review configuration settings on the existing DNS server to confirm root hints

1. On LON-DC1, in the DNS Manager console, click and then right-click **LON-DC1**, and then click **Properties**.

2. In the **LON-DC1 Properties** dialog box, click the **Root hints** tab. Ensure that root hints servers display.

3. Click the **Forwarders** tab. Ensure that the list displays no entries, and that the **Use root hints if no forwarders are available** option is selected.

4. Click **Cancel**.

5. Close the DNS Manager console.

6. In the taskbar, click the **Windows PowerShell** icon.

7. In Windows PowerShell, type the following cmdlets, pressing Enter after each, and observe the output returned:

```
Get-DnsServerRootHint
Get-DnsServerForwarder
```

   Note that both cmdlets are the respective Windows PowerShell equivalents of the DNS Console actions performed in steps 2 and 3 above.

### ▶ Task 4: Add the DNS server role for the branch office on the domain controller

1. On LON-SVR1, in the Server Manager console, click **Add roles and features**.

2. On the **Before you begin** page, click **Next**.

3. On the **Select installation type** page, click **Next**.

4. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.

5. On the **Select server roles** page, select **DNS Server**.

6. When the Add Roles and Features Wizard appears, click **Add Features**, and then click **Next**.

7. On the **Select Features** page, click **Next**.

8. On the **DNS Server** page, click **Next**.

9. On the **Confirm installation selections** page, click **Install**.

10. On the **Installation progress** page, when the "Installation succeeded" message appears, click **Close**.

### ▶ Task 5: Verify replication of the Adatum.com Active Directory®–integrated zone

1. On LON-SVR1, in the Server Manager console, click **Tools**.

2. On the list of tools, click **DNS**.

3. In the DNS Manager console, expand **LON-SVR1**, and then expand **Forward Lookup Zones**.

   This container is probably empty.

4. Switch back to **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.

5. In the **Active Directory Sites and Services** console, expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, expand **LON-DC1**, and then click **NTDS Settings**.

6. In the right pane, right-click the **LON-SVR1** replication connection, and select **Replicate Now**.

**Note:** If you receive an error message, proceed to the next step, and then retry this step after 3-4 minutes. If this retry fails, wait a few more minutes, and then try again.

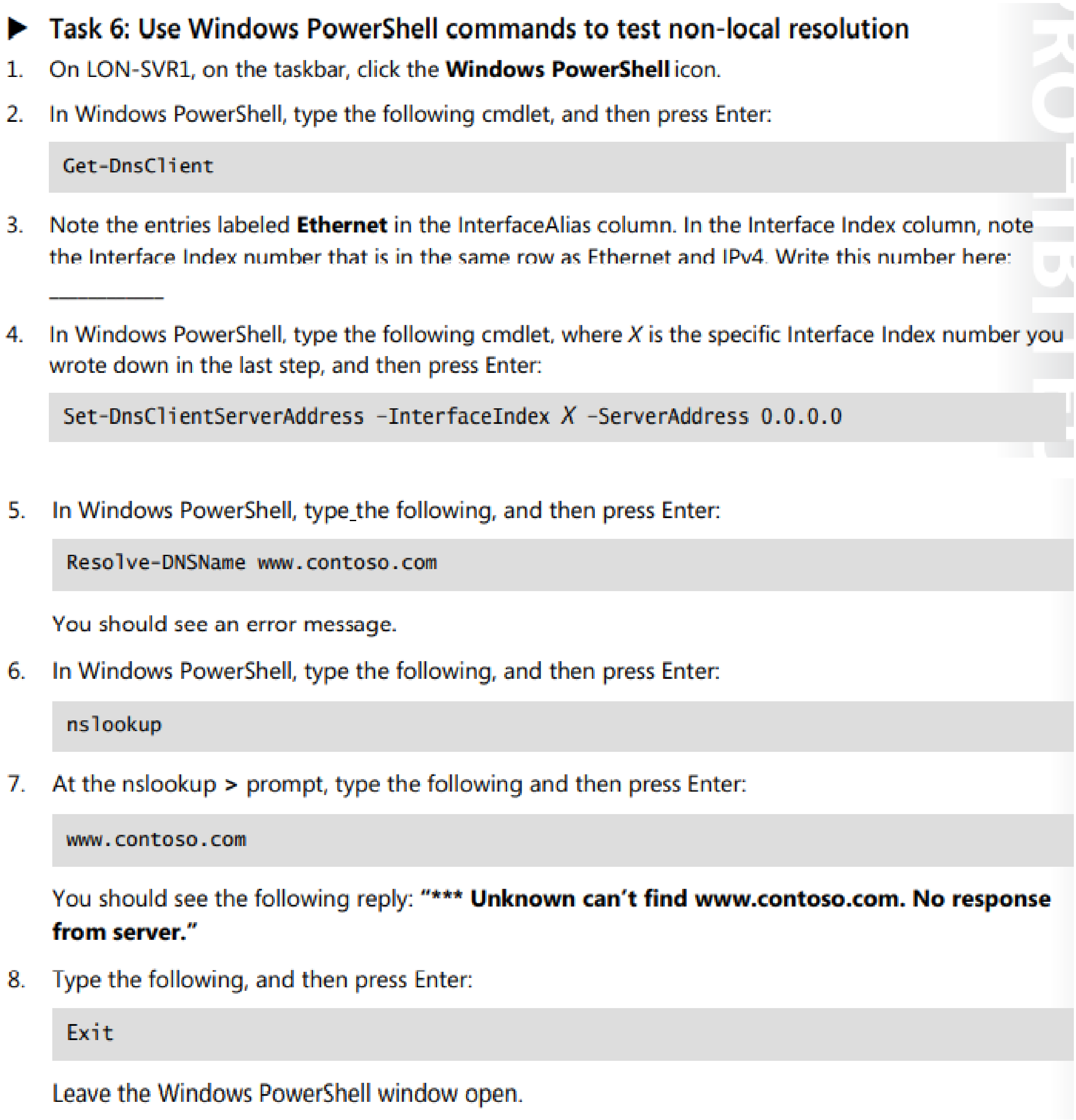
7. In the navigation pane, expand **LON-SVR1**, and then click **NTDS Settings**.

8. In the right pane, right-click the **LON-DC1** replication connection, click **Replicate Now**, and then click **OK**.

9. Switch back to the DNS Manager console, right-click **Forward Lookup Zones**, and then click **Refresh**.

10. Ensure that both the **_msdcs.Adatum.com** and **Adatum.com** containers display.

11. Close DNS Manager.



### ▶ Task 6: Use Windows PowerShell commands to test non-local resolution

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
2. In Windows PowerShell, type the following cmdlet, and then press Enter:

   ```
   Get-DnsClient
   ```

3. Note the entries labeled **Ethernet** in the InterfaceAlias column. In the Interface Index column, note the Interface Index number that is in the same row as Ethernet and IPv4. Write this number here:

   __________

4. In Windows PowerShell, type the following cmdlet, where *X* is the specific Interface Index number you wrote down in the last step, and then press Enter:

   ```
   Set-DnsClientServerAddress –InterfaceIndex X -ServerAddress 0.0.0.0
   ```

5. In Windows PowerShell, type_the following, and then press Enter:

   ```
   Resolve-DNSName www.contoso.com
   ```

   You should see an error message.

6. In Windows PowerShell, type the following, and then press Enter:

   ```
   nslookup
   ```

7. At the nslookup **>** prompt, type the following and then press Enter:

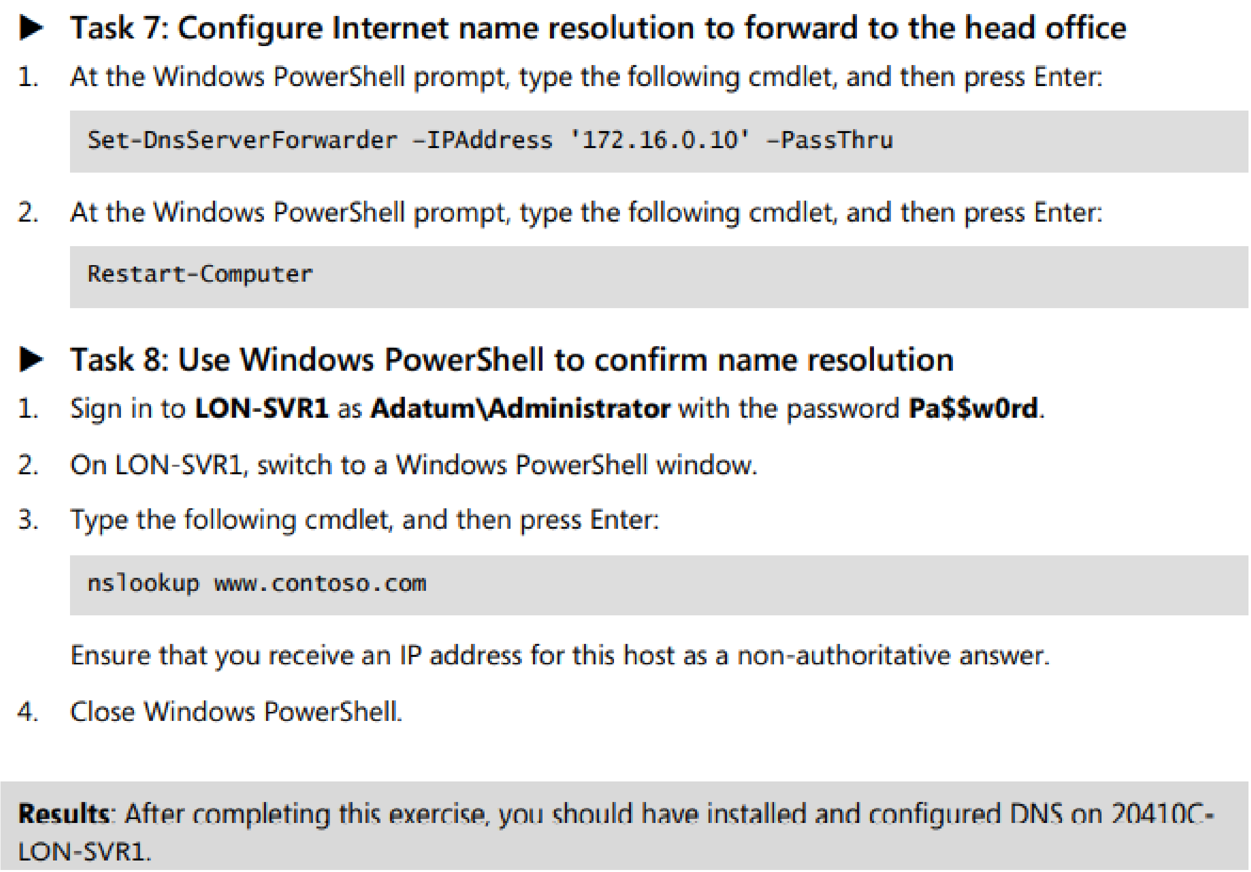
   ```
   www.contoso.com
   ```

   You should see the following reply: **"*** Unknown can't find www.contoso.com. No response from server."**

8. Type the following, and then press Enter:

   ```
   Exit
   ```

   Leave the Windows PowerShell window open.



### ▶ Task 7: Configure Internet name resolution to forward to the head office

1. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
Set-DnsServerForwarder -IPAddress '172.16.0.10' -PassThru
```

2. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
Restart-Computer
```

### ▶ Task 8: Use Windows PowerShell to confirm name resolution

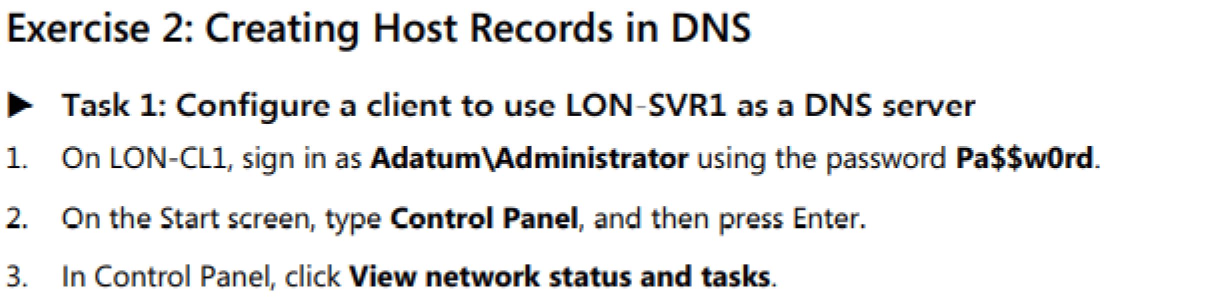
1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-SVR1, switch to a Windows PowerShell window.
3. Type the following cmdlet, and then press Enter:

```
nslookup www.contoso.com
```

   Ensure that you receive an IP address for this host as a non-authoritative answer.

4. Close Windows PowerShell.

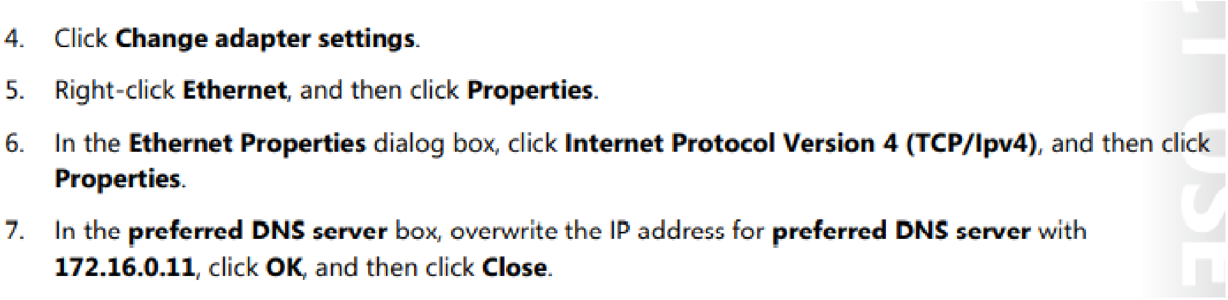
**Results**: After completing this exercise, you should have installed and configured DNS on 20410C-LON-SVR1.



## Exercise 2: Creating Host Records in DNS

### ▶ Task 1: Configure a client to use LON-SVR1 as a DNS server

1. On LON-CL1, sign in as **Adatum\Administrator** using the password **Pa$$w0rd**.
2. On the Start screen, type **Control Panel**, and then press Enter.
3. In Control Panel, click **View network status and tasks**.



4. Click **Change adapter settings**.
5. Right-click **Ethernet**, and then click **Properties**.
6. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 4 (TCP/Ipv4)**, and then click **Properties**.
7. In the **preferred DNS server** box, overwrite the IP address for **preferred DNS server** with **172.16.0.11**, click **OK**, and then click **Close**.

### ▶ Task 2: Create several host records for web apps in the Adatum.com domain

1. On LON-DC1, in the Server Manager console, click **Tools**, and then click **DNS**.
2. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, configure the following settings:
    - Name: **www**
    - IP address: **172.16.0.200**
5. Click **Add Host**, and then click **OK**.
6. In the **New Host** window, configure the following settings:
    - Name: **ftp**
    - IP address: **172.16.0.201**
7. Click **Add Host**, click **OK**, and then click **Done**.

### ▶ Task 3: Verify replication of new records to LON-SVR1

1. On LON-SVR1, in the Server Manager console, click **Tools**, and then click **DNS**.
2. In the DNS Manager console, expand **LON-SVR1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Ensure that both **www** and **ftp** resource records display. It might take several minutes for the records to display.

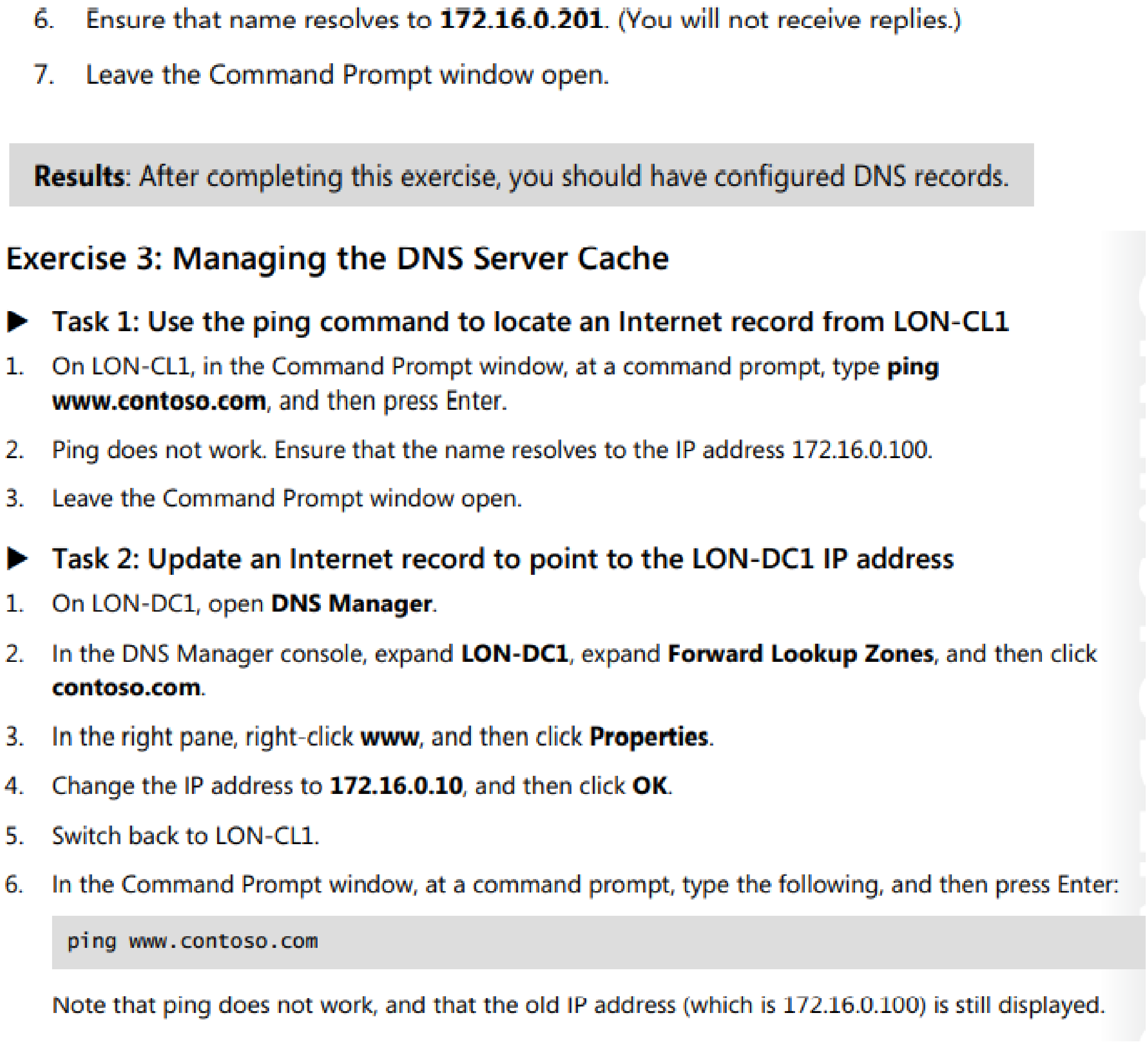
**Note:** If the **www** and **ftp** resource records do not display within several minutes, right-click **Adatum.com**, and then click **Refresh**.

### ▶ Task 4: Use the ping command to locate new records from LON-CL1

1. On LON-CL1, on the taskbar, right-click the **Windows** icon, and then click **Run**.
2. In the Run pop-up window, in the **Open** text box, type **cmd**, and then press Enter.
3. In the Command Prompt window, at a command prompt, type **ping www.adatum.com**, and then press Enter.
4. Ensure that the name resolves to **172.16.0.200**.

**Note:** You will not receive replies.

5. At a command prompt, type **ping ftp.adatum.com**, and then press Enter.



6. Ensure that name resolves to **172.16.0.201**. (You will not receive replies.)

7. Leave the Command Prompt window open.

**Results**: After completing this exercise, you should have configured DNS records.

## Exercise 3: Managing the DNS Server Cache

### ▶ Task 1: Use the ping command to locate an Internet record from LON-CL1

1. On LON-CL1, in the Command Prompt window, at a command prompt, type **ping www.contoso.com**, and then press Enter.

2. Ping does not work. Ensure that the name resolves to the IP address 172.16.0.100.

3. Leave the Command Prompt window open.

### ▶ Task 2: Update an Internet record to point to the LON-DC1 IP address

1. On LON-DC1, open **DNS Manager**.

2. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **contoso.com**.

3. In the right pane, right-click **www**, and then click **Properties**.

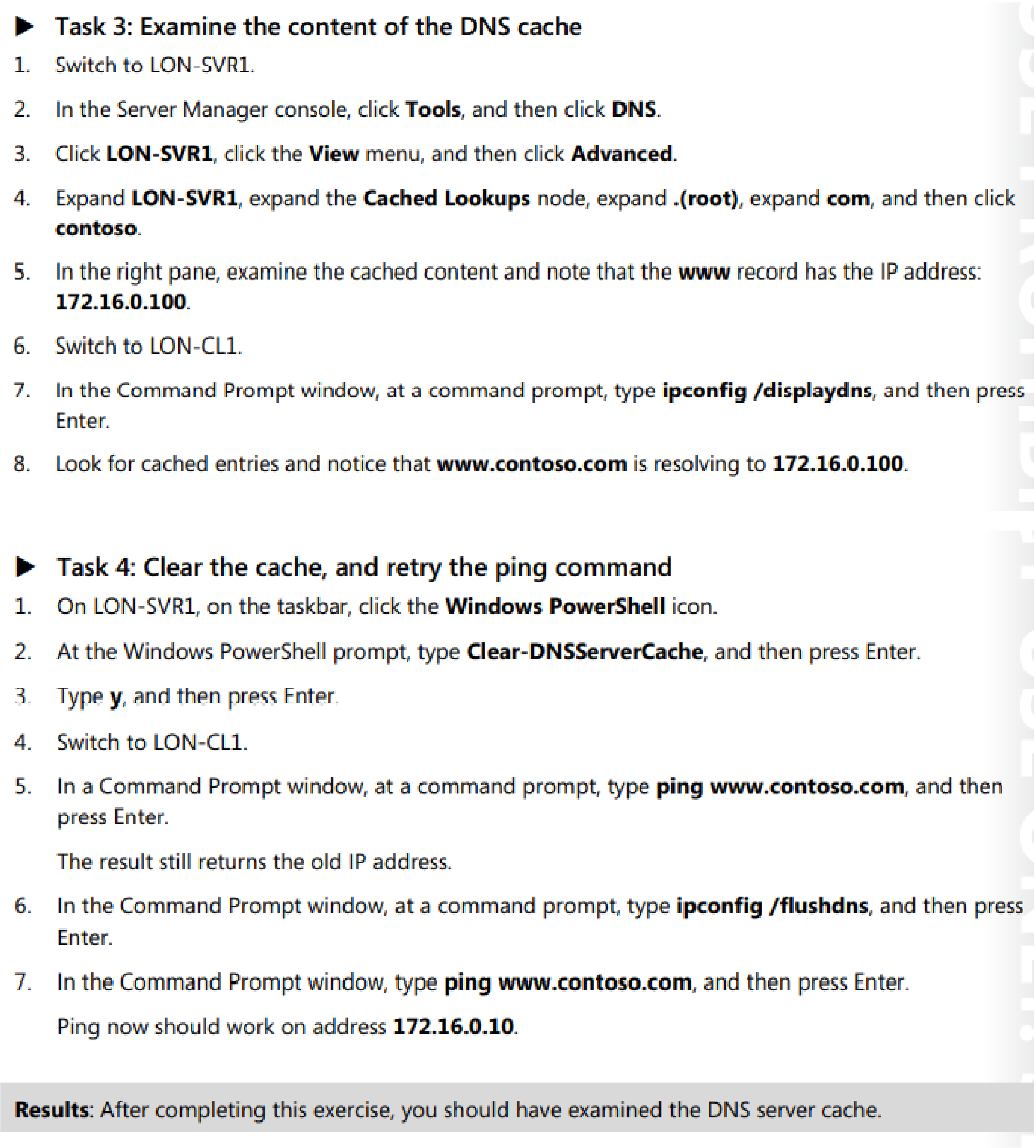
4. Change the IP address to **172.16.0.10**, and then click **OK**.

5. Switch back to LON-CL1.

6. In the Command Prompt window, at a command prompt, type the following, and then press Enter:

```
ping www.contoso.com
```

Note that ping does not work, and that the old IP address (which is 172.16.0.100) is still displayed.



### ▶ Task 3: Examine the content of the DNS cache

1. Switch to LON-SVR1.
2. In the Server Manager console, click **Tools**, and then click **DNS**.
3. Click **LON-SVR1**, click the **View** menu, and then click **Advanced**.
4. Expand **LON-SVR1**, expand the **Cached Lookups** node, expand **.(root)**, expand **com**, and then click **contoso**.
5. In the right pane, examine the cached content and note that the **www** record has the IP address: **172.16.0.100**.
6. Switch to LON-CL1.
7. In the Command Prompt window, at a command prompt, type **ipconfig /displaydns**, and then press Enter.
8. Look for cached entries and notice that **www.contoso.com** is resolving to **172.16.0.100**.

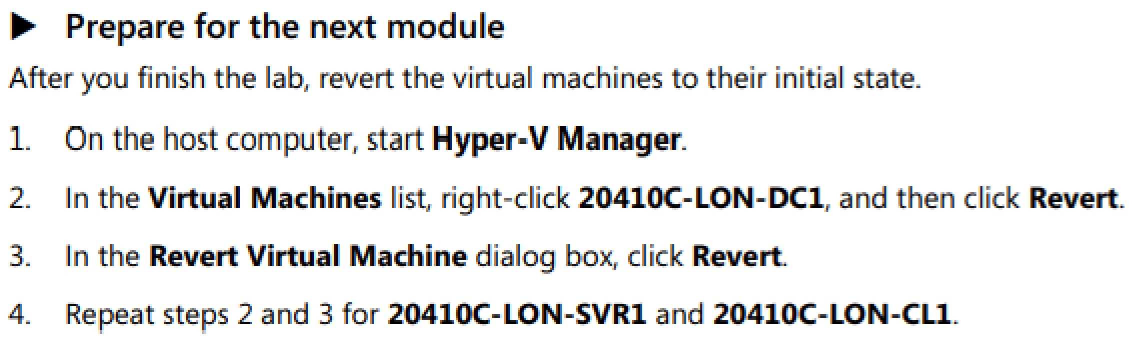
### ▶ Task 4: Clear the cache, and retry the ping command

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type **Clear-DNSServerCache**, and then press Enter.
3. Type **y**, and then press Enter.
4. Switch to LON-CL1.
5. In a Command Prompt window, at a command prompt, type **ping www.contoso.com**, and then press Enter.

   The result still returns the old IP address.
6. In the Command Prompt window, at a command prompt, type **ipconfig /flushdns**, and then press Enter.
7. In the Command Prompt window, type **ping www.contoso.com**, and then press Enter.

   Ping now should work on address **172.16.0.10**.

**Results**: After completing this exercise, you should have examined the DNS server cache.



### ▶ Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410C-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410C-LON-SVR1** and **20410C-LON-CL1**.