Microsoft

Administering Windows Server 2012 R2

Exam Ref 70-411

Charlie Russel

Microsoft

Exam Ref 70-411: Administering Windows Server 2012 R2

Charlie Russel

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2014940584
ISBN: 978-0-7356-8479-9

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Brian Svidergol
Cover: Twist Creative • Seattle

Contents at a glance

This page intentionally left blank

Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

This page intentionally left blank

Introduction

This book is written for IT professionals who want to earn the MCSA: Windows Server 2012 certification. This certification includes three exams:

- **70-410** Installing and Configuring Windows Server 2012
- **70-411** Administering Windows Server 2012
- **70-412** Configuring Advanced Windows Server 2012 Services

Exam 70-411, the focus of this book, serves as the middle exam in the path to the Windows Server 2012 MCSA for those who are not currently Microsoft certified in an earlier version of Windows Server. This book is therefore written specifically for IT professionals who want to demonstrate that they have the primary set of Windows Server 2012 skills, relevant across multiple solution areas in a business environment, to reduce IT costs and deliver more business value. Starting in January, 2014, this exam covers topics that include new features and capabilities introduced in Windows Server 2012 R2.

The three exams—Exam 70-410, Exam 70-411, and Exam 70-412—allow you to earn the Windows Server 2012 MCSA from scratch, without any prior certification. Together, these three exams include 18 domains of broader skills and 62 more specific objectives. Because the exams are intended for individuals who haven't yet earned Windows Server certification, the exams test new features in Windows Server 2012 as well as older features that haven't changed since Windows Server 2008 or even earlier.

The 70-411 exam tests six domains, and 22 objectives that comprise the core knowledge needed to administer a Windows Server 2012 R2 infrastructure.

In order to create a book that is a manageable study tool, we've focused on covering primarily the new features and capabilities of Windows Server 2012 R2, while not ignoring likely test subjects that were introduced in earlier versions of Windows Server.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible for us to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in the book to find more information—and then take the time to research and study the topic. Valuable information is available on MSDN, TechNet, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premise and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*.

Acknowledgments

As only writers can fully appreciate, no book ever makes it into a reader's hands without the work of many, many people, some of whom I'll never know, but all of whose efforts I greatly appreciate. Of those I do know, I'd like to sincerely thank Anne Hamilton and Karen Szall at Microsoft Press for their long-standing support and friendship. Gaby Kaplan and Dave Bishop at Microsoft for patiently taking my "bug" reports on Windows PowerShell documentation without ever once suggesting that the problem might be self-inflicted; Jeff Riley at Box Twelve Communications for his unflagging attention to keeping the project on course while working around and through whatever came our way; Rich Kershner for his excellent design and layout skills, and especially for saving me from the consequences of my own actions; Nancy Sixsmith for her light, but highly competent editing; Brian Svidergol for his meticulous technical review; and Angie Martin for creating an outstanding Index that helps you quickly find what you're looking for, no matter how obscure the topic.

I'd also like to sincerely thank two of my fellow Microsoft MVPs, Karen McCall and Jay Freedman. Their invaluable assistance with creating a Microsoft Word macro rescued me from a significant annoyance. I really, really appreciated their help. They exemplify the spirit of MVPs around the world and in every discipline, who give of their time and expertise unstintingly to make life better for the computing community.

Finally, my Research and Support Department, headed by Sharon Crawford, who came out of retirement to dig in and help when I really needed it. Her team includes Spuds Trey, Boots Khatt, and Sir William Wallace who put in especially long hours of support. I couldn't have done it without them.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections on the Errata & Updates tab of the book page at:

http://aka.ms/ER411R2

If you discover an error that is not already listed, please submit it to us at the same page.

For additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority and your feedback is our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

This page intentionally left blank

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your "at home" preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

This page intentionally left blank

This page intentionally left blank

CHAPTER 3

Configure network services and access

This chapter covers essential network technologies that will play an important part in the exam: the Domain Name System (DNS); Virtual Private Networks (VPNs) and routing; and DirectAccess, which enables remote domain-joined computers to be managed by the same tools you use to manage locally connected computers, while optionally providing users who work remotely a seamless experience that allows them to work remotely as easily as in the office.

Objectives in this chapter:

- Objective 3.1: Configure DNS zones
- Objective 3.2: Configure DNS records
- Objective 3.3: Configure virtual private network (VPN) and routing
- Objective 3.4: Configure DirectAccess

Objective 3.1: Configure DNS zones

There are three basic types of DNS zones: primary, secondary, and stub. Primary zones can be Active Directory-integrated or can be conventional, stand-alone primary zones. A primary zone is a zone hosted on the DNS server that is both authoritative for the zone and the primary point of storage for the zone. The zone data can be hosted in Active Directory Domain Services (AD DS) or in a local file on the DNS server.

Secondary zones contain all the information that a primary zone contains, but get their information by transferring zone information from other DNS servers. Changes to DNS records can't originate in a secondary zone, and a secondary zone is never authoritative for the zone.

Stub zones are zones that contain only information about the servers that are authoritative for the zones. Stub zones are useful for distributing information about where the full information for a zone can be found, but don't have all the zone data.

Beginning with Windows Server 2012, there is full Windows PowerShell parity with the user interface and the legacy dnscmd.exe command-line tool. There are two Windows PowerShell modules that support DNS: DnsClient, and DnsServer.

This objective covers how to:

- Configure primary and secondary zones
- Configure stub zones
- Configure conditional forwards
- Configure zone and conditional forward storage in Active Directory
- Configure zone delegation
- Configure zone transfer settings
- Configure notify settings

Configuring primary and secondary zones

A primary DNS zone is required for DNS functionality and name resolution of any domain name. A primary DNS zone is both authoritative for the zone and the primary point of storage for the zone. Secondary zones are not required and not authoritative, but are useful to reduce network traffic and provide faster name resolution, especially when not using an Active Directory-integrated primary zone.

Configuring primary DNS zones

Primary DNS zones can be both forward lookup zones and reverse lookup zones. The most common use of a forward lookup zone is to translate a device name into the IP address that is represented by that name. A reverse lookup zone is used to obtain the device name when you only know the device's IP address.

The zone data can be hosted in AD DS or in a local file on the DNS server. If stored in a local file, it is in the %windir%\System32\Dns directory on the DNS server. The file name is *zonename*.dns where *zonename* is the name of the DNS zone.

A forward lookup zone, such as treyresearch.net, is composed of records of the names of devices in the treyresearch.net namespace and their corresponding IP addresses. If a client computer wants to connect to trey-dc-02.treyresearch.net, it requests the IP address for trey-dc-02 from the client's primary DNS server. If that server hosts the record, it replies immediately. If it doesn't, it either forwards that request to a server on its forwarders list, or looks up who the authoritative DNS server is for treyresearch.net and queries that server for the information and then returns the answer to the client that asked for the information in the first place.

A reverse lookup zone enables clients to look up the name of a device when all they know is the IP address for the device. So if I want to know the computer associated with

192.168.10.2, I would look it up on my local DNS server and it would reply immediately if it hosted the 10.168.192.in-addr.arpa zone. If my local DNS server didn't host the zone, it would forward the request to one of its forwarders.

To configure a new primary zone, use either the DNS Management console (dnsmgmt.msc) or Windows PowerShell. To create a new primary forward lookup zone for TailspinToys.com, follow these steps:

1. Open the DNS Manager console.
2. Expand the server you are adding the zone to and right-click Forward Lookup Zones.
3. Select New Zone from the menu to open the New Zone Wizard.
4. Click Next on the Welcome page and select Primary Zone.
5. If running the New Zone Wizard on a writeable domain controller, you can select the Store The Zone In Active Directory check box if you want to store the zone in Active Directory or clear the check box to use conventional files (see Figure 3-1).

FIGURE 3-1 The New Zone Wizard

6. If storing the zone in Active Directory, click Next and specify which DNS servers to replicate the zone to, as shown in Figure 3-2. (Skip this if running zone files instead of AD DS-integrated zones.)

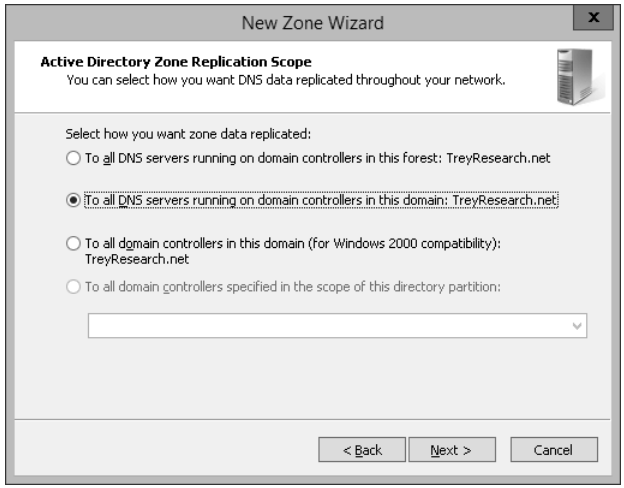


FIGURE 3-2 The Active Directory Zone Replication Scope page of the New Zone Wizard

7. Click Next and enter the Zone Name. Click Next again.
8. On the Zone File page of the New Zone Wizard, select Create A New File With This File Name and click Next. (Skip this step if this zone will be an Active Directory-integrated zone.)
9. Select whether to allow dynamic updates. If the zone is stored in Active Directory you have the option of using only secure dynamic updates, as shown in Figure 3-3.

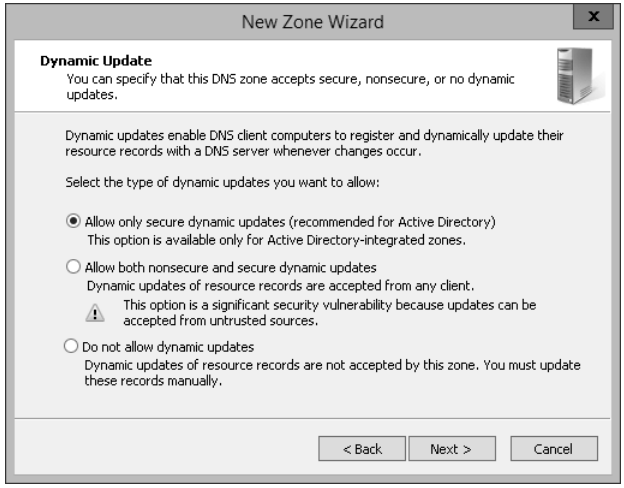


FIGURE 3-3 The Dynamic Update page of the New Zone Wizard

10. Click Next and then Finish to complete the wizard and create the primary DNS forward lookup zone.

To create a primary forward lookup zone by using Windows PowerShell, use the Add-DnsServerPrimaryZone cmdlet. To create an Active Directory-integrated primary zone for TailspinToys.com that allows only secure dynamic updates and is replicated to the entire Forest, use the following command:

```
Add-DnsServerPrimaryZone -Name 'TailspinToys.com' `
                         -ReplicationScope 'Forest' `
                         -DynamicUpdate 'Secure'
```

To create a reverse lookup zone, use the -NetworkID parameter. For example, use this command:

```
Add-DnsServerPrimaryZone -NetworkID 192.168.10.0/24 `
                         -ReplicationScope 'Forest' `
                         -DynamicUpdate 'Secure'
```

To create a file-based primary DNS zone for TailspinToys.com, use the following command:

```
Add-DnsServerPrimaryZone -Name 'TailspinToys.com' `
                         -ZoneFile 'TailspinToys.com.dns' `
                         -DynamicUpdate 'None'
```

EXAM TIP

The Windows PowerShell commands to create a DNS zone are fairly straightforward, but there are a couple of places that can easily create problems for the careless exam taker. For example, the -ReplicationScope parameter can't be used with the -ZoneFile parameter because zone files are used for storage only when the zone is not integrated into Active Directory and replication is possible only for an Active Directory-integrated zone. Another possible trip point is the -DynamicUpdate parameter. You can't have secure updates in a file-based DNS zone.

Configuring secondary zones

Secondary DNS zones can be both forward lookup zones and reverse lookup zones. The most common use of a forward lookup zone is to translate a device name into the IP address that is represented by that name. A reverse lookup zone is used to obtain the device name when you only know the device's IP address.

Secondary DNS zones depend on transferring the data for the zone from another DNS server. That other DNS server must have enabled zone transfers.

To create a secondary forward lookup zone, follow these steps:

1. Open the DNS Manager console.
2. Expand the server you are adding the zone to and right-click Forward Lookup Zones.
3. Select New Zone from the menu to open the New Zone Wizard.

4. Click Next on the Welcome page and select Secondary Zone.

5. On the Zone Name page, enter the name of the zone you want to create a secondary zone of, as shown in Figure 3-4, and then click Next.

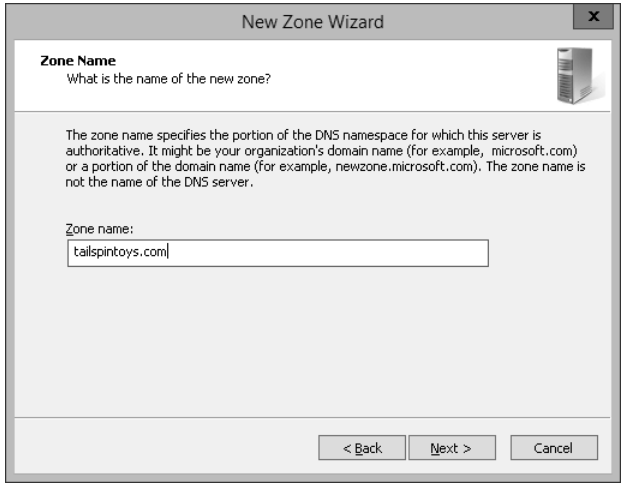


FIGURE 3-4 The Zone Name page of the New Zone Wizard

6. Enter the fully qualified domain name (FQDN) or IP address of the primary DNS server or other Master Server for the zone. You can enter an IPv4 or IPv6 address, or both.

EXAM TIP

The Master Server that you specify when creating a secondary DNS zone is usually the primary DNS server for the zone, especially when referencing an Active Directory-integrated zone, but that isn't a requirement. A secondary DNS server can act as a Master Server for other secondary servers.

7. If the IP address is correct, and the Master DNS server has enabled zone transfers to the secondary server, you'll see a green check mark, as shown in Figure 3-5. If not, you see a red X and you'll have to correct the issue before the zone transfer occurs.

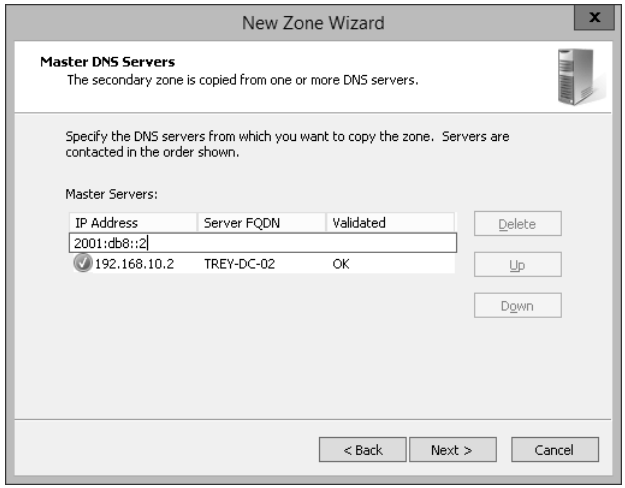


FIGURE 3-5 The Master DNS Servers page of the New Zone Wizard

8. Click Next and then Finish to create the secondary zone, as shown in Figure 3-6.

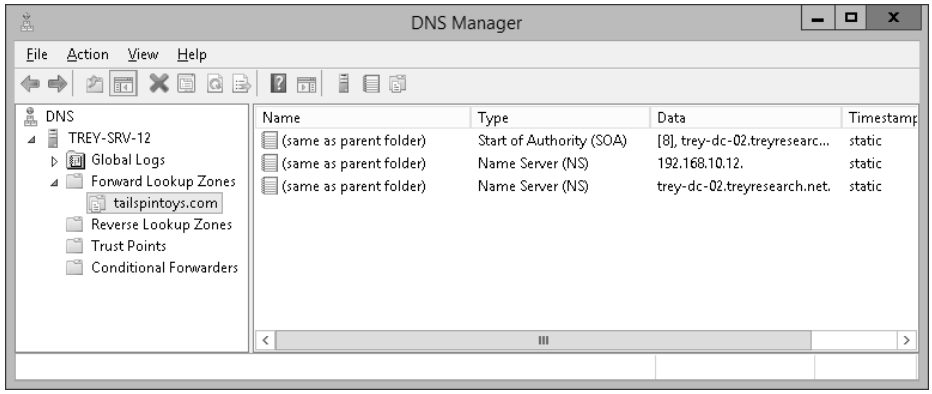


FIGURE 3-6 The DNS Manager console

To create a reverse lookup secondary zone, use the same procedure. There is no difference in the procedure regardless of whether the primary zone is Active Directory-integrated or file-based.

To create a new secondary zone at the command line by using Windows PowerShell, use the Add-DnsServerSecondaryZone cmdlet. For example:

```
Add-DnsServerSecondaryZone -Name 10.168.192.in-addr.arpa `
                           -ZoneFile "10.168.192.in-addr.arpa.dns" `
                           -MasterServers 192.168.10.2,2001:db8::2
```

If there is a problem with the zone transfer, the zone will still be created, and you can correct the issue and then reinitiate the transfer. (A failed zone transfer looks like Figure 3-7.) Correct the source of the problem and then reinitiate the transfer by right-clicking the failing zone and selecting Transfer From Master from the menu.

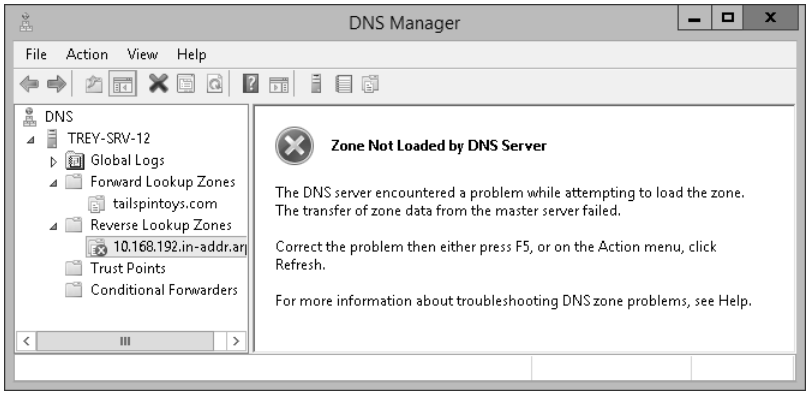


FIGURE 3-7 The DNS Manager console showing a failed initial zone transfer

EXAM TIP

Although not explicitly called out in the objective for this exam, there is one other way to create a primary or secondary DNS zone: convert an existing zone to a different type. So, for example, you can convert a file-based primary zone to a secondary zone as long as another primary zone exists. And you can convert a secondary zone to a primary zone as long as the creation doesn't result in more than one file-based primary zone.

Configuring stub zones

Stub DNS zones are zones that contain only data about a zone's name servers, without maintaining all the data for the entire zone. Stub zones are a useful way, for example, to keep track of the currently authoritative servers for a child zone without maintaining the full records of the child zone. Unlike secondary zones, stub zones contain only the records for the name servers of the zone. Also, unlike secondary zones, stub zones can be Active Directory-integrated. Stub zones can be created for both forward and reverse lookup zones.

Stub zones also alleviate a significant security concern about secondary zones. Because secondary zones contain a full copy of all DNS records in the zone, they provide a potential attacker with important information that could jeopardize network security. Stub zones expose only the IP addresses of the designated name servers. Because stub zones use standard DNS queries to obtain their information, they can be used even when the zone is marked "Do not transfer."

To create a stub zone, use essentially the same procedures as creating a primary or secondary server, as detailed in the following steps:

1. Open the DNS Manager console.
2. Expand the server you are adding the zone to and right-click Forward Lookup Zones.
3. Select New Zone from the menu to open the New Zone Wizard.
4. Click Next on the Welcome page and select Stub Zone on the Zone Type page.
5. Click Next and enter the Zone Name. Click Next.
6. Accept the default value in the Create A New File With This Name box and then click Next.
7. On the Master DNS Servers page, enter the IP address or FQDN of a Master Server in the zone for which you are creating a stub, click OK, and then click OK again.

To create a stub zone at the command line by using Windows PowerShell, use the Add-DnsServerStubZone cmdlet. For example:

```
Add-DnsServerStubZone -Name TailspinToys.com `
                      -MasterServers 192.168.10.4 `
                      -ReplicationScope "Tree"
```

Configuring conditional forwards

Conditional forwards allow you to specify a specific DNS server or servers to which you can forward DNS requests based on the DNS domain for which the request is made. This is useful when you have multiple internal namespaces (such as after a merger or acquisition). By creating conditional forwards, you allow DNS requests to stay internal without having to completely take over the DNS server role or create secondary zones. For example, if the DNS server at 192.168.10.2, which is a DNS server for the TreyResearch.net domain, receives a request for the address of tail-rdsh-105.tailspintoys.com, the DNS server would first look to see whether it hosted the domain or a stub for it. Failing that, it would check its cache to see whether it had already looked up the address. If it still didn't have the address, it would next forward a request to the Internet, either to a configured forwarding address or to the root DNS servers. But, if you have a conditional forwarder configured for TailspinToys.com at 192.168.10.102, it will instead send the request to the conditional forwarder.

Conditional forwarders can be maintained on an individual DNS server basis, or integrated into Active Directory and replicated. To configure a conditional forwarder, follow these steps:

1. Open the DNS Manager console.
2. Expand the server you are adding the forwarder to and right-click Conditional Forwarders.

3. Select New Conditional Forwarder from the menu to open the New Conditional Forwarder dialog box shown in Figure 3-8.

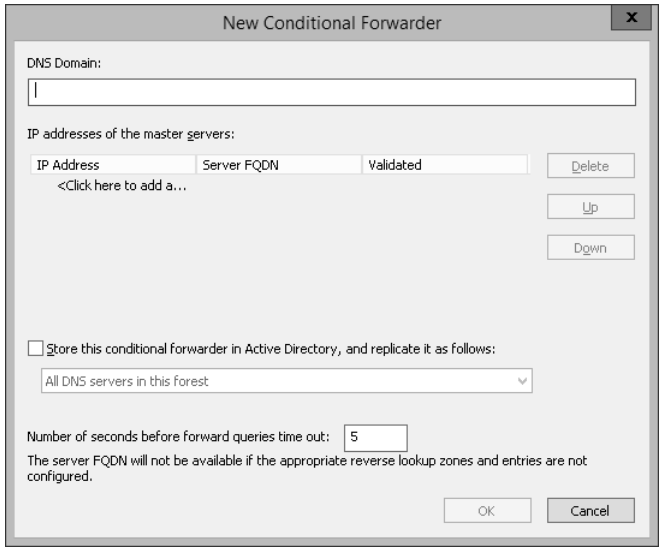


FIGURE 3-8 The New Conditional Forwarder dialog box

4. Enter the DNS domain to forward and the IP address of the target DNS server. (You can specify more than one target DNS server.)
5. Select Store This Conditional Forwarder In Active Directory, And Replicate It As Follows; then select the replication scope from the list.
6. Click OK, and the conditional forwarder is created.

You can also use the Add-DnsServerConditionalForwarderZone cmdlet. For example:

```
Add-DnsServerConditionalForwarderZone -Name treyresearch.net `
                                      -MasterServers 192.168.10.2,2001:db8::2 `
                                      -ForwarderTimeout 10 `
                                      -ReplicationScope "Forest"
```

Configuring zone and conditional forward storage in Active Directory

When you create a zone, be it a primary zone or a stub zone, or you create a forwarder, you have the option of storing the data in Active Directory by choosing Active Directory-integrated. This option is *not* available for a secondary zone. A secondary zone can never be stored in Active Directory, which leads to an exam tip, of course.

EXAM TIP

Secondary zones are a seductive solution to many situations, but they have some limitations that exam question writers are likely to take advantage of. One is that they present a potential security consideration because the entire zone is available, so be leery of questions that include security as a called-out concern where a secondary zone appears to be the answer. The other limitation is that they can't be Active Directory-replicated because they can't be stored in Active Directory. Secondary zones are always file-based zones.

Zone and conditional forwarder storage is usually set at creation time, but you have the option to change it after the fact by using either the DNS Management console. To configure an existing conditional forwarder that is not stored in Active Directory to one that is, use the DNS Management console (the operation is not supported in Windows PowerShell). The same is true for converting a file-based DNS zone into an Active Directory-integrated one. Use the DNS Management console.

So to convert a DNS file-based stub zone into an Active Directory-integrated one, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you are converting the stub zone.
3. Select the stub zone folder in the console tree and right-click.
4. Select Properties from the menu to open the Zone Properties dialog box shown in Figure 3-9.

FIGURE 3-9 The Zone Properties dialog box for tailspintoys.com

5. Click Change to open the Change Zone Type dialog box. Select the Store The Zone In Active Directory check box, as shown in Figure 3-10.

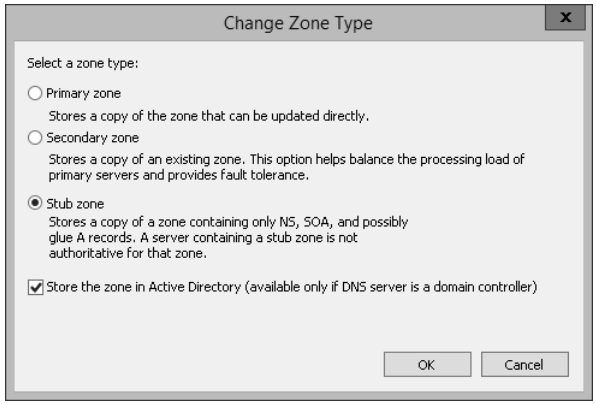


FIGURE 3-10 The Change Zone Type dialog box

6. Click OK and click Yes on the DNS prompt shown in Figure 3-11.

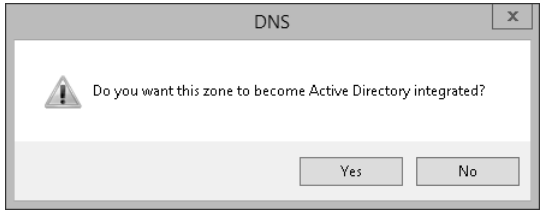


FIGURE 3-11 The DNS dialog box

7. Click OK, and the zone is converted.

EXAM TIP

With the nearly 100 percent coverage of the Windows PowerShell DNS cmdlets, you'd expect that you could convert a file-based zone to an Active Directory-integrated zone by using the appropriate Set-DnsServer* cmdlet. But that option fails with a "not supported" message. You should expect to see at least one question on the exam that revolves around that limitation.

Configuring zone delegation

Zone delegation allows you to delegate the administration of a portion of your DNS namespace, and to divide up a large zone into smaller subzones to distribute the load and improve performance.

To delegate a zone, follow these steps:

1. Open the DNS Manager console.
2. Expand the zone for which you are making the delegation.
3. Right-click the zone you want to delegate and select New Delegation from the menu.
4. On the Welcome screen, click Next. On the Delegated Domain Name page, enter the Delegated Domain, as shown in Figure 3-12, and click Next.

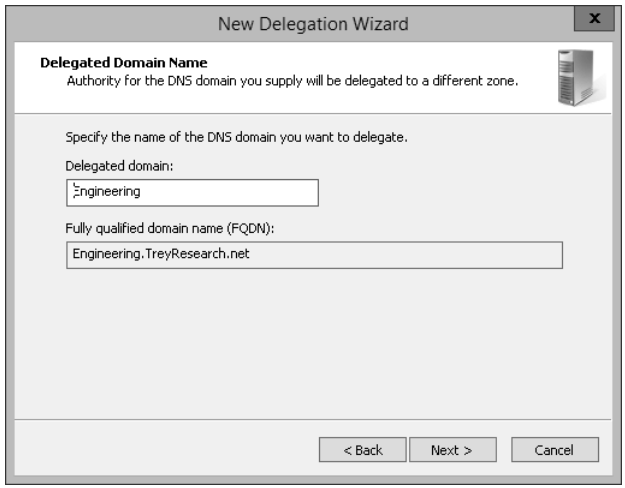


FIGURE 3-12 The New Delegation Wizard

5. On the Name Servers page, click Add and then enter the DNS name of the server that is authoritative for the zone to be delegated and click Resolve, as shown in Figure 3-13.

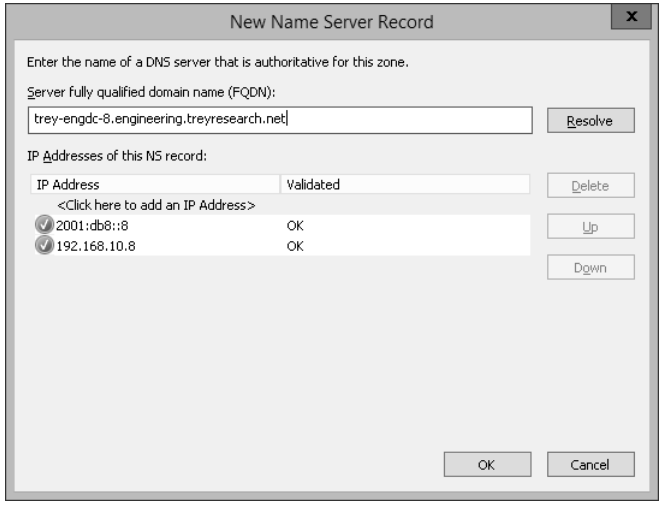


FIGURE 3-13 The New Name Server Record dialog box

6. Click OK to close the New Name Server Record dialog box and return to the Name Servers page of the New Delegation Wizard.

7. Click Next and then Finish to complete the delegation.

To create a zone delegation by using Windows PowerShell, use the Add-DnsServerZoneDelegation cmdlet. For example:

```
Add-DnsServerZoneDelegation -Name TreyResearch.net `
                            -ChildZoneName Engineering `
                            -IPAddress 192.168.10.8,2001:db8::8 `
                            -NameServer trey-engdc-8.engineering.treyresearch.net
```

Configuring zone transfer settings

You can configure the zone transfer settings that control transfers to secondary DNS zones either through the DNS Management console, or by using the Set-DnsServerPrimaryZone cmdlet.

Zone transfers can be disallowed to all servers or enabled to the following servers:

- **To Any Server** Any server can request a zone transfer, including servers that you know nothing about and don't manage or control.
- **Only To Servers Listed On The Name Servers Tab** Only designated Name Servers are allowed to request a zone transfer.
- **Only To The Following Servers** Only specified servers are allowed to request a zone transfer.

The options for the Set-DnsServerPrimaryZone are worded slightly differently, but have the same effect. The choices for the -SecureSecondaries parameter are these:

- **NoTransfer** No transfers are allowed for this zone from this server.
- **TransferAnyServer** Any server can request a zone transfer, including servers that you know nothing about and don't manage or control.
- **TransferToZoneNameServer** Only servers in the NS records for this zone are allowed to request transfers.
- **TransferToSecureServers** Only servers specified with the -SecondaryServers parameter are allowed to request a zone transfer.

To configure the zone transfer settings in the DNS Management console, right-click the zone folder on the server you want to configure and select Properties from the menu. Click the Zone Transfers tab and select the zone transfer settings appropriate for your environment, as shown in Figure 3-14.

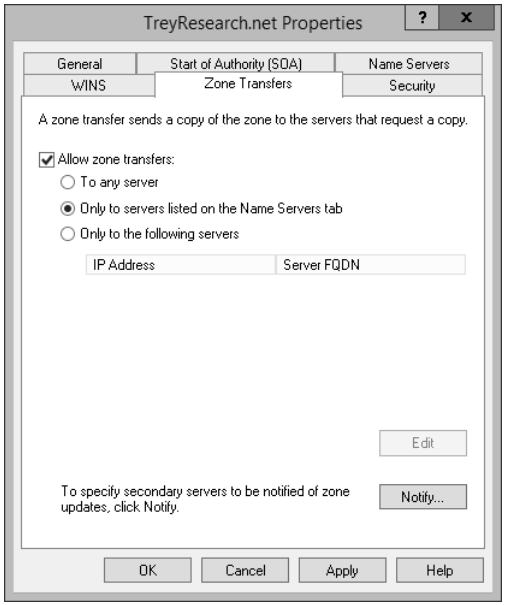


FIGURE 3-14 The Zone Transfers tab of the DNS Zone Properties dialog box

Configuring notify settings

You can configure which secondary servers are notified of changes to the zone by clicking the Notify button on the Zone Transfers tab of the DNS Manager console or by using the Set-DnsServerPrimaryZone cmdlet. The settings in the DNS Manager console are these:

- **Automatically Notify** When disabled, no notifications are sent, and secondary servers need to manually request a zone transfer or update. When enabled, the primary DNS server will automatically notify the following:
  - **Servers Listed On The Name Servers Tab** All servers for whom there are NS records in the zone are automatically notified whenever a change is made to the zone.
  - **The Following Servers** Only the specifically listed servers are automatically notified of changes in the zone. Any other servers that are allowed to request zone transfers must request the transfer manually.

The equivalent Set-DnsServerPrimaryZone parameter is the -Notify parameter, which accepts the following strings:

- **NoNotify** No notifications are sent, and secondary servers need to manually request a zone transfer or update.
- **Notify** All servers for whom there are NS records in the zone are automatically notified whenever a change is made to the zone.

- **NotifyServers** Only servers specified by the -NotifyServers parameter are automatically notified of changes to the domain. Any other servers that are allowed to request zone transfers must request the transfer manually.

Thought experiment

Designing namespace and DNS zones

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the network administrator for Trey Research. Your Forest root zone is TreyResearch.net, with child domains of Engineering and Finance, and a tree domain of TailspinToys.com. Users are located in several branch locations, as well as a central main office, and all need access to resources in both trees.

You need to design your namespace and DNS zones to provide fast and efficient lookups while maintaining as secure an environment as possible, especially in branch office locations. Further, you need to minimize network traffic.

1. **It has been suggested that you use secondary zones at the branch sites to provide a better resource lookup experience. The branch sites do not have domain controllers. What are the pluses and minuses of using secondary zones at the branch offices, and what other solutions might you consider?**
2. **There is a lot of computer name churn in the Engineering department as they continually build and rebuild clients and servers to support ever-changing project requirements. This name churn includes both static DNS names and DHCP names. What are your options to reduce the management overhead to the system administrators?**
3. **Consider the DNS churn and management overhead in the Engineering department DNS structure from a broader perspective. What other steps might you suggest?**

Objective summary

- Windows DNS Server supports primary, secondary, and stub DNS zones.
- Primary and stub DNS zones can be Active Directory-integrated.
- Both forward and reverse lookup zones are supported.
- Starting with Windows Server 2012, full Windows PowerShell support for DNS servers is included.

- Use stub zones and conditional forwarders to replace the need for secondary zones.
- Conditional forwarders provide a means to manage to which DNS server a DNS query is forwarded for specific zones.
- You can change whether a zone or conditional forward is stored in Active Directory or in files, except for secondary zones, which are always file based.
- Use DNS zone delegation to delegate administration of a portion of your DNS namespace.
- Zone transfers are disallowed unless explicitly allowed.

Objective review

1. You need to create a new primary forward lookup zone for Engineering.TreyReseach.net. The zone should have its data stored in Active Directory and be available to all domain controllers in the domain. What Windows PowerShell commands would you use?

   A. Add-DnsServerPrimaryZone -Name 'Engineering.TreyResearch.net' -zone 'engineering.treyresearch.net.dns' -replication Domain

   B. Add-DnsServerPrimaryZone -Name 'Engineering.TreyResearch.net' -zone 'engineering.treyresearch.net.dns' -replication Forest

   C. Add-DnsServerPrimaryZone -Name 'Engineering.TreyResearch.net' -replication Domain

   D. Add-DnsServerPrimaryZone -Name 'Engineering.TreyResearch.net' -replication Forest

2. You need to create a new secondary reverse lookup zone for the TreyResearch.net, which uses 192.168.10.0 - 192.168.10.255 for network addresses. The Primary zone is hosted by trey-dc-02 at 192.168.10.2. What Windows PowerShell commands would you use?

   A. Add-DnsSecondaryZone -Name 'TreyResearch.net' -NetworkID "192.168.10.0/24" -Replication Domain -Master "trey-dc-02.treyresearch.net"

   B. Add-DnsSecondaryZone -NetworkID "192.168.10.0/24" -Master 192.168.10.2 -Zone "10.168.192.in-addr.arpa"

   C. Add-DnsSecondaryZone -NetworkID "192.168.10.0/24" -Master 192.168.10.2 -Zone "0.10.168.192.in-addr.arpa"

   D. Add-DnsSecondaryZone -NetworkID "192.168.10.0/24" -Master "trey-dc-02.treyresearch.net" -Zone "10.168.192.dns"

3. You are the enterprise administrator for Trey Research. Your domain name is TreyResearch.net, and your IPv4 address range is 192.168.10.0-192.168.10.255. Your IPv6 address range is 2001:db8:10::/64. The primary domain controller for TreyResearch.net is trey-dc-02 and it hosts the Active Directory-integrated DNS. The Engineering department is migrating to use a new child domain, Engineering. TreyResearch.net, with a domain controller of trey-engdc-8. What commands would you use to delegate this domain?

   A. Add-DnsServerZoneDelegation -Name TreyResearch.net `
   -ChildZoneName Engineering `
   -IPAddress 192.168.10.8,2001:db8:10::8 `
   -NameServer trey-engdc-8.engineering.treyresearch.net

   B. Add-DnsServerZoneDelegation -Name Engineering.TreyResearch.net `
   -ChildZoneName Engineering `
   -IPAddress 192.168.10.8,2001:db8:10::8 `
   -NameServer trey-dc-02.treyresearch.net

   C. Add-DnsServerZoneDelegation -Name Engineering.TreyResearch.net `
   -ChildZoneName Engineering `
   -IPAddress 192.168.10.8,2001:db8:10::8 `
   -NameServer trey-engdc-02.engineering.treyresearch.net

   D. Add-DnsServerZoneDelegation -Name TreyResearch.net `
   -ChildZoneName Engineering `
   -IPAddress 192.168.10.8,2001:db8:10::8 `
   -NameServer trey-dc-02.engineering.treyresearch.net

Objective 3.2: Configure DNS records

DNS servers support many different kinds of resource records. For the 70-411 exam, you should understand which resource record types are supported by the Windows Server 2012 and Windows Server 2012 R2 DNS server, and how to configure those records. You should also know how to configure zone and record options, as well as how to configure round robin load balancing.

This objective covers how to:

- Create and configure DNS resource records (RR) including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records
- Configure zone scavenging
- Configure record options including Time To Live (TTL) and weight
- Configure round robin
- Configure secure dynamic updates

Creating and configuring DNS resource records

The DNS server in Windows Server supports a very wide variety of resource records, but the ones that most people have to deal with are the following:

- **A** An IPv4 host address record. The A record is a forward lookup record that translates a host name into an IPv4 address.
- **AAAA** An IPv6 host address record. The AAAA record is a forward lookup record that translates a host name into an IPv6 address.
- **CName** A canonical name record. The CName record allows the use of more than one resource record to refer to a single host.
- **MX** A Mail Exchanger record. The MX record identifies the email server for a domain. There can be multiple MX records for a domain, and they are used in order of precedence.
- **NS** A Name Server record. The NS record identifies a name server for the domain. There can be multiple NS records in a domain.
- **PTR** A pointer record. The PTR record is a reverse lookup record that translates an IP address into a host name. PTR records can be IPv4 or IPv6 addresses.
- **SOA** A Start of Authority record. The SOA record is a version number record identifying the version number of the DNS zone.
- **SRV** A Service record. The SRV record identifies the host name and port number of servers for the specified service.

All these resource records can be created or generated in the DNS Management console. They can also be created or generated by using Windows PowerShell, with the exception of the SOA record, which can't be directly manipulated by Windows PowerShell. You can use the general Add-DnsServerResourceRecord or Set-DnsServerResourceRecord for all the resource records listed except the SOA record, plus there are specific Add cmdlets for the A, AAAA, CName, MX, and PTR records.

There are a wide variety of other DNS record types, but they are rarely of concern on typical Windows networks and they are not called out in the description for this objective, so they are unlikely to be on the exam.

The procedure for setting these record types is essentially the same for all except the SOA and NS records.

Creating A resource records

The A resource record is a host address record that points to an IPv4 address. DNS clients query the DNS server with a name, and if it matches an A record, the DNS server returns an IPv4 address. You can create an A record with either the DNS Manager console or by using the Add-DnsServerResourceRecordA or Add-DnsServerResourceRecord cmdlet.

In most DHCP-managed networks, the A record is usually automatically generated when the IPv4 address is handed out to the DHCP client. This is the preferred method for DHCP

clients whose address is subject to change, but you can create a static A record by manually creating it. The problem with static records is that they need to be manually maintained if there are changes in the network. However, if there are servers with static IP addresses (as opposed to DHCP reservations), you might need to manually create the records.

To create an A record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the DNS domain name in which you want to create the record and select New Host (A Or AAAA).
4. Enter the host name in the Name box. (You don't need to enter the FQDN, just the host name.)
5. Enter the IPv4 address in the IP Address box, as shown in Figure 3-15, and select Create Associated Pointer (PTR) Record if you're using reverse lookup zones.

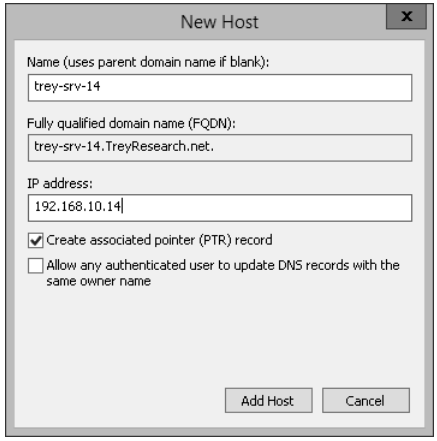


FIGURE 3-15 The New Host dialog box

6. Click Add Host to create the record.

To create the A record with Windows PowerShell, use the Add-DnsServerResourceRecordA cmdlet. For example:

```
Add-DnsServerResourceRecordA -ZoneName "TreyResearch.net" `
                             -Name trey-srv-14 `
                             -IPv4Address 192.168.10.14 `
                             -CreatePtr
```

You can also use the more general Add-DnsServerResourceRecord cmdlet to create the record. For example:

```
Add-DnsServerResourceRecord  -ZoneName "TreyResearch.net" `
                             -A `
                             -Name trey-srv-14 `
                             -IPv4Address 192.168.10.14 `
                             -CreatePtr
```

Both Windows PowerShell cmdlets create the exact same record and produce no output unless you include the -PassThru parameter. If you do include that, you see this:

```
HostName        RecordType Timestamp           TimeToLive      RecordData
--------        ---------- ---------           ----------      ----------
trey-srv-14     A          0                   01:00:00        192.168.10.14
```

Creating AAAA resource records

The AAAA resource record is a host address record that points to an IPv6 address. DNS clients query the DNS server with a name, and the DNS server returns an IPv6 address if it matches an AAAA record. You can create an AAAA record with either the DNS Manager console or by using the Add-DnsServerResourceRecordAAAA or Add-DnsServerResourceRecord cmdlet.

In most DHCP-managed networks, the AAAA record is usually automatically generated when the IPv6 address is handed out to the DHCP client. This is the preferred method for DHCP clients whose address is subject to change, but you can create a static AAAA record by manually creating it. The problem with static records is that they need to be manually maintained if there are changes in the network. However, if there are servers with static IP addresses (as opposed to DHCP reservations), you might need to manually create the records.

To create an AAAA record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the DNS domain name in which you want to create the record and select New Host (A Or AAAA).
4. Enter the host name in the Name box. (You don't need to enter the FQDN, just the host name.)
5. Enter the IPv6 address in the IP Address box, as shown in Figure 3-16, and select Create Associated Pointer (PTR) Record if you're using reverse lookup zones.

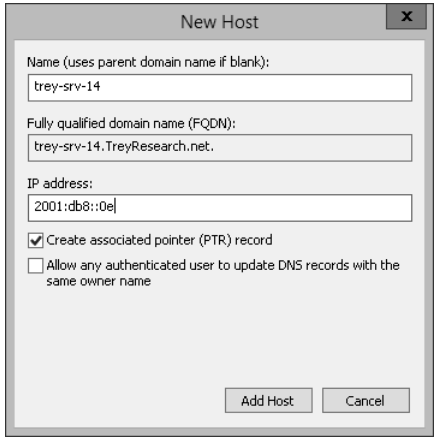


FIGURE 3-16 New Host dialog box

6. Click Add Host to create the record.
7. Click OK to acknowledge the successful creation of the record and then click Done to exit out of the New Host dialog box.

To create the AAAA record with Windows PowerShell, use the Add-DnsServerResourceRecordAAAA cmdlet. For example:

```
Add-DnsServerResourceRecordAAAA -ZoneName "TreyResearch.net" `
                                -Name trey-srv-14 `
                                -IPv6Address 2001:db8::0e `
                                -CreatePtr
```

You can also use the more general Add-DnsServerResourceRecord cmdlet to create the record. For example:

```
Add-DnsServerResourceRecord  -ZoneName "TreyResearch.net" `
                             -AAAA `
                             -Name trey-srv-14 `
                             -IPv6Address 2001:db8::0e `
                             -CreatePtr
```

Both Windows PowerShell cmdlets create the exact same record and produce no output unless you include the -PassThru parameter. If you do include that, you see this:

```
HostName        RecordType Timestamp           TimeToLive      RecordData
--------        ---------- ---------           ----------      ----------
trey-srv-14     AAAA       0                   01:00:00        2001:db8::e
```

Creating CNAME resource records

The CNAME resource record is a canonical record that adds an additional host name for a server. It is also called an Alias. The CNAME record points to a host name record and provides an alternative name for that host name. DNS clients query the DNS server

with a name, and if it matches an CNAME record, the DNS server looks up the IP address for the host name that the CNAME points to and returns an IPv4 address for that host name. You can create a CNAME record with the DNS Manager console or by using the Add-DnsServerResourceRecordCName or Add-DnsServerResourceRecord cmdlet.

CNAME records are typically used to provide an alternate host name during a transition phase or to point to specific services that run on the same server. So, for example, you might use a CNAME of ns1 to point to trey-dc-02 in the treyresearch.net zone and also use a CNAME of ns1 to point to tail-dc-102 in the tailspintoys.com zone, enabling you maintain a uniform naming convention across domains.

To create a CNAME record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the DNS domain name in which you want to create the record and select New Alias (CNAME).
4. Enter the host name in the Name box. (You don't need to enter the FQDN, just the host name.)
5. Enter the FQDN of the target host, as shown in Figure 3-17.

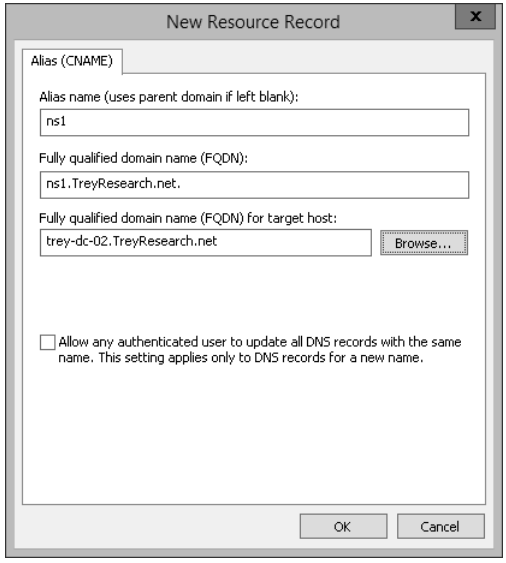


FIGURE 3-17 The New Resource Record dialog box

6. Click OK to create the record.

To create the CNAME record with Windows PowerShell, use the Add-DnsServerResourceRecordCName cmdlet. For example:

```
Add-DnsServerResourceRecordCNAME -ZoneName "TreyResearch.net" `
                                 -Name dc1 `
                                 -HostNameAlias trey-dc-02.treyresearch.net
```

You can also use the more general Add-DnsServerResourceRecord cmdlet to create the record. For example:

```
Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" `
                            -CName `
                            -Name dc1 `
                            -HostNameAlias trey-dc-02.treyresearch.net
```

Both Windows PowerShell cmdlets create the exact same record and produce no output unless you include the -PassThru parameter. If you do include that, you see this:

```
HostName RecordType Timestamp TimeToLive RecordData
-------- ---------- --------- ---------- ----------
dc1      CNAME      0         01:00:00   trey-dc-02.treyresearch.net.
```

Creating MX resource records

The MX resource record is a Mail Exchanger record that tells Simple Mail Transfer Protocol (SMTP) servers which host or hosts handle email for the domain. The MX record points to a host name record and includes a Mail Server Priority box that allows you to have backup mail servers with the email always being delivered to the mail server with the lowest value available. DNS clients query the DNS server for the MX record. If there is one or more, the DNS server returns the host names that the MX records point to, along with the priority for each server. You can create an MX record with the DNS Manager console or by using the Add-DnsServerResourceRecordMX or Add-DnsServerResourceRecord cmdlet.

To create an MX record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the DNS domain name in which you want to create the record and select New Mail Exchanger (MX).
4. Enter a Host Or Child Domain if appropriate. (In most environments, you can leave this box blank.)
5. Enter the FQDN of the mail server in the Fully Qualified Domain Name (FQDN) Of Mail Server box.

6. Enter the Mail Server Priority, as shown in Figure 3-18.

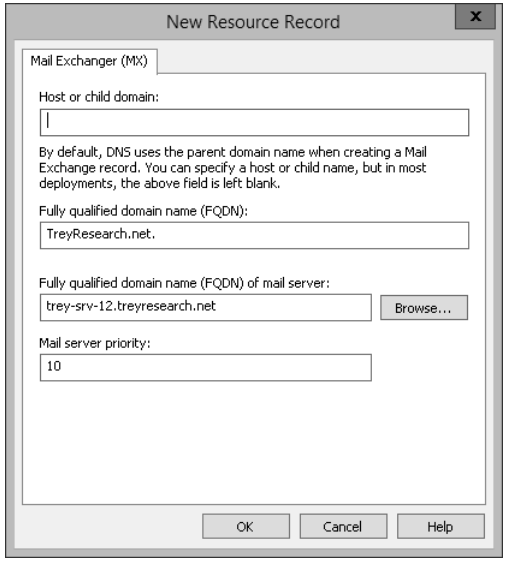


FIGURE 3-18 The New Resource Record dialog box for an MX Record

7. Click OK to create the record.

To create the MX record with Windows PowerShell, use the Add-DnsServerResourceRecordMX cmdlet. For example:

```
Add-DnsServerResourceRecordMX -ZoneName "TreyResearch.net" `
                              -Name "."  `
                              -MailExchange trey-srv-12.treyresearch.net `
                              -Preference 10
```

You can also use the more general Add-DnsServerResourceRecord cmdlet to create the record. For example:

```
Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" `
                            -Name "."  `
                            -MX
                            -MailExchange trey-srv-12.treyresearch.net `
                            -Preference 10
```

Both Windows PowerShell cmdlets create the exact same record and produce no output unless you include the -PassThru parameter. If you do include that, you see this:

```
HostName RecordType Timestamp TimeToLive RecordData
-------- ---------- --------- ---------- ----------
@        MX         0         01:00:00   [10][trey-srv-12.treyresearch.net.]
```

Creating PTR resource records

The PTR resource record is a pointer record that does a reverse lookup to point to a host name. DNS clients query the DNS server with an IP address. If it matches a PTR record, the DNS server returns the host name for that IP address. You can create a PTR record with the DNS Manager console or by using the Add-DnsServerResourceRecordPTR or Add-DnsServerResourceRecord cmdlet.

Reverse lookup zones are not required for most Windows networks, but when they are used, the PTR record is automatically generated when the IP address is handed out to the DHCP client or when the A or AAAA record is manually created. This is the preferred method, but you can create a static PTR record by manually creating it. The problem with static records is that they need to be manually maintained if there are changes in the network. However, if you don't initially create a reverse lookup zone and then decide that you need one, you might well have servers with static addresses that need manually created records.

To create PTR record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Reverse Lookup Zones. For an IPv4 address in the 192.168.10/24 network, this is the 10.168.192.in-addr.arpa zone; for an IPv6 address in the 2001:db8::/64 network, the zone is the 0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa zone.
3. Right-click the zone in which you want to create the record and select New Pointer (PTR).
4. Enter the IP address in the Host IP Address box. (You don't need to enter the FQDN, just the IP address.)
5. Enter the FQDN in the Host Name box, as shown in Figure 3-19.
6. Click OK to create the record.

To create the PTR record with Windows PowerShell, use the Add-DnsServerResourceRecordPtr cmdlet. For example:

```
Add-DnsServerResourceRecordPtr -ZoneName 10.168.192.in-addr.arpa `
                               -Name "14" `
                               -PtrDomainName "trey-srv-14.treyresearch.net"
```

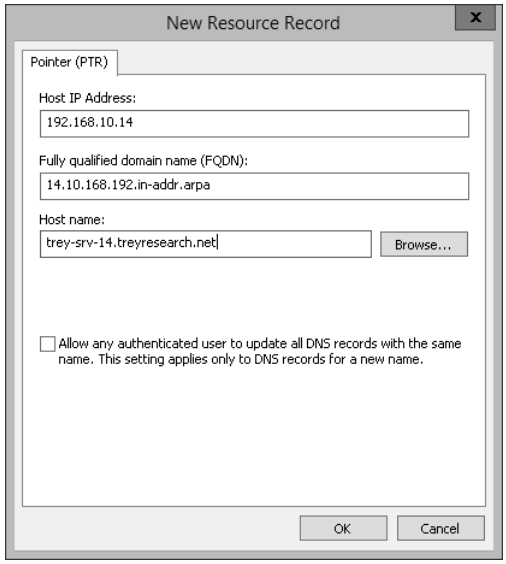


FIGURE 3-19 The New Resource Record dialog box for creating a PTR record

You can also use the more general Add-DnsServerResourceRecord cmdlet to create the record. For example:

```
Add-DnsServerResourceRecordPtr -ZoneName 10.168.192.in-addr.arpa `
                               -PTR
                               -Name "14" `
                               -PtrDomainName "trey-srv-14.treyresearch.net"
```

Both Windows PowerShell cmdlets create the exact same record, and produce no output unless you include the -PassThru parameter. If you do include that, you see the following:

```
HostName RecordType Timestamp TimeToLive RecordData
-------- ---------- --------- ---------- ----------
14       PTR        0         01:00:00   trey-srv-14.treyresearch.net.
```

Creating SRV resource records

The SRV resource record is a service location record that points to the location of key network resources. SRV records are required for AD DS domain controllers, but can also be required for other services. The necessary SRV records for domain controllers are created as part of the process of promoting a server to be a domain controller. Typically, _ldap and _kerberos SRV

records are created in the _msdcs.<domainname> zone. The _kerberos record has a protocol of _tcp and a port number of 88, as shown in Figure 3-20.

FIGURE 3-20 The Properties dialog box for the _kerberos SRV record

The _ldap record is similar to the _kerberos record, except that it uses a port of 389. You usually should not modify these records, but it might be necessary to re-create them in the case of recovery from an unplanned event. Alternately, you might want to adjust the weight and priority of individual servers providing the service to manage load.

Other services that can use SRV records typically create their own records in DNS as part of their installation process, but you might have to manually create them as well. One other Microsoft service that uses SRV records is Microsoft Exchange, which uses SRV records to allow Outlook and other clients to autodiscover the Exchange server.

You can create an SRV record with the DNS Manager console or by using the Add-DnsServerResourceRecord cmdlet. To create an SRV record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server you on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the DNS domain name in which you want to create the record and select Other New Records.
4. Select Service Locator (SRV) from the list on the Resource Record Type dialog box, as shown in Figure 3-21, and click Create Record.

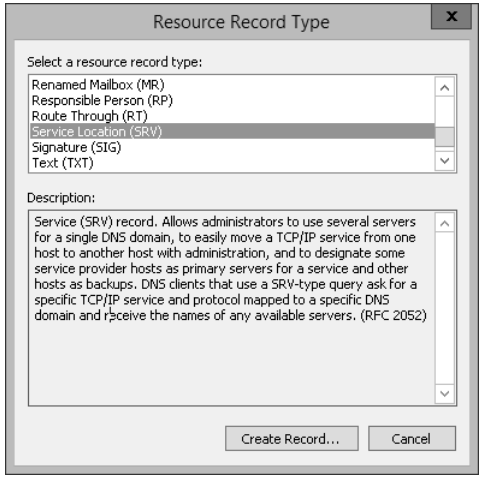


FIGURE 3-21 The Resource Record Type dialog box

5. Fill in the Service, Protocol, Priority, Weight, Port Number, and Host Offering This Service boxes on the New Resources Record dialog box, as shown in Figure 3-22.

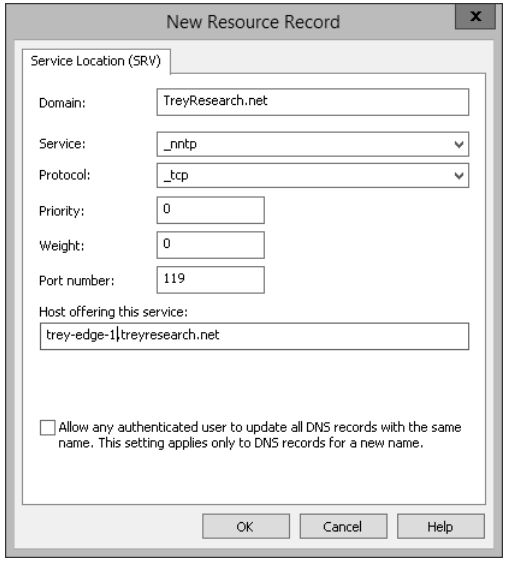


FIGURE 3-22 The New Resource Record dialog box for a new SRV record

6. Click OK to create the record.

To create the SRV record with Windows PowerShell, use the Add-DnsServerResourceRecord cmdlet with the -SRV parameter set. For example:

```
Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" `
                            -Name _nntp._tcp `
                            -SRV `
                            -DomainName "trey-edge-1.treyresearch.net" `
                            -Port 119 `
                            -Priority 0 `
                            -Weight 0 `
                            -PassThru
```

The Windows PowerShell cmdlet doesn't produce output unless you include the -PassThru parameter. If you do include it, you see the following:

```
HostName RecordType Timestamp TimeToLive RecordData
-------- ---------- --------- ---------- ----------
_nntp    SRV        0         01:00:00   [0][0][113][trey-edge-1.treyresearch.net.]
```

Creating NS resource records

The NS resource record is a name server record that identifies a name server for the domain. You can create an NS record with the DNS Manager console or by using the Add-DnsServerResourceRecord cmdlet.

NS records are usually created automatically when servers are promoted to a domain controller, but you might have to manually create the NS record.

To create an NS record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand Forward Lookup Zones.
3. Right-click the Zone Name for the zone for which you want to create an NS record and select Properties from the menu.
4. Select the Name Servers tab and click Add to open the New Name Server Record dialog box shown in Figure 3-23.
5. Enter FQDN of the new name server in the Server Fully Qualified Domain Name (FQDN) box and click the Resolve button.
6. Click OK and then OK again to create the record.

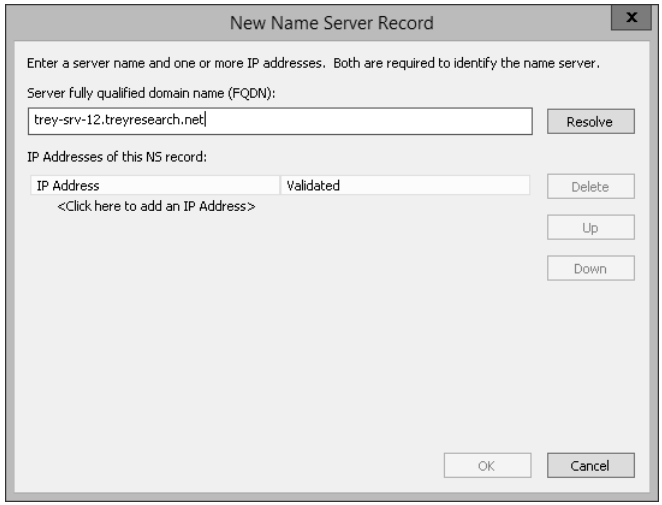


FIGURE 3-23 The New Name Server Record dialog box

To create the NS record with Windows PowerShell, use the Add-DnsServerResourceRecord cmdlet. For example:

```
Add-DnsServerResourceRecord  -ZoneName "TreyResearch.net" `
                             -NS `
                             -Name "." `
                             -NameServer trey-srv-12.treyresearch.net `
                             -PassThru
```

The Windows PowerShell cmdlet produces no output unless you include the -PassThru parameter. If you do include it, you see this:

```
HostName   RecordType Timestamp  TimeToLive RecordData
--------   ---------- ---------  ---------- ----------
@          NS         0          01:00:00   trey-srv-12.treyresearch.net.
```

EXAM TIP

The NS record is a bit different from other resource records, and it's easy to get the fields wrong with the Windows PowerShell cmdlet. The Name field needs to be "(same as parent folder)" (without the quotes), and the way to enter it is with a value of "." for the -Name parameter. There are several compelling alternatives that the exam writers might offer as distractors, but don't be seduced by them.

Configuring SOA resource records

The SOA resource record is a Start of Authority record that sets the version number of a DNS zone. Typically, this record is not manipulated manually, but is automatically incremented whenever there is a change to the zone. The version number is used to determine which zone record is authoritative if there have been DNS zone changes in more than one location.

To update a SOA record with the DNS Manager console, follow these steps:

1. Open the DNS Manager console.
2. Expand the server on which you want to create the record and then expand the Zone you want to configure.
3. Right-click the zone name and select Properties from the menu.
4. Click the Start Of Authority (SOA) tab, as shown in Figure 3-24.

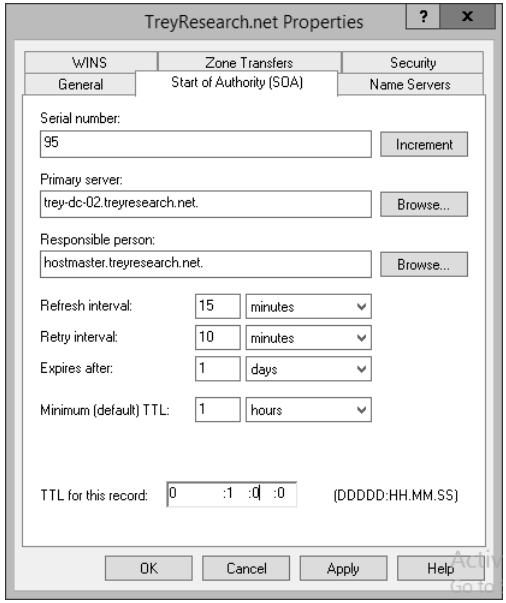


FIGURE 3-24 The Start Of Authority (SOA) tab of the zone Properties dialog box

5. Enter the host name in the Primary Server box.
6. Click Increment to increment the Serial Number for the record.
7. Set Refresh Interval, Retry Interval, Expires After, Minimum TTL, and TTL For This Record and then Click OK to update the zone.

Configuring zone scavenging

You can enable DNS scavenging and aging on a per-zone basis or for all zones on an Active Directory-integrated DNS server. To enable and configure scavenging for all zones on the server, follow these steps:

1. Open the DNS Manager console.
2. Right-click the server name and select Set Aging/Scavenging For All Zones.
3. On the Server Aging/Scavenging Properties dialog box, shown in Figure 3-25, select Scavenge Stale Resource Records.

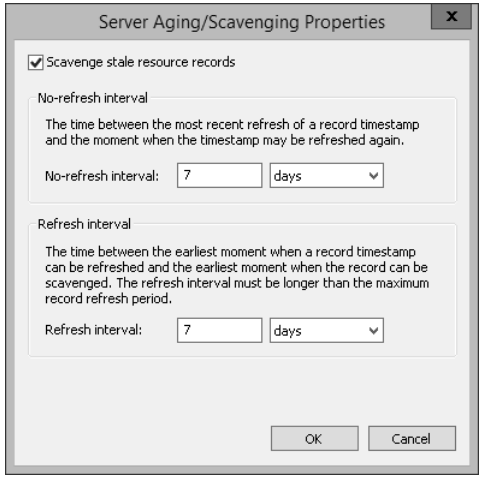


FIGURE 3-25 The Server Aging/Scavenging Properties dialog box

4. Adjust the no-refresh and refresh intervals if necessary and then click OK.
5. On the Server Aging/Scavenging Confirmation dialog box, shown in Figure 3-26, select Apply These Settings To The Existing Active Directory-Integrated Zones and then click OK.

FIGURE 3-26 The Server Aging/Scavenging Confirmation dialog box

Next, enable scavenging on at least one DNS server hosting Active Directory-integrated primary DNS zones:

6. Right-click the name of the DNS server in the console tree of the DNS Manager console and select Properties from the menu.

7. Click the Advanced tab, shown in Figure 3-27, and select Enable Automatic Scavenging Of Stale Records.

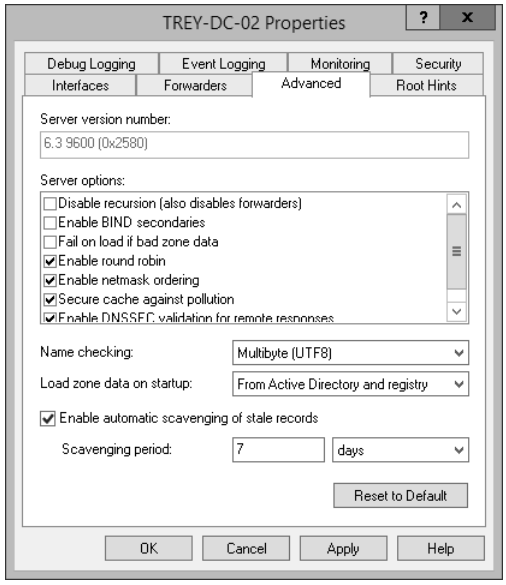


FIGURE 3-27 The Advanced tab of the DNS Server Properties dialog box

8. Set the Scavenging Period as appropriate for your environment (the default is 7 days.)

9. Click OK to close the Properties dialog box and enable automatic scavenging.

You can control which zones are subject to scavenging on a zone-by-zone basis. To enable or disable scavenging for an individual zone, follow these steps:

1. Open the DNS Manager console and expand the server name that hosts the primary zone for which you want to enable or disable scavenging.

2. Right-click the zone you want to configure and select Properties. You can set aging and scavenging on both forward lookup zones and reverse lookup zones.

3. On the General tab, click Aging to open the Zone Aging/Scavenging Properties, shown in Figure 3-28.

4. Select or clear the Scavenging Stale Resource Records check box to enable or disable scavenging for the zone.

5. If enabled, you can also set the No-Refresh Interval and Refresh Interval.

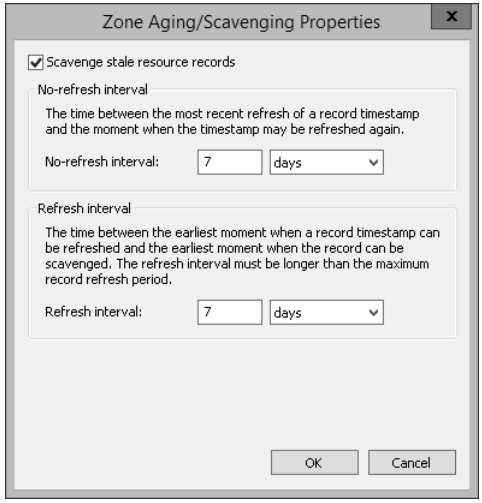


FIGURE 3-28 The Zone Aging/Scavenging Properties dialog box

6. Click OK and then OK again to close the Zone Properties dialog box.

Alternately, you can use Windows PowerShell to set the scavenging settings, by using the Set-DnsServerScavenging cmdlet. For example, to configure the settings for all zones, set a scavenging interval of three days, and enable scavenging on new zones by default, use the following command:

```
Set-DnsServerScavenging -ScavengingState:$True `
                        -ScavengingInterval 3:00:00:00 `
                        -ApplyOnAllZones `
                        -PassThru
```

This command returns the following (because the -PassThru parameter is set):

```
NoRefreshInterval  : 7.00:00:00
RefreshInterval    : 7.00:00:00
ScavengingInterval : 3.00:00:00
ScavengingState    : True
LastScavengeTime   :
```

To set the aging and scavenging for an individual zone, use Set-DnsServerZoneAging to enable aging and scavenging for a zone, and use Set-DnsServerResourceRecordAging to set a timestamp on the records in a zone and begin the aging. For example:

```
Set-DnsServerZoneAging -Name TreyResearch.net `
                       -Aging:$True `
                       -RefreshInterval 3:00:00:00
                       -NoRefreshInterval 3:00:00:00
                       -ScavengeServers 192.168.10.2
                       -PassThru
```

This command returns the following (because the -PassThru parameter is set):

```
ZoneName             : TreyResearch.net
AgingEnabled         : True
AvailForScavengeTime : 4/7/2014 10:00:00 AM
RefreshInterval      : 3.00:00:00
NoRefreshInterval    : 3.00:00:00
ScavengeServers      : 192.168.10.2
```

Next, begin the aging process on the zone with the following:

```
Set-DnsServerResourceRecordAging -ZoneName TreyResearch.net
```

Configuring record options including Time To Live (TTL) and weight

You can configure resource record options for record types that support individual configuration of options, such as SRV resource records. The combination of weight and priority control the server that will deliver specific services. So, for example, if you have multiple Network News Transfer Protocol (NNTP) servers that use SRV records, you can set both a Priority value and a Weight value. For example, assume that you have two SRV records for the service, each with a priority of 1 and each pointing to a different service provider. If one has a weight of 2, and the other a weight of 8, a query for the service will return the SRV record with the weight of 8 four times for every one time it returns the SRV record with a weight of 2.

MX resource records support a Preference setting. This is equivalent to the Priority setting on an SRV record. The record returned includes the Preference or Priority value, and the lowest Preference (MX) or Priority (SRV) value is used if the server it points to is available.

To set the weight on an SRV record, follow these steps:

1. Open the DNS Manager console and navigate to the zone that hosts the SRV record.
2. Right-click the SRV record and select Properties from the menu.
3. Enter the weight and priority in the appropriate boxes and click OK to update the record and close the Property dialog box.

To set the weight at the command line, use the DnsServerResourceRecord cmdlets. For example, to set the weight of the _nntp SRV record to 10, use the following commands:

```
$NewRRObj = $OrigRRObj = Get-DnsServerResourceRecord -Name _nntp `
   -ZoneName TreyResearch.net `
   -RRType SRV
$NewRRObj.RecordData.Weight = 20
Set-DnsServerResourceRecord -NewInputObject $NewRRObj `
   -OldInputObject $OrigRRObj `
   -ZoneName treyresearch.net
```

You can also use this same technique to set the TTL for an individual resource record. For example, to change the A record for server trey-wds-11 to have a TTL of two hours, use the following:

```
$NewRRObj = $OrigRRObj = Get-DnsServerResourceRecord -Name trey-wds-11 `
   -ZoneName TreyResearch.net `
   -RRType A
$NewRRObj.TimeToLive = [System.TimeSpan]::FromHours(2)
Set-DnsServerResourceRecord -NewInputObject $NewRRObj `
   -OldInputObject $OrigRRObj `
   -ZoneName treyresearch.net `
   -PassThru

HostName                  RecordType Timestamp            TimeToLive      RecordData
--------                  ---------- ---------            ----------      ----------
trey-wds-11               A          0                    02:00:00        192.168.10.11
```

Configuring round robin

Round robin load balancing is an easy and unsophisticated way to distribute load across a group of servers that provide the same service. The basic process is to create A or AAAA records with the same name pointing to each of the servers in the round robin. By default, round robin is enabled on Windows Server 2012 R2 DNS servers. If the service uses an SRV record, the SRV record should use that A or AAAA record name in the Host Offering This Service box.

Each time a new client requests the service or server, the DNS server returns one of the IP addresses that matches the host name queried. After clients have cached the DNS information locally, they usually won't need to request it again until the record they've cached ages out. But different clients get a different IP address in the round robin group.

Windows Server also uses netmask ordering to attempt to connect to the service or server that is closest. This proximity awareness is used to return the A or AAAA record whose IPv4 address is in the same subnet, or whose IPv6 address has the longest prefix match. When both netmask ordering and DNS round robin are enabled, round robin load balancing might not always return a load balanced address.

Configuring secure dynamic updates

Another option you can configure for resource records is what type of update is permitted. By default, Active Directory-integrated zones are set to allow only secure dynamic updates. When DNS records are created or updated by a Windows DHCP server, the update automatically updates the A or AAAA record and the PTR record. It can be further configured on the DHCP server to enable DHCP Name Protection. If DHCP Name Protection is enabled, the DHCP server attempts to register the A or AAAA and PTR records for the client, but if a different client already has the name registered on the DNS server, the new registration will fail.

Enabling Name Protection is possible only with Secure Dynamic Updates enabled. Enabling Name Protection will set the following DHCP server settings:

- DHCP Server honors requests for registration from Windows DHCP clients.
- DHCP Server dynamically updates A (or AAAA) and PTR records for non-Windows DHCP clients.
- DHCP Server discards the A (or AAAA) and PTR records when the client lease is deleted.

The Secure Updates option is set in the DNS Manager console and is set at the zone level. To change the setting, open the DNS Manager, right-click the zone you want to change, and select properties from the menu. On the General tab, select one of three options:

- **Secure Only** Only devices that are in the same DNS domain are permitted to register their DNS records.
- **Nonsecure And Secure** Any device can update a dynamic DNS record.
- **None** No dynamic updates are accepted. All DNS records must be manually maintained.

Thought experiment

Configuring round robin

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the network administrator for TreyResearch.net. Engineering users run specialized applications on a trio of dedicated Remote Desktop Session Host (RDSH) servers to reduce the need to install them on each workstation locally. Especially because there is a large amount of computer churn in the department as compute resources get scavenged for other uses. These computers are all on the same subnet, and each has a single IP address.

1. **Currently, users connect to one or another RDSH server, depending on how their client is configured. If their primary RDSH is down, they connect to one of the alternate ones manually, which doesn't provide a good user experience. How can you use DNS round robin to distribute the load across the RDSH servers and improve the user experience?**
2. **How would you configure the round robin records? (Assume that the three RDSH servers are rdsh1, rdsh2, and rdsh3.)**

Objective summary

- The DnsServer Windows PowerShell module includes cmdlets to create and manage DNS resource records.
- The Windows DNS server supports a wide variety of resource records, including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records.
- You can use the DNS Manager console or Windows PowerShell to manage DNS record options such as TTL.
- DNS resource records can be used to do basic round robin load balancing.
- Use DHCP Name Protection with DNS secure dynamic updates to ensure that you don't end up with conflicting DNS records.
- Use DNS zone scavenging and aging to remove stale records from your DNS servers.

Objective review

1. Which records do you need to create to support a new application server that uses both IPv4 and IPv6? (Choose all that apply.)
   - **A.** MX
   - **B.** SRV
   - **C.** A
   - **D.** AAAA
   - **E.** PTR
   - **F.** CNAME
2. What command should you use to create a new name server record for ns13.treyresearch.net at 192.168.10.13?
   - **A.** Add-DnsServerResourceRecord -ZoneName "treyresearch.net" -NS -Name "." -NameServer "ns13.treyresearch.net"
   - **B.** Add-DnsServerResourceRecord -ZoneName "treyresearch.net" -NS -Name "ns13" -NameServer "ns13.treyresearch.net"
   - **C.** Add-DnsServerResourceRecord -Name "treyresearch.net" -NS -NameServer "ns13.treyresearch.net"
   - **D.** Add-DnsServerResourceRecord -ZoneName "treyresearch.net" -NS -Name "ns13.treyresearch.net" -NameServer "."
3. How do you update the SOA resource record?
   - **A.** Use the Set-DnsServerResourceRecordSOA cmdlet
   - **B.** Use the Add-DnsServerResourceRecordSOA cmdlet
   - **C.** Use the DNS Manager console Properties of the zone
   - **D.** Use the DNS Manager console Properties of the server

Objective 3.3: Configure virtual private network (VPN) and routing

The traditional methods of providing remote access include dial-in modems and virtual private network (VPN) connections. Dial-in modems use standard telephone lines and hardware or software modems that enable a direct connection from a remote client to the internal network without using the Internet at all. They have the advantage that they require only an available telephone line; no Internet connection is necessary. Their disadvantages, however, include their speed—they are limited to the speed of the modem and they are hardware-intensive, requiring a dedicated bank of phone lines and modems.

By contrast, VPNs require no additional hardware beyond that required for Internet connectivity; they use the public Internet as the transmission medium. VPN remote access creates a dedicated encrypted tunnel between a client computer and a VPN endpoint computer on the internal network. VPNs, however, have some limitations of their own. The biggest is that VPNs limit the ability of the connected client to be managed.

Routing and Network Address Translation (NAT) are two technologies used by internal computers accessing the Internet. Routing controls which path a packet takes to get to its destination; NAT maps internal private IP addresses to external public addresses, enabling a single public IP address to serve for many internal devices.

Finally, Web Application Proxy is a Remote Access role service in Windows Server 2012 R2 that provides a reverse proxy that allows remote users to access web applications on the internal network from anywhere.

This objective covers how to:

- Install and configure the Remote Access role
- Implement Network Address Translation (NAT)
- Configure VPN settings
- Configure remote dial-in settings for users
- Configure routing
- Configure Web Application proxy in passthrough mode

Installing and configuring the Remote Access role

The first step of implementing VPNs and routing is installing the Remote Access role and doing the basic initial configuration.

Installing the Remote Access role

Installing the Remote Access role is the same basic process as installing any other role in Windows Server. You can install the role from Server Manager by using the Add Roles And Features Wizard or you can use the Install-WindowsFeature cmdlet. To install by using Server Manager, follow these steps:

1. Open Server Manager either locally on the edge server that will host the Remote Access role or on a computer that has Server Manager configured to connect to the edge server.
2. Select Add Roles And Features from the Manage menu. Click Next on the Before You Begin page if it is displayed.
3. Select Role-Based Or Feature-Based Installation and click Next.
4. Choose Select A Server From The Server Pool and then select the server that will host the role. Click Next.
5. On the Select Server Roles page, shown in Figure 3-29, select Remote Access. Click Next and then click Next again.

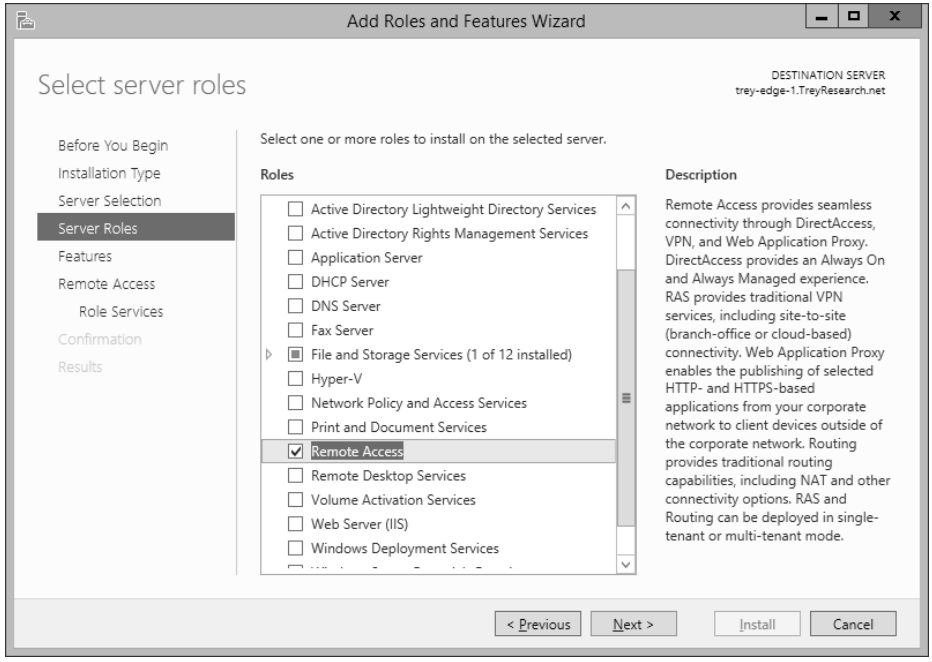


FIGURE 3-29 The Select Server Roles page of the Add Roles And Features Wizard

6. Read the Remote Access page and then click Next.

7. On the Select Role Services page, shown in Figure 3-30, select which role services you want to enable on this server. The choices are these:
   - DirectAccess and VPN (RAS)
   - Routing
   - Web Application Proxy

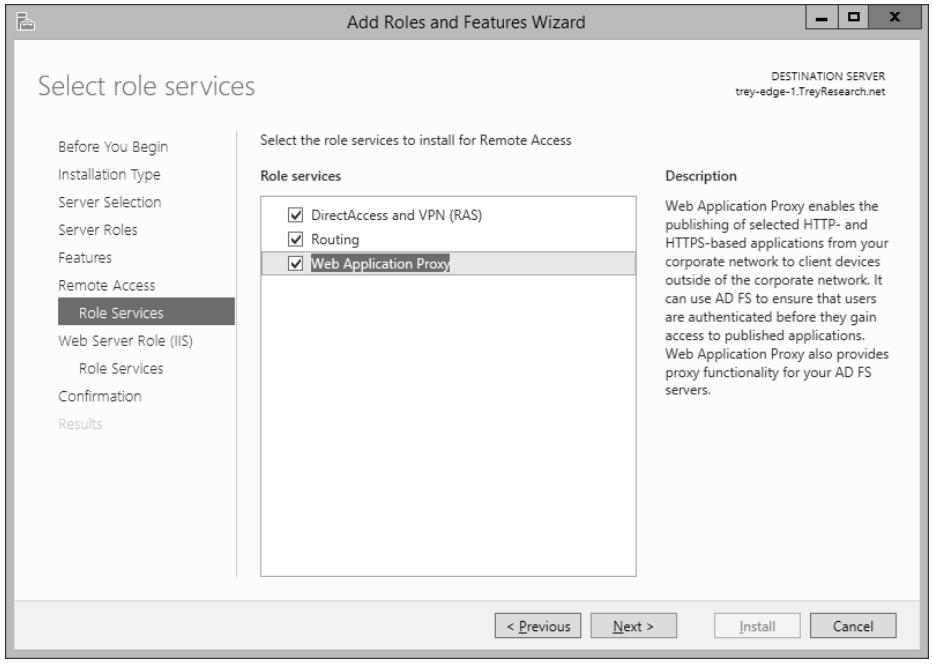


FIGURE 3-30 The Select Role Services page of the Add Roles And Features Wizard

8. Click Add Features if prompted by selecting a Role Service.
9. Click Next as required until the Confirm Installation Selections page is displayed.
10. Click Install; when the installation is complete, click Close.

To install the Remote Access role, including all the Role Services, you can use the Install-WindowsFeature cmdlet. For example:

```
Install-WindowsFeature -Name RemoteAccess `
                       -IncludeAllSubFeatures `
                       -IncludeManagementTools
```

Initial configuration

The initial configuration of the Remote Access role can be done by using the Getting Started Wizard, or the Remote Access Setup Wizard from the Remote Access Management console, as shown in Figure 3-31. The Getting Started Wizard is a quick way to get a VPN and

DirectAccess configured and set up. It makes all the initial settings and configuration decisions based on default recommended settings, and it is a huge improvement over the early days of setting up DirectAccess, especially. However, because it hides most of the choices, it's not particularly appealing to write exam questions about.

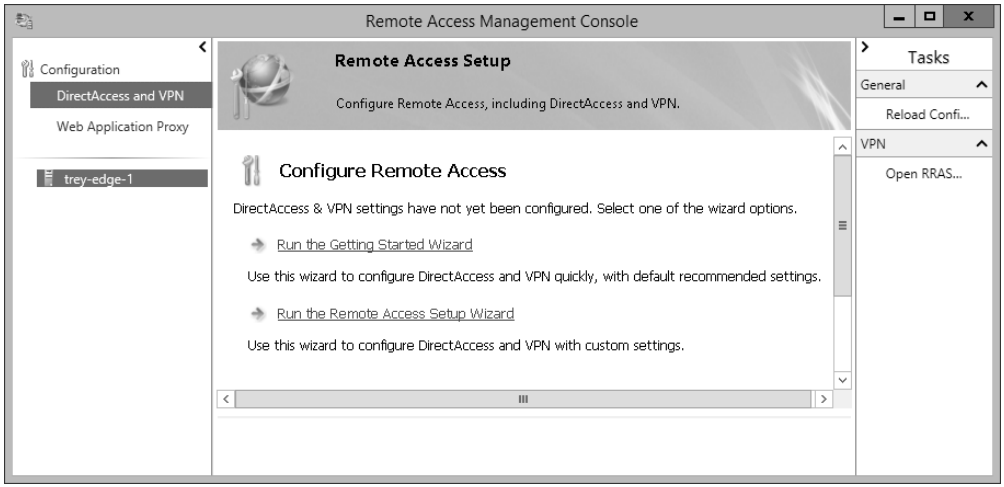


FIGURE 3-31 The Configure Remote Access screen of the Remote Access Management console

Regardless of whether you choose the Configure Remote Access Wizard or the Getting Started Wizard, the first page of each wizard is essentially the same—you need to choose what kind of Remote Access you want to deploy. The choices are these:

- **Deploy Both DirectAccess And VPN** Configures the server as a VPN endpoint and also configures DirectAccess (DirectAccess is covered in Objective 3.4).
- **Deploy DirectAccess Only** Configures the server as a DirectAccess server and enables DirectAccess client computers.
- **Deploy VPN Only** Configures the servers as a VPN endpoint by using the Routing And Remote Access console. VPNs can be remote client VPNs or site-to-site VPNs.

For the sections in this objective, configure the Remote Access server by using the Deploy VPN Only option. (The Web Access Proxy is configured separately and is not dependent on which option you choose for this initial configuration.)

To do the initial configuration of the Remote Access server, follow these steps:

1. Open the Remote Access Management Console by selecting Remote Access Management from the Tools menu in Server Manager.
2. Click DirectAccess And VPN under the Configuration option in the left pane, as shown in Figure 3-31.
3. Select Run The Remote Access Setup Wizard in the Remote Access Setup pane to open the Configure Remote Access page shown in Figure 3-32.

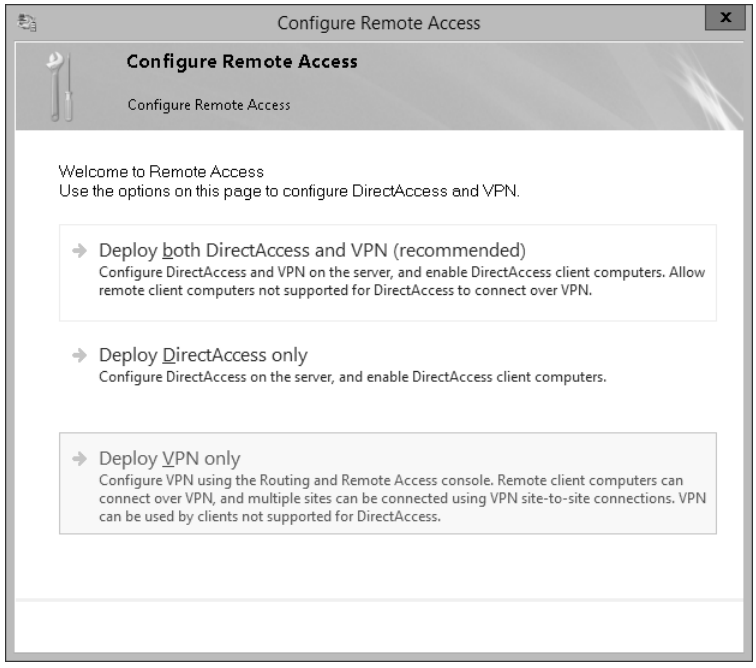


FIGURE 3-32 The Welcome To Remote Access page of the Configure Remote Access Wizard

4. Select Deploy VPN Only to open the Routing And Remote Access console, as shown in Figure 3-33.

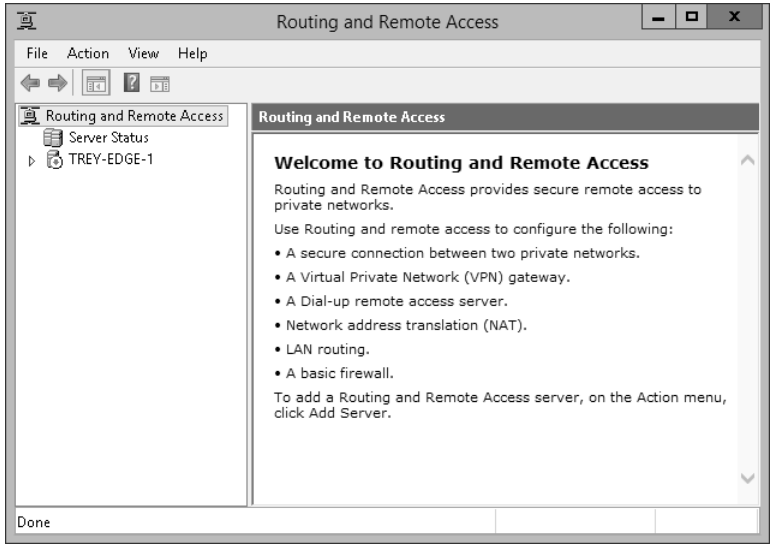


FIGURE 3-33 The Routing And Remote Access console

5. Select the server you are configuring and then select Configure And Enable Routing And Remote Access from the Action menu.
6. Click Next on the Welcome page of the Routing And Remote Access Server Setup Wizard.
7. Select Virtual Private Network (VPN) Access And NAT on the Configuration page and click Next.
8. On the VPN Connection page, select the network interface that connects the server to the Internet, as shown in Figure 3-34.

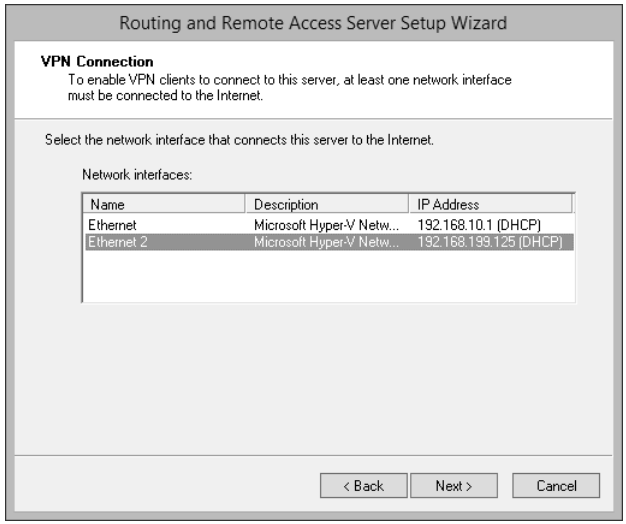


FIGURE 3-34 The VPN Connection page of the Routing And Remote Access Server Setup Wizard

9. If you're using DHCP on your network, select Automatically on the IP Address Assignment page or select From A Specified Range Of Addresses to have the Remote Access server assign the IP addresses of incoming VPN connections. Click Next.
10. On the Managing Multiple Remote Access Servers page, select No, Use Routing And Remote Access To Authenticate Connection Requests.
11. Click Next and then click Finish to return to the Remote Access Management console.

Implementing Network Address Translation (NAT)

NAT allows computers with private IP addresses to share a single public IP address. NAT can be implemented on Windows Server by using the Remote Access role or can be implemented on a network edge device such as a router or firewall. When you configure Windows Server as a NAT device, the server requires at least two network adapters: one connected to the private network and the second to the public network, as shown in Figure 3-35.

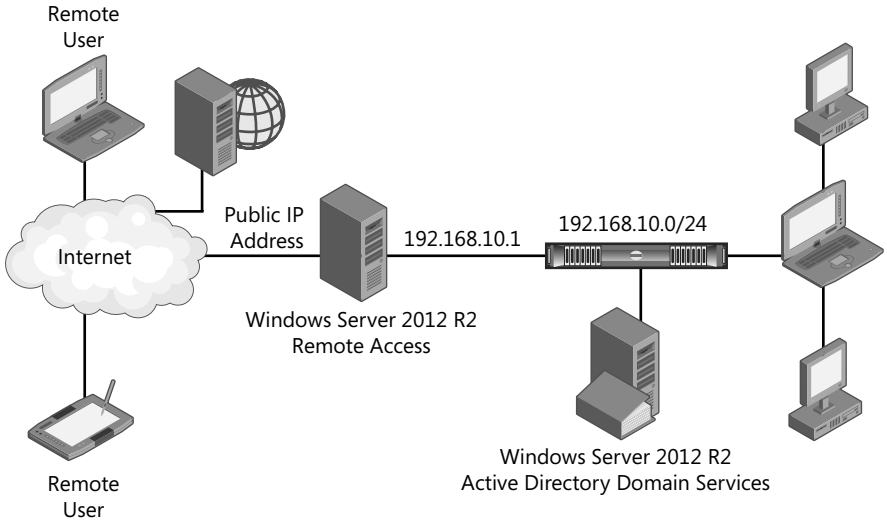


FIGURE 3-35 NAT network design

Internal networks are typically configured with private IP addresses. These private IP addresses cannot be routed to the public Internet, so before computers with private addresses can connect to the Internet, their private address needs to be translated into a public IP address. Private address ranges for IPv4 were designated by the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1918. Those private addresses come in three ranges:

- **10.0.0.0/8** 10.0.0.0 through 10.255.255.255 and a subnet mask of 255.0.0.0
- **172.16.0.0/12** 172.16.0.0 through 172.32.255.255 and a subnet mask of 255.255.0.0
- **192.168.0.0/16** 192.168.0.0 through 192.168.255.255 and a subnet mask of 255.255.0.0

When you run the Routing And Remote Access Server Setup Wizard, it enables NAT on the IPv4 address of the public facing network adapter. The second adapter is connected to the private, internal local area network (LAN). Packets to the public Internet are translated to show that they came from the public IP address of the public facing network adapter. When a reply comes back from the Internet, the Remote Access server reads the packet and routes it onto the private internal LAN to the originating device.

When you configure NAT using the Routing And Remote Access console, you specify which network adapter is connected to your private network and which adapter is connected to the public network. The Routing And Remote Access Server Setup Wizard creates two additional network interfaces, as shown in Figure 3-36: an internal interface, and a loopback interface.

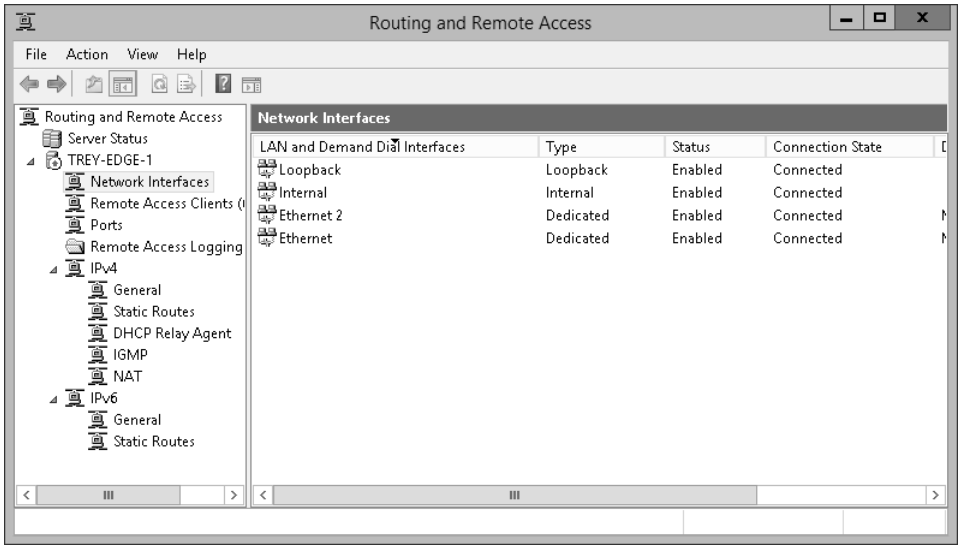


FIGURE 3-36 The Network Interfaces in the Routing And Remote Access console

You can specify specific services that are available on your internal network and map ports and protocols to the servers providing that service across the NAT boundary. For example, if you have a mail server at 192.168.10.5, you can configure port mapping on the public facing network interface to forward all SMTP packets (port 25) to the server at 192.168.10.5, as shown in Figure 3-37. However, this port mapping capability should *not* be substituted for a firewall.

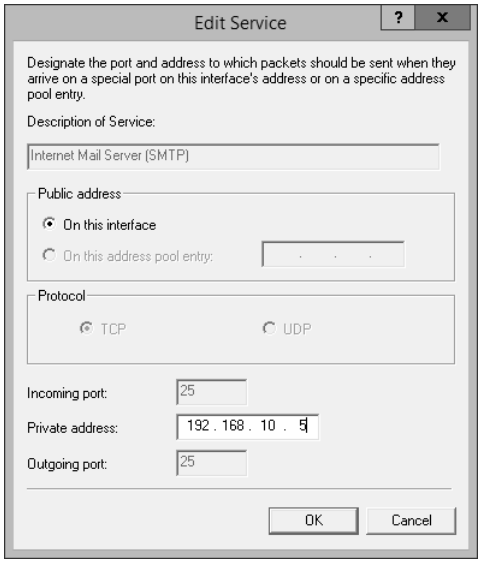


FIGURE 3-37 The Edit Service dialog box

Configuring VPN settings

Windows Server 2012 R2 supports four different VPN protocols, Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Key Exchange version 2 (IKEv2), and Secure Socket Tunneling Protocol (SSTP). These protocols are compared in Table 3-1. By default, when you use the Routing And Remote Access Server Setup Wizard to configure VPN, it creates VPN ports for all four protocols with a maximum of 128 ports each.

TABLE 3-1 VPN Protocols

Protocol	IP Protocol and Ports	Security	Comments
PPTP	TCP 1723; GRE 47	Low	Widely available across virtually all platforms.
L2TP	UDP 500, UDP 4500, UDP 1701; ESP 50	High	Uses IPSec, IKEv1. Difficult to configure, but suitable for site-to-site VPNs and client VPNs. Supported by Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.
SSTP	TCP 443 (SSL)	High	Easily used from almost any location. High overhead Supported on Windows Vista SP1 and later, and on Windows Server 2008. Used for Client VPN only, not site-to-site VPN. Not cross-platform.
IKEv2	UDP 500, UDP 4500, UDP 1701; ESP 50	High	Supports VPN Reconnect. Supports NAT Transversal. Supported by Windows Server 2008 R2, Windows 7, Windows Server 2012, Windows Server 2012 R2 and Windows 8.x.

Windows Server 2012 added support for many VPN management operations. The two modules that include VPN-related cmdlets are the RemoteAccess module and the VpnClient module. The related cmdlets in the RemoteAccess module are for VPN server operations, and the cmdlets in the VpnClient module are client operations. You can get a complete list of VPN-related cmdlets by using the following command:

```
Get-Command -Module RemoteAccess,VpnClient `
    | Sort-Object module,noun,verb `
    | where {$_.Noun -match "Vpn" } `
    | ft -auto verb,noun,Module
```

Configuring available VPN protocols

You can configure which protocols are available for VPN. The default is to use any available protocol; follow these steps to remove a protocol:

1. Open the Routing And Remote Access console (rrasmgmt.msc).
2. Select and expand the VPN server you want to manage.
3. Right-click Ports and select Properties.
4. Select the Device for which you want to remove support and click Configure.

5. Clear the check box for Remote Access Connections (Inbound Only).
6. Clear the check box for Demand-dial Routing Connections (Inbound And Outbound) if it is selected.
7. Change Maximum Ports to 0, as shown in Figure 3-38.

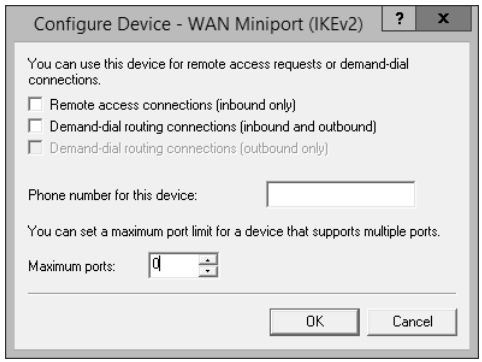


FIGURE 3-38 The Configure Device - WAN Miniport dialog box

8. Click OK and click Yes to acknowledge that you're reducing the number of ports for the connection. Any users using the ports you're eliminating will be disconnected.
9. Click OK to return to the Routing And Remote Access console.

You can add support for the removed protocol by reversing the preceding process.

Configuring DHCP and security settings for VPN connections

If you took the default settings when you configured VPN by using the Routing And Remote Access Server Setup Wizard, VPN clients will get their IP address from your existing DHCP server if one was detected. You can change this by configuring Routing And Remote access service (RRAS) to issue an IP address from a set block of addresses rather than requesting an address from the DHCP server. You can also change which network interface RRAS uses to request a DHCP address for the client. Follow these steps to configure DHCP on the server:

1. Open the Routing And Remote Access console (rrasmgmt.msc).

> ***NOTE*** **DIFFERENT IF DIRECTACCESS IS ENABLED**
>
> **If you have both DirectAccess and VPN enabled, you must configure DHCP and authentication settings from the Remote Access Management console, not RRAS. The settings are the same, but the location is different.**

2. Select the VPN server you want to manage and right-click.
3. Select Properties from the menu and then click the IPv4 tab shown in Figure 3-39.

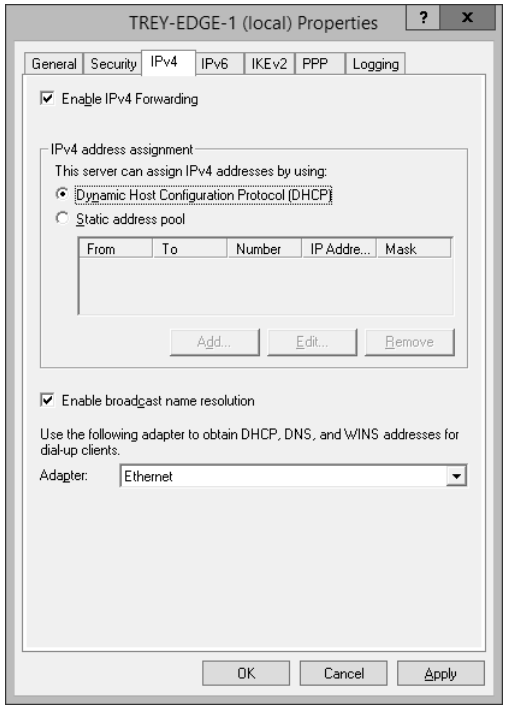


FIGURE 3-39 The IPv4 tab of the RRAS Server Properties dialog box

4. Select Dynamic Host Configuration Protocol (DHCP) to use network DHCP servers or Static Address Pool to issue IP addresses from the VPN server.

5. If using a static address pool, click Add to add a range of IP addresses to use for VPN clients, as shown in Figure 3-40.

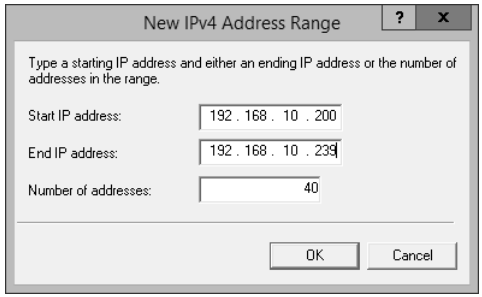


FIGURE 3-40 The New IPv4 Address Range dialog box

IMPORTANT **DHCP EXCLUSION**

If you choose to use a static IP address range for VPN clients, make sure to exclude that range from DHCP servers on the network to avoid an IP address conflict.

6. Select Enable Broadcast Name Resolution to specify the adapter to use for DHCP, DNS, and WINS.

7. Select the IPv6 tab to configure IPv6 properties, as shown in Figure 3-41.

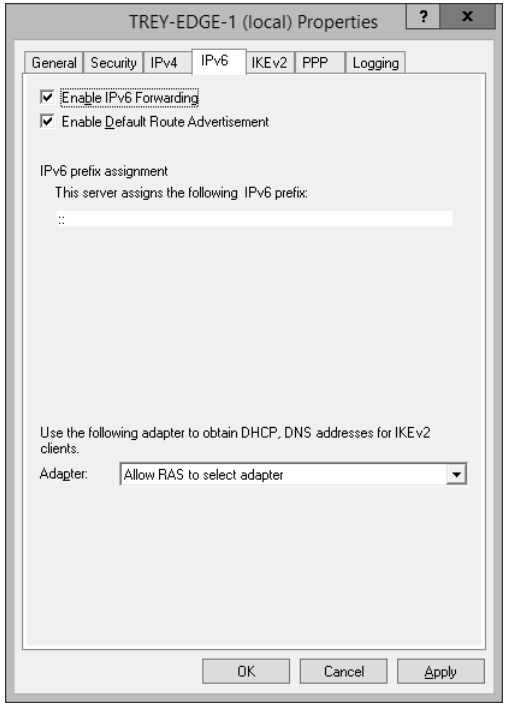


FIGURE 3-41 The IPv6 tab of the RRAS Server properties dialog box

8. Select the Security tab to configure security settings for remote access clients. The settings are these:

   - **Authentication Provider** Choose Windows Authentication or RADIUS Authentication. Click the Authentication Methods button to select the authentication methods that are allowed. Choices include EAP, MS-CHAPv2, CHAP, PAP, unauthenticated, and machine certificates for IKEv2.
   - **Accounting Provider** Choose Windows Accounting or RADIUS Accounting.
   - **Allow Custom IPsec Policy For L2TP/IKEv2 Connection** When selected, you can enter a Pre-shared Key.
   - **Use HTTP** When selected, SSL Certificate Binding can use HTTP. When deselected, specify the certificate that SSTP should use.

EXAM TIP

Support for the MS-CHAP, SPAP, and EAP-MD5 protocols ended with Windows Server 2008, and these protocols are no longer supported beginning with Windows Server 2008 R2.

9. Select the General tab to enable or disable portions of RRAS. In the Enable This Computer As A section, the options are these:
   - **IPv4 Router** Enabled by default. When enabled, can be set to Local Area Network (LAN) routing only, or LAN And Demand-Dial Routing (default).
   - **IPv6 Router** Disabled by default. When Enabled, can be set to Local Area Network (LAN) routing only or to LAN And Demand-Dial Routing.
   - **IPv4 Remote Access Server** Enabled by default.
   - **IPv6 Remote Access Server** Disabled by default.

Use the Set-VpnIPAddressAssignment cmdlet to set IP address assignment to DHCP or Static, and if static, to set a range of addresses to use. For example:

```
Set-VpnIPAddressAssignment `
    -IPAssignmentMethod StaticPool `
    -IPAddressRange "192.168.10.200","192.168.10.239"
```

Use the Set-VPNAuthProtocol cmdlet to set acceptable authentication protocols, and the Set-VPNAuthType cmdlet to set to "Windows" or "ExternalRadius"; if set to ExternalRadius, set the RadiusServer, SharedSecret, RadiusScore, RadiusTimeout, and RadiusPort parameters.

Configuring remote dial-in settings for users

The Routing And Remote Access console is also the interface for configuring remote dial-in settings. To enable dial-up remote access, open the Routing And Remote Access console and follow these steps:

1. Select the server you want to configure in the Tree pane and select Configure And Enable Routing And Remote Access from the Action menu.
2. Click Next on the Welcome page and then select Remote Access (Dial-Up Or VPN) on the Configuration page shown in Figure 3-42.
3. Click Next and select Dial-Up on the Remote Access page shown in Figure 3-43. You can also select VPN. If you do, you'll get a slightly different page progression through these steps.

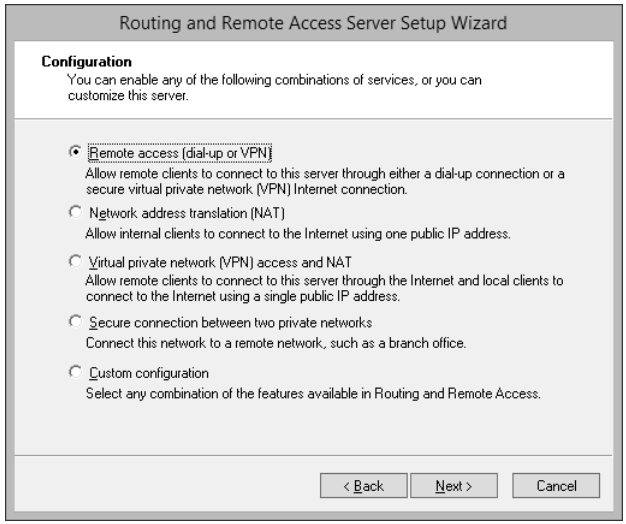


FIGURE 3-42 The Configuration page

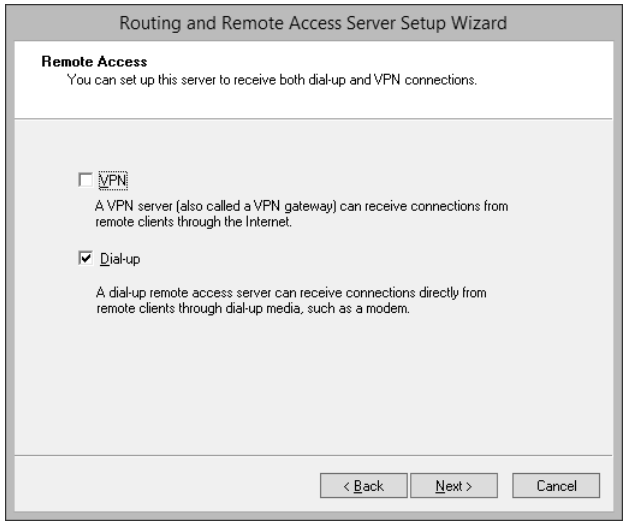


FIGURE 3-43 The Remote Access page

4. Click Next and select the network that dial-up clients will be connected to.
5. Click Next and specify whether to assign IP addresses Automatically or From A Specified Range Of Addresses. Automatically depends on an available DHCP server.
6. Click Next and specify whether to use Routing And Remote Access to authenticate connection requests or to use an RADIUS server. Click Next.

7. If you selected RADIUS, specify the details of the RADIUS server on the RADIUS Server Selection page shown in Figure 3-44. Click Next.

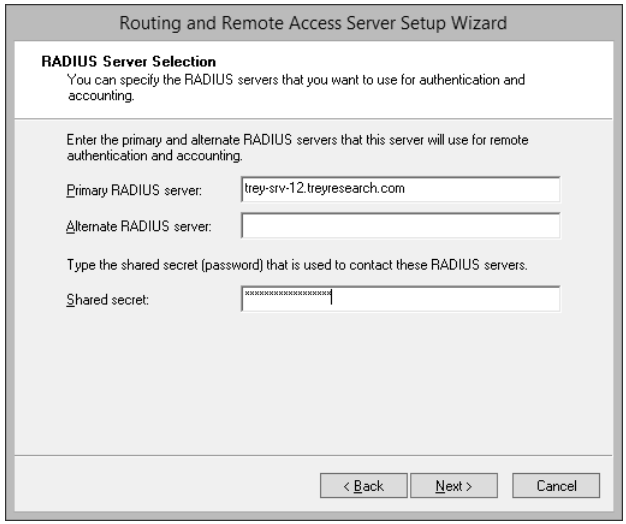


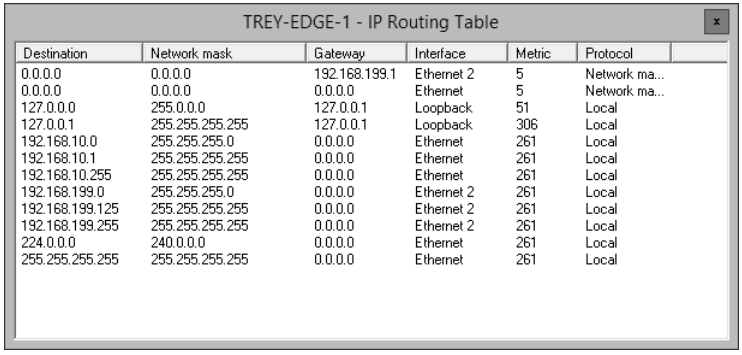
FIGURE 3-44 The RADIUS Server Selection page

8. Click Finish; the server is configured for dial-up remote access.

Configuring routing

You can configure the Remote Access server to also do routing between the LAN and the Internet, with or without NAT. When you install NAT, routing is also configured and enabled.

You can see the routing table for a default installation in Figure 3-45 by right-clicking the Static Routes node under IPv4 in the Routing And Remote Access console. The public facing IP address is 192.168.199.125, and the private LAN IP address is 192.168.10.1 for this figure.



Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	192.168.199.1	Ethernet 2	5	Network ma...
0.0.0.0	0.0.0.0	0.0.0.0	Ethernet	5	Network ma...
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	51	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	306	Local
192.168.10.0	255.255.255.0	0.0.0.0	Ethernet	261	Local
192.168.10.1	255.255.255.255	0.0.0.0	Ethernet	261	Local
192.168.10.255	255.255.255.255	0.0.0.0	Ethernet	261	Local
192.168.199.0	255.255.255.0	0.0.0.0	Ethernet 2	261	Local
192.168.199.125	255.255.255.255	0.0.0.0	Ethernet 2	261	Local
192.168.199.255	255.255.255.255	0.0.0.0	Ethernet 2	261	Local
224.0.0.0	240.0.0.0	0.0.0.0	Ethernet	261	Local
255.255.255.255	255.255.255.255	0.0.0.0	Ethernet	261	Local

FIGURE 3-45 The IP Routing Table for Trey-Edge-1

Adding a new routing protocol

You can add the Routing Information Protocol (RIP) version 2 routing protocol to the Routing And Remote Access server by following these steps:

1. Open the Routing And Remote Access console (rrasmgmt.msc).
2. Expand the server to which you want to add the protocol in the console tree.
3. Right-click the General node of the IPv4 folder and select New Routing Protocol, as shown in Figure 3-46.

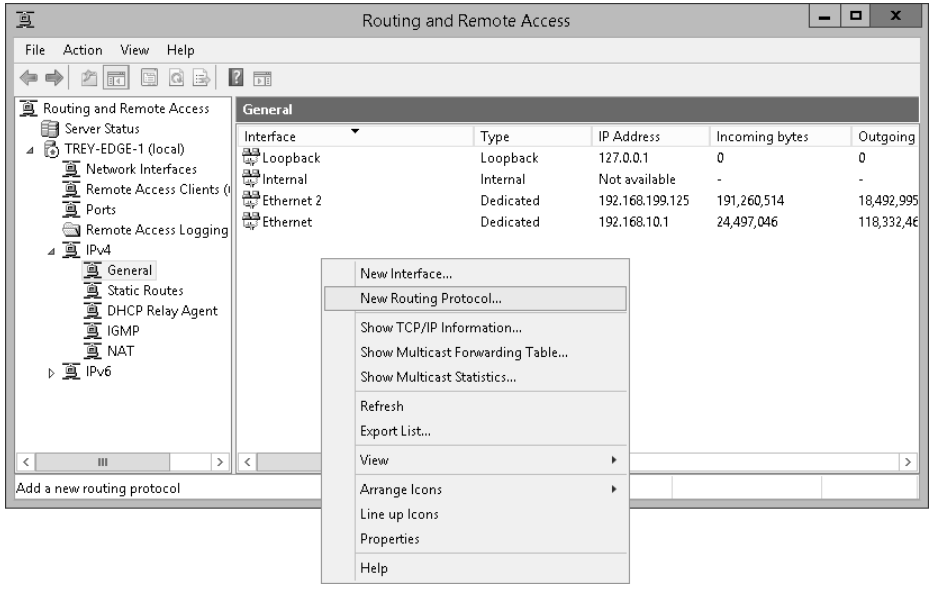


FIGURE 3-46 The context menu for the General IPv4 node

4. On the New Routing Protocol dialog box, select RIP Version 2 For Internet Protocol and click OK. A New RIP node is added to the IPv4 folder of the server. (There is no RIP or equivalent protocol for IPv6.)
5. Right-click the new RIP node and select New Interface from the menu.
6. Select the interface on which you want to enable RIP, usually the Internet facing interface, and click OK.
7. On the RIP Properties page, shown in Figure 3-47, set the options for RIP.

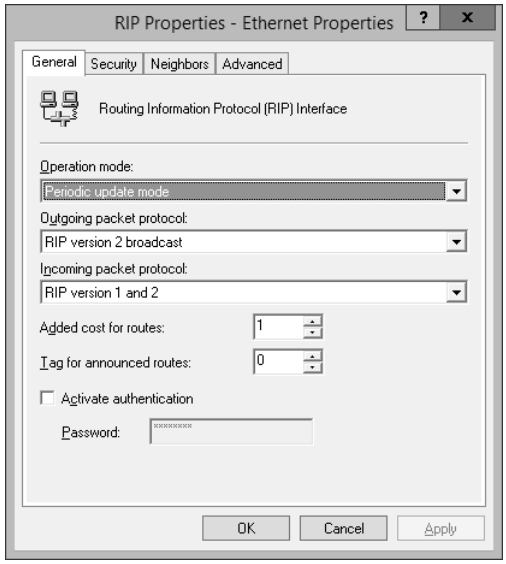


FIGURE 3-47 The RIP Properties dialog box

8. There are four tabs on the RIP Properties dialog box:
   - **General** Includes settings for Operation Mode, Outgoing Packet Protocols, Incoming Packet Protocols, Added Cost For Routes, Tag For Announced Routes, and an option to Activate Authentication.
   - **Security** Includes settings For Incoming Routes and For Outgoing Routes. You can choose to Accept All Routes or specify the incoming route ranges to accept or ignore, and you can specify to announce all routes, announce only specified routes, or not announce specified routes.
   - **Neighbors** Includes settings for how the router interacts with neighboring RIP routers. You can use Broadcast Or Multicast Only, Use Neighbors In Addition To Broadcast Or Multicast, or Use Neighbors Instead Of Broadcast Or Multicast. You can specify the IP Address of neighbors.
   - **Advanced** Includes timing settings and processing options, as shown in Figure 3-48.

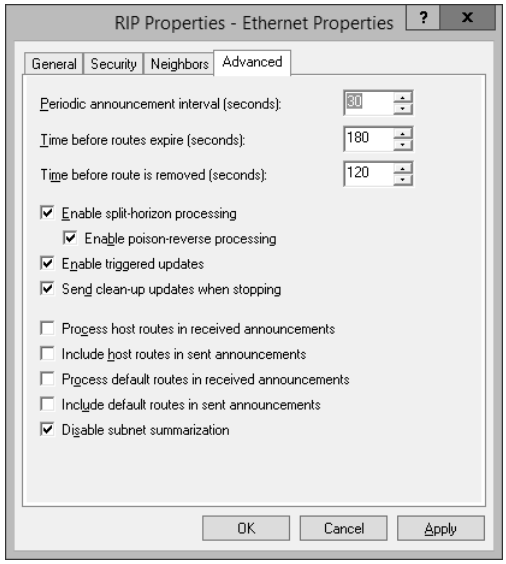


FIGURE 3-48 The Advanced tab of the RIP Properties dialog box

9. After you make any choices appropriate for your environment on the RIP Properties dialog box, click OK; the interface is added to the RIP node.

You can add the DHCPv6 Relay Agent routing protocol to the Routing And Remote Access server by following these steps:

1. Open the Routing And Remote Access console (rrasmgmt.msc).
2. Expand the server to which you want to add the protocol in the console tree.
3. Right-click the General node of the IPv6 folder and select New Routing Protocol from the menu.
4. In the New Routing Protocol dialog box, select DHCPv6 Relay Agent and click OK. A new DHCPv6 Relay Agent node is added to the IPv6 folder.
5. Right-click the new DHCPv6 Relay Agent node and select New Interface from the menu.
6. Select the interface on which you want to relay DHCPv6 packets and click OK to open the DHCP Relay Properties dialog box for that interface, as shown in Figure 3-49.

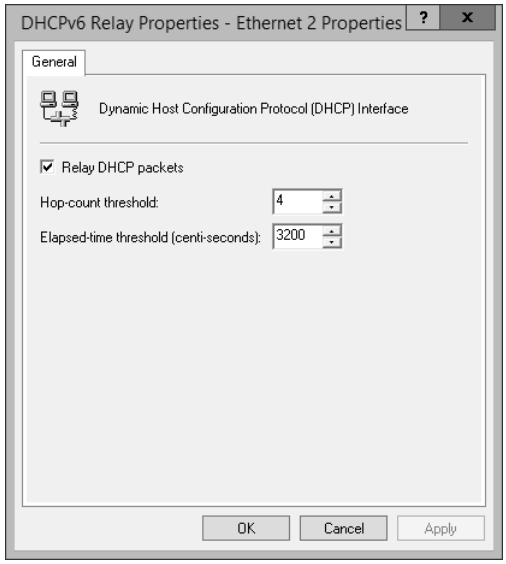


FIGURE 3-49 The DHCP Relay Properties dialog box

7. Click OK to enable the DHCPv6 Relay Agent.

Adding static routes

In addition to adding routing protocols, you can manually configure the RRAS server to use specific static routes. To add a static route, follow these steps:

1. Open the Routing And Remote Access console (rrasmgmt.msc).
2. Select and expand the server to which you want to add a route in the console tree.
3. Select IPv4 to add an IPv4 static route or IPv6 to add an IPv6 static route.
4. Right-click in the details pane and select New Static Route from the menu.
5. On theIPv4 Static Route dialog box (or the IPv6 Static Route dialog box), select the Interface and enter a Destination, Network Mask, Gateway, and Metric for the route, as shown in Figure 3-50.
6. Click OK to create the static route.

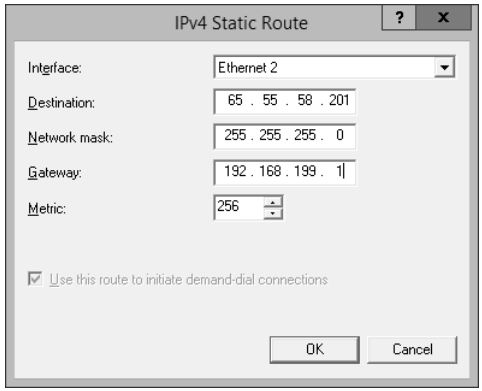


FIGURE 3-50 The IPv4 Static Route dialog box

Configuring Web Application Proxy in passthrough mode

Web Application Proxy can be configured to do passthrough preauthentication without requiring Active Directory Federation Services (AD FS) to publish applications. When Web Application Proxy is used in pass-through mode, domain users who have authenticated to the domain as part of their sign in on their computer can then access the application by passing through their AD DS credentials. When configured this way, the applications can't take advantage of Workplace Join, Multi-Factor Authentication (MFA), or Multi-factor Access Control. These features require AD FS. The flow for Web Application Proxy in passthrough mode is as follows:

1. A client attempts to connect to a public resource URL for an application. This URL is a public address that the Web Application Proxy listens on for HTTPS requests.
2. The Web Application Proxy passes the HTTPS request to the backend server hosting the application via HTTP or HTTPS.
3. Optionally, the user authenticates directly to the backend server or application.
4. If the user successfully authenticates (or if no authentication is required), the client now has access to the published application.

To publish an application using passthrough mode, follow these steps:

1. Open the Remote Access Management Console and click Web Application Proxy.
2. Right-click Web Application Proxy and select Publish.
3. Click Next. On the Preauthentication page of the Publish New Application Wizard, click Pass-Through and then Next.

4. On the Publish Settings page, do the following:
   - Enter a friendly name in the Name box.
   - In the Enter URL box, enter the fully qualified resource URL for the application.
   - Select a certificate from the External Certificate list. Click Next.
5. Click Publish and then Close when the application publish completes.

The Windows PowerShell method for publishing an application in passthrough mode, uses the Add-WebApplicationProxyApplication cmdlet. For example:

```
Add-WebApplicationProxyApplication `
     -BackendServerURL "https://app.treyresearch.net/" `
     -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b' `
     -ExternalURL "https://app.treyresearch.net/" `
     -Name "Trey App" `
     -ExternalPreAuthentication PassThrough
```

Thought experiment

Configuring VPN protocols

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the network administrator for TreyResearch.net. You need to deploy VPN to support legacy remote users and non-domain-joined remote clients, including includes both Windows and non-Windows devices. You also have users running Windows 8 and Windows 8.1 who need to use VPN as a fallback for their DirectAccess connection.

1. **What protocols provide the widest range of support for different operating systems and devices? Do you really need or want all four available protocols?**
2. **You currently use DirectAccess with Windows Authentication, but you want to move to two-factor authentication for DirectAccess and VPN. What are your options?**

Objective summary

- Windows Server 2012 introduced the new combined Remote Access role that combines Routing, VPN, DirectAccess, and Web Application Proxy.
- A single Remote Access server can provide both VPN and DirectAccess.

- Network Address Translation (NAT) allows multiple computers to share a single public IP address.
- The RemoteAccess Windows PowerShell module provides support for some VPN Server management functions, and the VpnClient module is used for VPN client functions.
- The Routing And Remote Access console is used to configure routing, NAT, and dial-up remote access and VPN remote access.
- Windows Server 2012 supports four VPN protocols: PPTP, L2TP, IKEv2, and SSTP.
- Windows Server optionally supports the RIPv2 routing protocol.
- Windows Server 2012 R2 adds Web Application Proxy as a reverse proxy to make applications available for external access. Web Application Proxy can publish applications in passthrough mode.

Objective review

1. What command do you use to install *only* VPN and NAT and their management tools?
   - **A.** Enable-WindowsOptionalFeature -FeatureName RRAS -online
   - **B.** Add-WindowsFeature -Name RemoteAccess -IncludeManagementTools
   - **C.** Add-WindowsFeature -Name DirectAccess-VPN,Routing ` -IncludeManagementTools
   - **D.** Add-WindowsFeature -Name RRAS -IncludeManagementTools
2. You need to configure VPN to only support clients using the SSTP protocol. What changes do you need to make to the default VPN configuration in Windows Server 2012 R2?
   - **A.** Add the WAN Miniport for SSTP and set the maximum number of ports. Restart the RemoteAccess service.
   - **B.** Remove the PPTP WAN Miniport and set the maximum number of ports for PPTP to zero.
   - **C.** Clear Remote Access Connections for the WAN Miniport (PPTP), WAN Miniport (IKEv2), and WAN Miniport (L2TP).
   - **D.** Enable demand-dial for the WAN Miniport (PPPOE).

3. You use DirectAccess for all Windows 8 and later remote clients, but you use VPN to support Windows 7 clients. You need to configure VPN to use IP addresses controlled by the Remote Access server. What settings do you need to make? (Choose all that apply.)

   A. In the Routing And Remote Access console, select Assign Addresses Automatically.

   B. In the Routing And Remote Access console, select Assign Addresses From A Static Pool.

   C. In the DHCP Management console, create DHCP reservations for the IP addresses assigned to VPN clients.

   D. In the DHCP Management console, create a DHCP exclusion for the IP addresses assigned to VPN clients.

   E. In the Remote Access Management console, select Assign Addresses Automatically.

   F. In the Remote Access Management console, select Assign Addresses From A Static Address Pool.

Objective 3.4: Configure DirectAccess

Originally introduced in Windows Server 2008 R2 and Windows 7, DirectAccess is an always-on technology that allows remote management of domain-joined computers and optionally a transparent, always available, remote connection to the domain network that provides users remote access without having to initiate a VPN connection.

A DirectAccess remote connection has the following benefits as compared with VPNs:

- **Always-on** With a VPN, a user needs to initiate a connection before the computer is connected. With DirectAccess, the computer is connected to the domain network as soon as it has an Internet connection.
- **Seamless** A DirectAccess connected computer is transparently connected to the domain network. The computer seems to users as if they are directly connected to the domain network, with the exception of the connection speed, which is dependent on the Internet connection speed.
- **Security** A VPN connection is an unmanaged connection with Group Policy not enforced. A DirectAccess connection is a fully managed connection with all Group Policy Objects enforced; and management tools, such as Microsoft System Center Configuration Manager, can manage the client computer just as they do when it is connected locally. DirectAccess uses IPSec to authenticate the user and computer, and to encrypt communication.

This objective covers how to:

- Implement client configuration
- Implement server requirements
- Configure DNS for DirectAccess
- Configure certificates for DirectAccess

Installing DirectAccess

There are two different scenarios for DirectAccess: remote management only or remote management plus remote access. In either scenario, the DirectAccess server can be directly connected to the Internet as the edge device or connected behind an edge device. When connected directly to the Internet, the DirectAccess server needs at least two network adapters. When connected behind an edge device, the DirectAccess server can have a single network adapter if the edge device is doing NAT.

Follow the steps in the section titled "Installing the Remote Access role" in Objective 3.3 to install the Remote Access role on the DirectAccess server. The Getting Started Wizard or the Remote Access Setup Wizard from the Remote Access Management console can be used to initially configure the Remote Access role (refer to Figure 3-31). Each enables you to install both DirectAccess and VPN on the same server. The Getting Started Wizard is a very useful tool for configuring DirectAccess with only a very few mouse clicks, but that process is not terribly interesting from an exam viewpoint. It also hides a lot of the decisions by making default choices. For this objective, focus on using the Remote Access Setup Wizard and installing the DirectAccess role only.

When you install DirectAccess, there are four stages of the installation:

- **Configure DirectAccess Client** DirectAccess clients can be configured for both remote access and remote management, or remote management only. You also need to configure which security groups to enable for DirectAccess. Only client computers that are explicitly allowed can connect via DirectAccess. You can also enable DirectAccess for mobile computers only. This is the default for the Getting Started Wizard.
- **Configure DirectAccess Server** The DirectAccess server configuration varies, depending on the physical topology of the network. You configure where the server is located on your network and what network configuration to use.
- **Configure Infrastructure Servers** The DirectAccess Infrastructure Server Setup Wizard is used to configure settings for the network location server, the DNS server, and management servers used by DirectAccess clients.
- **Configure Internal Application Servers** The DirectAccess Application Server Setup page enables you to configure IPsec authentication for end-to-end authentication and encryption to specified servers, if desired. Traffic between the DirectAccess client and the DirectAccess server is always authenticated and encrypted with IPsec.

Implementing client configuration

The first step of installing and configuring DirectAccess is to set the client configuration. These steps are performed at the server or by using the Remote Server Administrative Tools (RSAT). To install DirectAccess after the Remote Access role is installed, follow these steps:

1. Open the Remote Access Management console and select DirectAccess And VPN in the left pane (refer to Figure 3-31).
2. Click Run The Remote Access Setup Wizard to open the Welcome To Remote Access page of the Configure Remote Access Wizard, as shown in Figure 3-51.

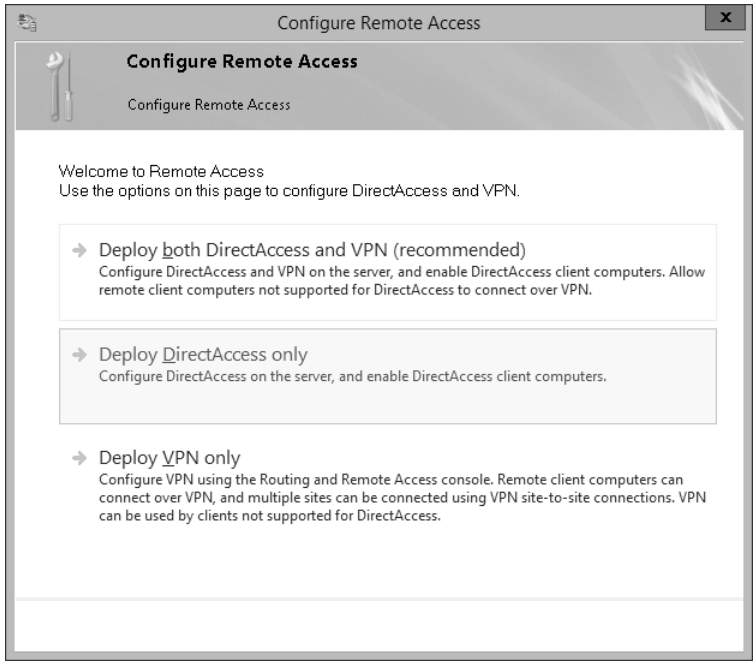


FIGURE 3-51 The Welcome To Remote Access page of the Configure Remote Access Wizard

The choices are as follows:

- **Deploy Both DirectAccess And VPN** Configures the server as a VPN endpoint and also configures DirectAccess.
- **Deploy DirectAccess Only** Configures the server as a DirectAccess server and enables DirectAccess client computers.
- **Deploy VPN Only** Configures the servers as a VPN endpoint by using the Routing And Remote Access console. VPNs can be remote client VPNs or site-to-site VPNs. (VPNs are covered in Objective 3.3.)

For the sections in this objective, configure the Remote Access server by using the Deploy DirectAccess Only option.

3. Select Deploy DirectAccess Only to open the Configure Remote Access, Including The DirectAccess And VPN page, as shown in Figure 3-52.

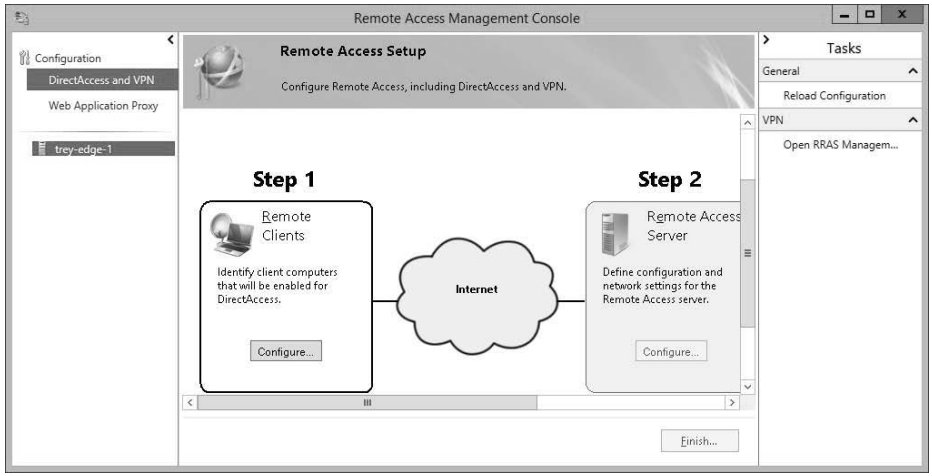


FIGURE 3-52 The Configure Remote Access, Including DirectAccess And VPN page

4. Click Configure in the Step 1 Remote Clients box to open the DirectAccess Client Setup Wizard shown in Figure 3-53. Choose whether DirectAccess clients will have remote access and remote management, or only remote management.

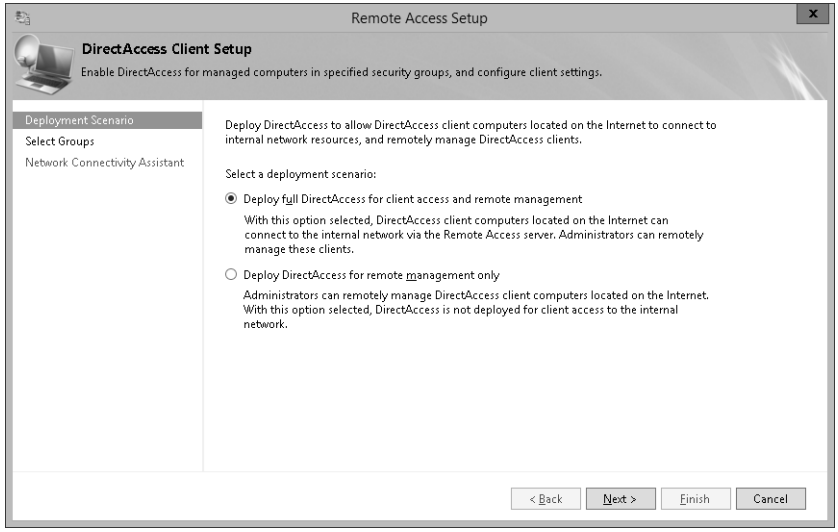


FIGURE 3-53 The Deployment Scenario page of the DirectAccess Client Setup Wizard

5. Click Next to open the Select Groups page of the DirectAccess Client Setup Wizard, as shown in Figure 3-54. The options are the following:
   - Click Add to open the standard Select Groups dialog box to add security groups that will have DirectAccess enabled.
   - Select Enable DirectAccess For Mobile Computers Only if you want DirectAccess to be enabled only on laptop and tablet computers.

EXAM TIP

The default for the Quick Start Wizard is to limit DirectAccess to mobile computers only. This sets up a scenario for which it is particularly easy to write an exam question. Why can laptops connect to the corporate network but not desktop computers?

   - Select Use Force Tunneling to force DirectAccess clients to send all Internet traffic through the corporate network.

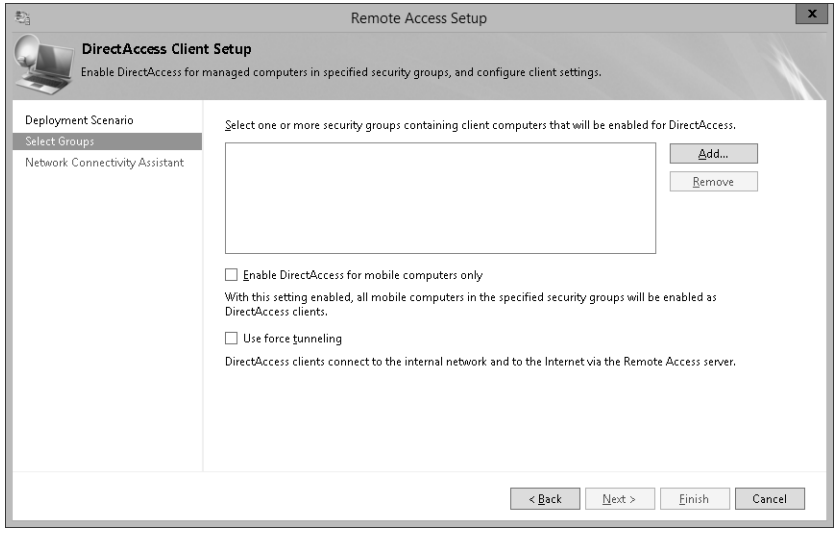


FIGURE 3-54 The Select Groups page of the DirectAccess Client Setup Wizard

6. Click Next to open the Network Connectivity Assistant page of the Direct Access Client Setup Wizard, as shown in Figure 3-55.

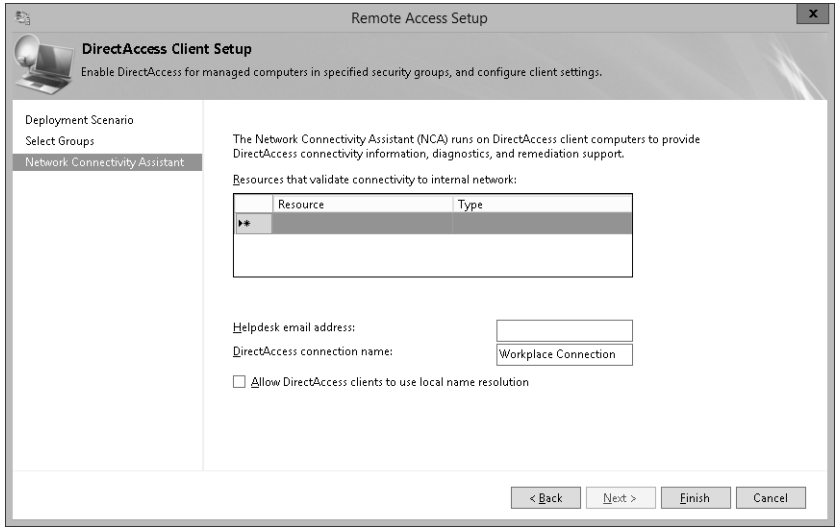


FIGURE 3-55 The Network Connectivity Assistant page of the DirectAccess Client Setup Wizard

7. Double-click in the first line in the Resources That Validate Connectivity To Internal Network box to open the Configure Corporate Resources For NCA dialog box shown in Figure 3-56. You can enter an HTTP address or a PING address that the Network Connectivity Assistant (NCA) can use to verify connectivity. You can add multiple resources if desired.

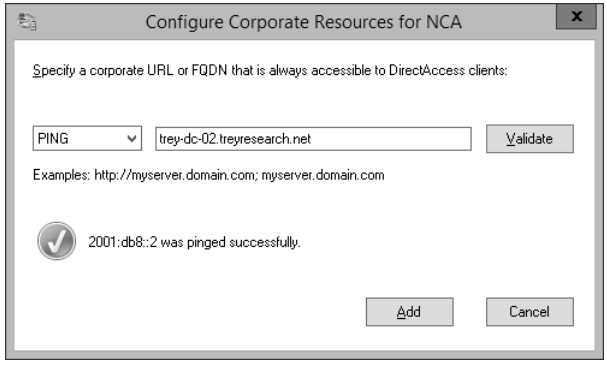


FIGURE 3-56 The Configure Corporate Resources For NCA dialog box

8. Select PING or HTTP for the resource type and enter the URL or FQDN of the resource. Click Validate to ensure that the resource is reachable.

NOTE **PING ISN'T ENOUGH**

When you configure corporate resources for the NCA, choose at least one HTTP resource type. PING doesn't use IPsec and is not sufficient to correctly detect the connectivity status.

9. Click Add to add the resource and return to the NCA page. On this page, you can also configure the following:
   - **Helpdesk Email Address** An email address dedicated to resolving DirectAccess client problems for remote users.
   - **DirectAccess Connection Name** A connection name that users will see on DirectAccess connected clients for the DirectAccess connection.
   - **Allow DirectAccess Clients To Use Local Name Resolution** When enabled, clients can use the broadcast protocols of NetBIOS over TCP/IP and Link-Local Multicast Name Resolution (LLMNR) to resolve single-level names when they can't resolve them through DNS. Local name resolution also needs to be configured on the Infrastructure Server Setup Wizard for this to work.
10. Click Finish; the DirectAccess Client Setup Wizard closes, and you're back at the main Configure Remote Access page. Step 1 now shows Edit instead of Configure.

Implementing server requirements

After you complete the client configuration section of Step 1 in the Configure Remote Access Wizard, the Configure button is enabled on Step 2. You can configure the DirectAccess server by following these steps:

1. Click the Configure button in Step 2 of the Remote Access Setup pane of the Remote Access Management console.
2. On the Network Topology page of the Remote Access Server Setup Wizard, select the topology that best describes your network. The choices are these:
   - **Edge** The DirectAccess server is at the edge of the internal network. The server has two network adapters, one of which is configured with a public IP address and is connected to the Internet. The second adapter is connected to the internal private network and has a private IP address.
   - **Behind An Edge Device (With Two Network Adapters)** The DirectAccess server is deployed behind an edge firewall or device. The server has two network adapters, one of which is connected to the perimeter network, and the other is connected to the internal private network. If the edge device uses NAT, only IP over HTTPS (IP-HTTPS) is deployed.
   - **Behind An Edge Device (With One Network Adapter)** The DirectAccess server is deployed with a single network adapter that is connected to the internal network. The edge device does NAT.

3. Enter the public DNS name or IPv4 address that remote clients use to connect to the remote access server, as shown in Figure 3-57.

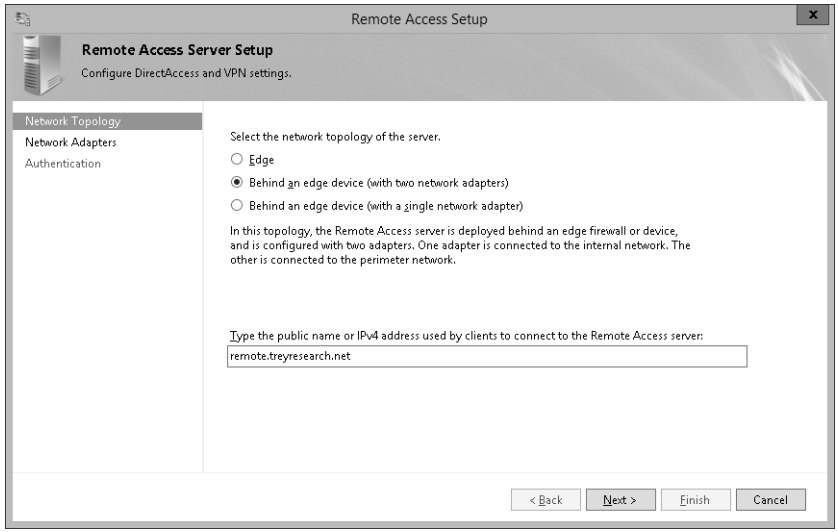


FIGURE 3-57 The Network Topology page of the Remote Access Server Setup Wizard

4. Click Next to open the Network Adapters page. The Remote Access Server Setup Wizard will attempt to determine your network adapter settings and configure them, as shown in Figure 3-58.

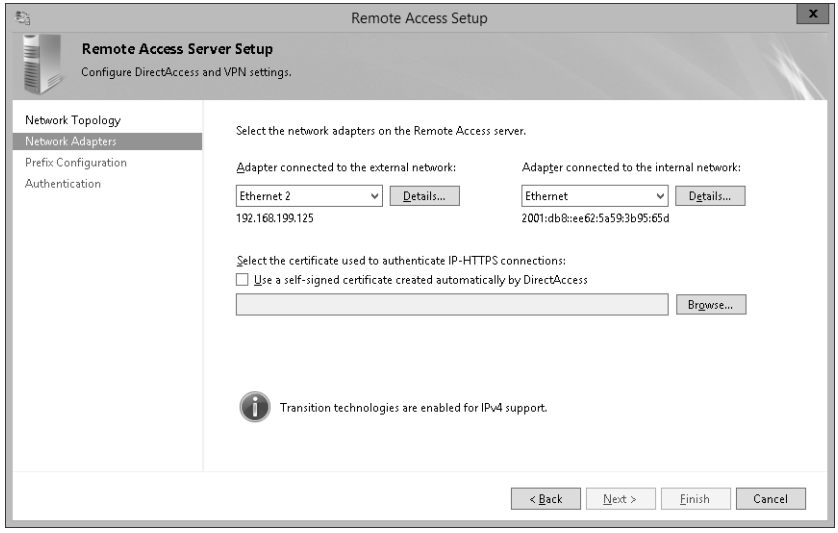


FIGURE 3-58 The Network Adapters page of the Remote Access Server Setup Wizard

5. Specify the certificate to use for IP-HTTPS connections. It can be a self-signed certificate that is automatically created by DirectAccess, or you can use a public certificate that matches the public DNS name or IP address you specified on the Network Topology page. Click Next.

6. On the Prefix Configuration page, the IPv6 prefix settings that have been detected are displayed, along with the IPv6 prefix that will be assigned to DirectAccess clients. You can edit these settings if they don't look right, but the wizard is usually correct. Click Next.

7. On the Authentication page, shown in Figure 3-59, specify the authentication used. The choices on the page are these:

   - **User Authentication** Active Directory credentials is the default choice. You can, however, specify Two-Factor Authentication, which uses a smart card or one-time password (OTP). Beginning with Windows Server 2012, the client computer's Trusted Platform Module (TPM) can be used as a virtual smart card. OTP requires configuring RADIUS and other configuration steps that are beyond the scope of this portion of the exam, although you should know that it is an option.

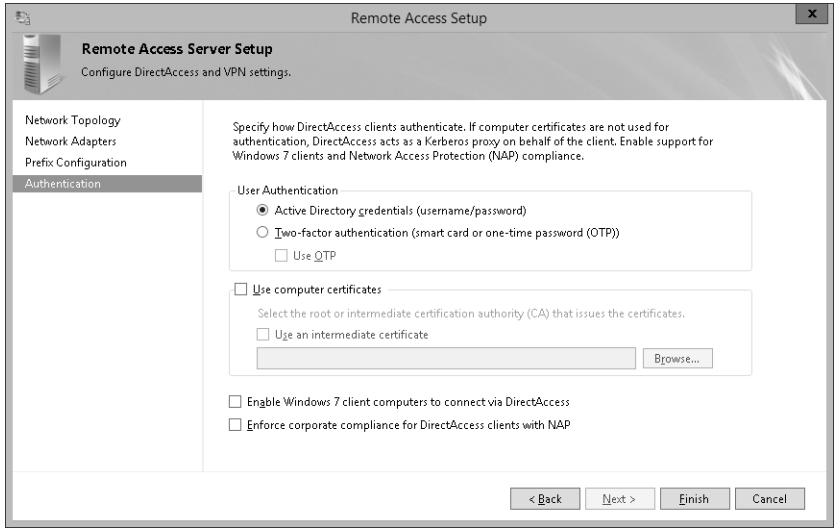


FIGURE 3-59 The Authentication page of the Remote Access Server Setup Wizard

   - **Computer Certificates** The default is to use Kerberos for client authentication, which doesn't require a certificate. However, certificate authentication is required for two-factor authentication, for a multisite deployment, and for Windows 7 DirectAccess clients.
   - **Windows 7 Clients** Windows 7 clients can't connect to a Windows Server 2012 DirectAccess deployment unless you configure computer certificates. If you select this box, it automatically selects the Use Computer Certificates box.

- **Network Access Protection** NAP is not supported for new DirectAccess deployments beginning with Windows Server 2012 R2.

8. Click Finish to close the Remote Access Server Setup Wizard and return to the Configure Remote Access Wizard. Step 2 now has an Edit button; and Step 3, Infrastructure Servers, has the Configure button enabled.

The settings on the Authentication page can also be configured with the Set-DAServer cmdlet.

Configuring DNS for DirectAccess

This item in the objective domain for the exam actually aligns with Step 3, the Infrastructure Server configuration, although Step 3 includes other name and location services. To run the Infrastructure Server Setup Wizard, follow these steps:

1. Click the Configure button in Step 3 of the Remote Access Setup pane of the Remote Access Management console.
2. On the Network Location Server page, enter the URL of the Network Location server if the server is on a remote web server and then click Validate. This is the preferred solution, but you can also host the network location server on the DirectAccess server. However, if you do, you need to provide a certificate or use a self-signed certificate, as shown in Figure 3-60.
3. On the DNS page of the Infrastructure Server Setup Wizard, shown in Figure 3-61, double-click the DNS Server Address to open the DNS Server Addresses dialog box.

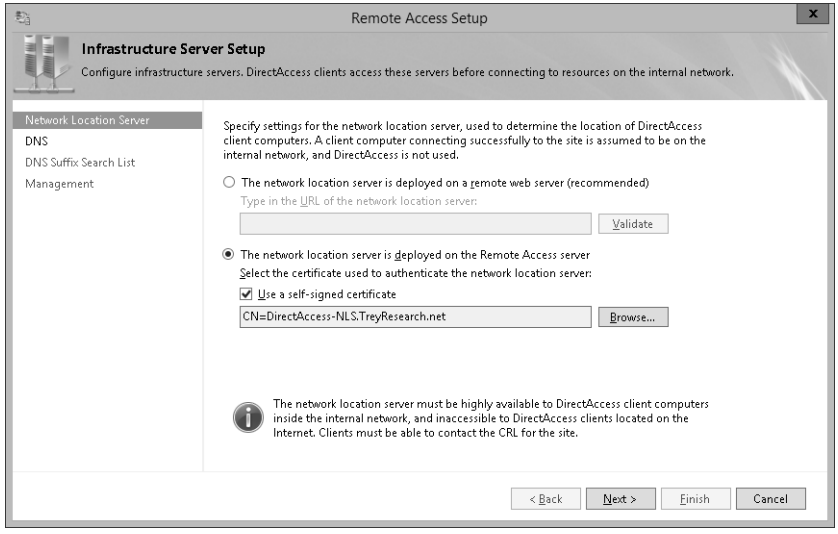


FIGURE 3-60 The Network Location Server page of the Infrastructure Server Setup Wizard

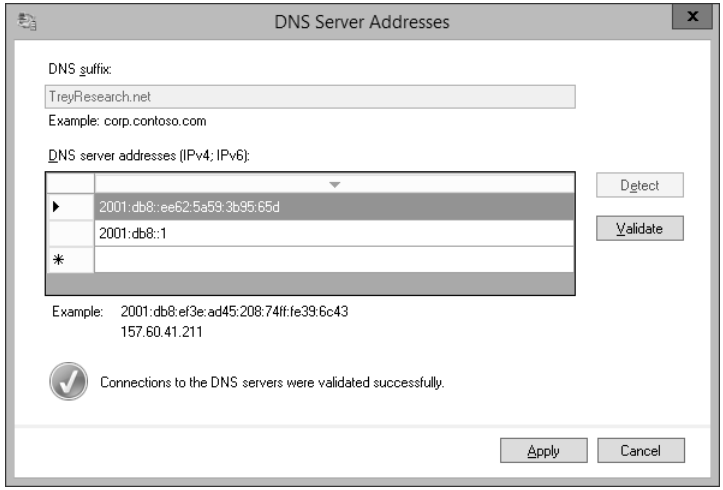


FIGURE 3-61 The DNS Server Addresses dialog box

4. Click the Validate button to validate the DNS Server address and DNS Suffix, and then click Apply to return to the DNS page. Select from the three Local Name Resolution options:
   - Use Local Name Resolution If The Name Does Not Exist In DNS. (Most restrictive)
   - Use Local Name Resolution If The Name Does Not Exist In DNS, Or DNS Servers Are Unreachable When The Client Computer Is On A Private Network. (Default, recommended)
   - Use Local Name Resolution For Any Kind Of DNS Resolution Error. (Least restrictive)
5. Click Next. On the DNS Suffix Search List page, shown in Figure 3-62, configure the Domain Suffixes to use for DNS search. The default values should include all detected internal domain DNS names. To add a suffix, use the New Suffix box plus the Add button. Use the up and down arrow buttons to reorder the list.
6. Click Next and enter any Management Servers on the Management page of the Infrastructure Server Setup Wizard. Any automatically discovered System Center Configuration Manager servers are added to the list after the wizard completes.
7. Click Finish to complete Step 3, Infrastructure Servers. Step 3 is changed to an Edit button, and Step 4 is now active with an enabled Configure button.

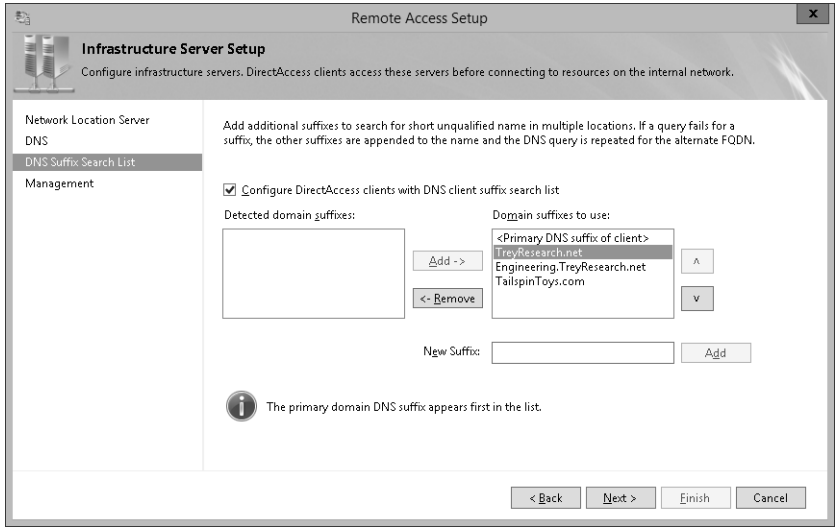


FIGURE 3-62 The DNS Suffix Search List page of the Infrastructure Server Setup Wizard

Step 4 of the Configure Remote Access Wizard is the DirectAccess Application Server Setup page. This page enables you to configure end-to-end authentication and encryption between the DirectAccess client and selected internal application servers. This is a single page with the option to Extend Authentication To Selected Application Servers, as shown in Figure 3-63.

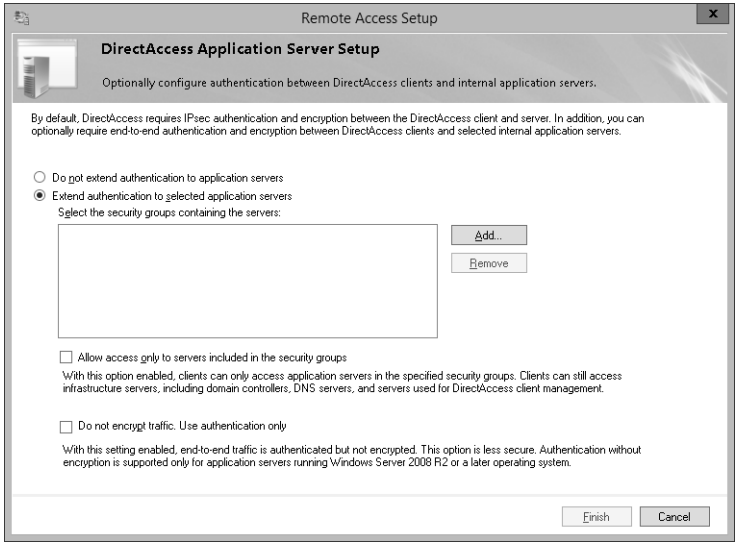


FIGURE 3-63 The DirectAccess Application Server Setup page

Add servers to the list for end-to-end authentication by adding the security group containing the servers to the list. You can restrict access to application servers to *only* the servers in the list by selecting Allow Access Only To Servers Included In The Security Groups. It does not restrict access to infrastructure servers used for DirectAccess, such as DNS servers and domain controllers.

You can also specify that the end-to-end scenario is for authentication only, but that encryption stops at the DirectAccess server. This less-secure option is available only for application servers running Windows Server 2008 R2 or later operating systems.

When you configure the Application Server settings, click Finish and then Finish again on the Remote Access Setup page to complete the configuration changes. The Remote Access Review page shown in Figure 3-64 opens. This page lists the GPO settings, Remote Clients settings, Remote Access Server settings, Infrastructure Server settings, and Application Server settings. You can save all these settings to a file by clicking the Save To A File link.

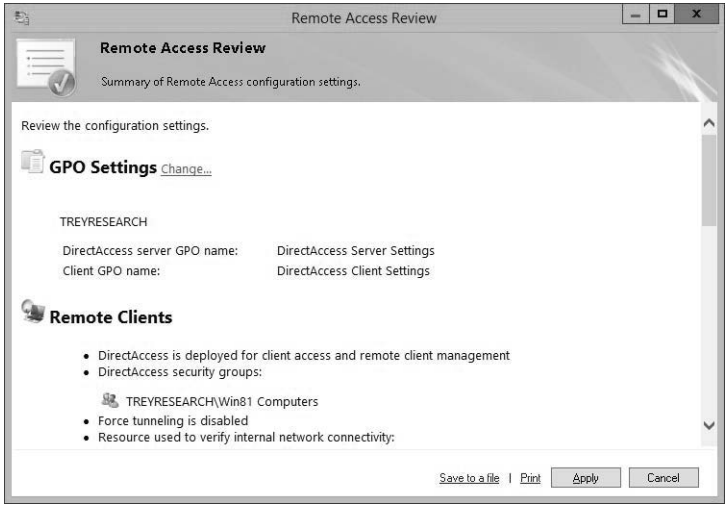


FIGURE 3-64 The Remote Access Review page

When you click Apply, the wizard will attempt to make the changes shown in the Remote Access Review page. If the wizard experiences a problem, it will identify it and then either roll back or issue a warning, as shown in Figure 3-65.

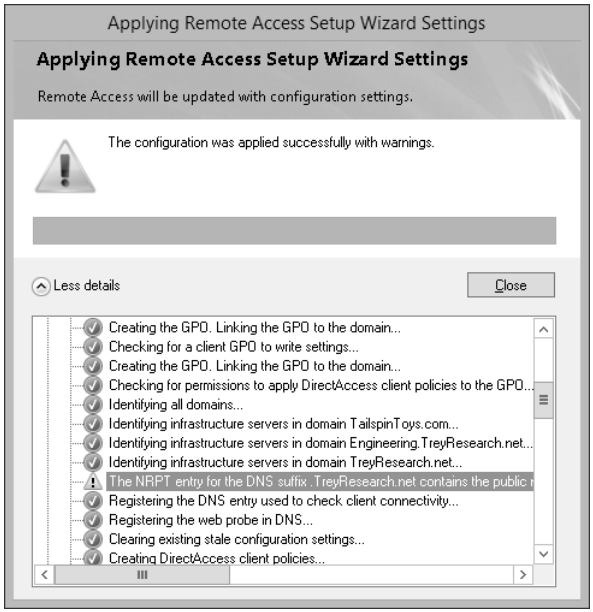


FIGURE 3-65 The Applying Remote Access Setup Wizard Settings dialog box

You can correct any errors and restart the applying step of the wizard from the main Remote Access Management console.

Configuring certificates for DirectAccess

Beginning with Windows Server 2012 and Windows 8, DirectAccess clients are configured to use Kerberos authentication by default. This means that Windows 8 and later clients do not need a certificate to connect. If you enable connecting with Windows 7 clients to a Windows Server 2012 or Windows Server 2012 R2 DirectAccess server, you need to enable computer certificate authentication. You also need to enable computer certificate authentication for two-factor authentication or for a multisite deployment of DirectAccess.

To enable computer certificate authentication, follow these steps:

1. Open the Remote Access Management console and select DirectAccess And VPN in the Configuration section of the left pane.
2. Click Edit in Step 2 Remote Access Server in the Remote Access Setup pane.
3. Click Authentication in the left pane and select Use Computer Certificates.
4. Select Use An Intermediate Certificate if you want to use an intermediate certificate authority certificate, such as the DirectAccess RADIUS certificate.
5. Click Browse to open a list of available certificates, as shown in Figure 3-66.
6. Select the certificate you want to use and click OK.

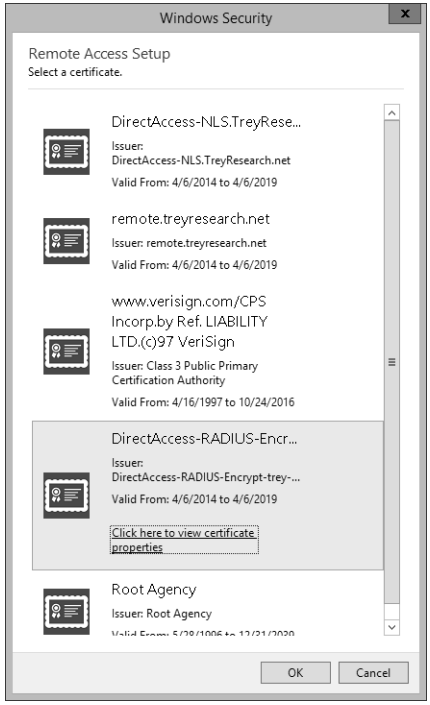


FIGURE 3-66 The Remote Access Setup Select A Certificate dialog box

Thought experiment

Configuring two-factor authentication

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are the network administrator for TreyResearch.net. You're migrating from purely VPN remote access to primarily DirectAccess for remote access, with VPN for fallback only.

The sensitive nature of much of the research data that users work with is a compelling driver in the move to DirectAccess. You want to be sure that you can remotely manage the computers that are connecting to your network and that those computers are meeting all company policies.

1. **You want to include two-factor authentication in your rollout of DirectAccess. What are the choices available, and what are the factors favoring each? What hardware or software considerations does your choice of two-factor authentication entail?**
2. **Because you intend to keep VPN available as a fallback option, what changes can you make to ensure that VPN also works with two-factor authentication? What other suggestions do you have for improving the security of the VPN fallback?**

Objective summary

- DirectAccess can be installed for remote access and remote management, or for remote management only.
- Windows 8 and later clients do not require certificates for DirectAccess.
- To support Windows 7, DirectAccess must be configured with computer certificates.
- DirectAccess can be installed with one or two network adapters, and can be installed directly connected to the Internet, in a perimeter network, or behind a NAT device.
- Client computers must be explicitly allowed to connect via DirectAccess.
- DirectAccess is configured in four steps: Client, Server, Infrastructure Servers, and Application Servers.
- You can limit DirectAccess to mobile computers only.
- All DirectAccess computers must be domain joined.
- DirectAccess can be co-installed with VPN.

Objective review

1. You are the network administrator for TreyResearch.net. You have deployed DirectAccess, and initial acceptance has been good, but now some users report that they cannot connect to the corporate network since the rollout, but have used VPN as a fallback. Other users report that they can connect via DirectAccess without problems. Upon investigation, all users reporting that they cannot connect are on desktop computers. What are the possible causes? (Choose all that apply.)

   A. During initial setup, you configured DirectAccess with the Quick Start Wizard.

   B. During initial setup, you configured DirectAccess with the Remote Access Setup Wizard and cleared both the Use Force Tunneling and Enable DirectAccess for Mobile Computers Only check boxes in the DirectAccess Client Setup Wizard.

   C. During initial setup, you configured DirectAccess with the Remote Access Setup Wizard, and added the Mobile Computers Security Group and the Home Computers Security Group to the Enabled For DirectAccess field.

   D. All of the above.

   E. None of the above.

2. You are the network administrator for TreyResearch.net. Your current network topology has a single-edge device that performs firewall and NAT functions. All client computers run Windows 8.1 and use VPN for remote access. Your ISP has provided you with a single, static public IP address. You have been asked to deploy DirectAccess for remote access, and a server has been identified for the project. The server has a single network adapter. What are the minimum steps you need to do before you can enable DirectAccess? (Choose all that are required.)

   A. Purchase and install an additional network adapter for the identified server.

   B. Install Windows Server 2012 R2 on the identified server.

   C. Install the Remote Access role as a role on the server.

   D. Purchase an additional static IP address from your ISP.

   E. Decommission your existing edge device.

   F. All of the above.

   G. None of the above.

3. You are the network administrator for TreyResearch.net. After an initial test deployment of DirectAccess, which reported no issues, you have now deployed DirectAccess across all remote users. Users are reporting a significant slowing of Internet access. What are the possible causes? (Choose all that apply.)

   A. During initial setup, you configured DirectAccess with the Quick Start Wizard.

   B. During initial setup, you configured DirectAccess with the Remote Access Setup Wizard and selected Use Force Tunneling.

   C. During initial setup, you configured DirectAccess with the Remote Access Setup Wizard and selected Enable DirectAccess for Mobile Computers Only.

   D. None of the above.

Answers

This section contains the solutions to the thought experiments and answers to the lesson review questions in this chapter.

Objective 3.1: Thought experiment

1. Secondary zones provide fast and efficient lookups because they need updating only when there are actual changes. They are local to the users who use them, reducing network traffic. But they are a security concern because they have the full list of all servers and clients in the zone, and they are located in what is often a less-secure environment of the branch office. Other solutions that could be considered are stub zones or conditional forwarders. Both would have a higher initial network traffic, but local caching would quickly overcome that. Another possible solution is to consider putting a Read-Only Domain Controller (RODC) at the branch offices. Doing so would provide faster resource lookups with the Active Directory-integrated zones loaded as read-only DNS records and also enable faster logons because logons wouldn't have to authenticate to the main office.
2. This is a classic scenario for zone delegation. Create the zone delegations and give limited admin privilege to someone in the Engineering group who can take control of the process.
3. Looking beyond just DNS zones, you might consider setting up an aggressive DNS record aging and scavenging schedule to keep the zones from building up lots of dead records. Also consider creating DHCP reservations for most or all the computers in use. As the computers get repurposed and renamed, they continue to get the same IP address and settings, which will simplify keeping track of machines. Also, if there's a lot of full rebuild going on, this is a perfect fit for enabling Windows Deployment Services (WDS) in the department.

Objective 3.1: Review

1. **Correct answer:** C
   - A. **Incorrect**. You can't have both a zone file and a replication parameter.
   - B. **Incorrect**. You can't have both a zone file and a replication parameter, and the replication is to the Forest, not the domain.
   - C. **Correct**. Creates a primary zone, replicated to the domain.
   - D. **Incorrect**. Creates a primary zone, but with Forest-wide delegation.

2. **Correct answer:** B

   A. **Incorrect**. Secondary zones can't be Active Directory-integrated, so they can't have a Replication parameter.

   B. **Correct**. The NetworkID, zone master, and zone file name are all correctly identified.

   C. **Incorrect**. The zone file name is incorrect. It should be "10.168.192.in-addr.arpa".

   D. **Incorrect**. The zone file name is not in the required .in-addr.arpa format.

3. **Correct answer:** A

   A. **Correct**. Creates a delegation of the child zone named Engineering to the domain controller trey-engdc-8.engineering.treyresearch.net.

   B. **Incorrect**. The Name parameter should point to the parent domain, and the NameServer parameter should point to the name server of the child domain.

   C. **Incorrect**. The Name parameter should point to the parent domain.

   D. **Incorrect**. The NameServer parameter should point to the DNS server of the child domain.

Objective 3.2: Thought experiment

1. Because all three servers are on the same subnet, netmask ordering will treat them as equivalent. Therefore, by using round robin load balancing, users connect to "rdsh". The first user gets connected to rdsh1, the second to rdsh2, and the third to rdsh3. The fourth gets connected to rdsh1, and so on. If the Remote Desktop Gateway (RD Gateway) is configured correctly, when one of the servers is unavailable, it is dropped from the rotation.

2. If you have three RDSH servers—rdsh1, rdsh2, and rdsh3—start by making three new A records: rdsh pointing to the IP address of rdsh1, a second rdsh pointing to the IP address of rdsh2, and a third rdsh A record pointing to the IP address of rdsh3. You then create an RD Gateway–managed computer group and add rdsh plus rdsh1, rdsh2, and rdsh3 to the group; and create an RDSH farm with appropriate resource authorization policy (RAP) and connection authorization policy (CAP) policies for it.

Objective 3.2: Review

1. **Correct answers:** C, D, E
   - **A. Incorrect**. MX records are required only for mail servers.
   - **B. Incorrect**. Depending on the specific application and the service it is providing, you might need to create one or more SRV records. In a real exam question, this would be very clearly called out.
   - **C. Correct**. The basic Address record is required.
   - **D. Correct**. The basic IPv6 Address record is required.
   - **E. Correct**. If the network is using reverse lookup zones, one or two PTR records should be created (one for IPv4, and possibly one for IPv6 if the network uses reverse lookup records for IPv6). As with answer B, a real exam question would call out clearly whether reverse lookup was being used.
   - **F. Incorrect**. CNAME records are usually needed for very specialized circumstances. Although it's possible that a particular application server might require one, especially during a transition period from an earlier version, normally CNAME records are not used.
2. **Correct answer:** A
   - **A. Correct**. Creates a new name server record with the name "(same as parent folder)".
   - **B. Incorrect**. Creates a separate folder with the name ns13 instead of creating the NS record in the parent folder with (same as parent folder).
   - **C. Incorrect**. Misses the ZoneName parameter; instead, it has the zone name as the Name parameter.
   - **D. Incorrect**. Has the NameServer and Name parameters reversed.
3. **Correct answer:** C
   - **A. Incorrect**. You can't create or update the SOA record explicitly from Windows PowerShell.
   - **B. Incorrect**. You can't create or update the SOA record explicitly from Windows PowerShell.
   - **C. Correct**. The zone properties allow you to increment the version of the zone, which updates the SOA record.
   - **D. Incorrect**. You don't modify the SOA record at the server level, but at the zone level.

Objective 3.3: Thought experiment

1. Unfortunately, the VPN protocol with the widest range of support is the one you probably don't want to use: PPTP. There are a number of security vulnerabilities related to PPTP, so it is no longer recommended. Many older clients using PPTP supported only MS-CHAP, which is now gone from the PPTP list of authentication providers. L2TP is also reasonably well supported by a wide range of clients.
2. Beginning with Windows Vista, Windows clients all support SSTP, which has the distinct advantage of being able to work behind virtually any firewall. However, it is not well supported natively by other operating systems, although there are third-party products that provide support.
3. Beginning with Windows 7, Windows clients support IKEv2, also known as VPN Reconnect. IKEv2 supports user or machine authentication and has the capability to seamlessly reconnect the VPN when the network adapter changes.
4. Both smart cards and OTPs can be used with VPN and DirectAccess. With smart cards, Windows 8 and later mobile users who have a TPM chip on their computer can use virtual smart cards to simplify the user experience.
5. Regardless of whether you choose smart cards or OTPs, you have to implement a Public Key Infrastructure (PKI) to support computer certificates. If you choose OTP, you also have to implement RADIUS.

Objective 3.3: Review

1. **Correct answer:** C
   - A. **Incorrect**. This is a client-only cmdlet from the DISM module.
   - B. **Incorrect**. Installs the Remote Access role, but not the VPN or Routing role features.
   - C. **Correct**. Installs the Remote Access role and the DirectAccess-VPN and Routing role features. The DirectAccess-VPN role feature meets the VPN requirement in the question, and the Routing role feature meets the NAT requirement. The -IncludeManagementTools parameter ensures that all management tools are also installed.
   - D. **Incorrect**. Not an available Windows role. The RRAS role has been replaced by the Remote Access role, and VPNs have been combined with DirectAccess in a unified remote access role.

2. **Correct answer:** C

   A. **Incorrect**. All WAN miniport devices are installed by default.

   B. **Incorrect**. Removes one of the WAN miniports, but leaves L2TP and IKEv2 still available.

   C. **Correct**. Disables remote access for these protocols.

   D. **Incorrect**. This is an outgoing protocol, not an incoming one.

3. **Correct answers:** D, F

   A. **Incorrect**. Because DirectAccess is enabled, you make VPN changes on the Remote Access Management console.

   B. **Incorrect**. Because DirectAccess is enabled, you make VPN changes on the Remote Access Management console.

   C. **Incorrect**. You don't make DHCP reservations; instead, make a DHCP exclusion.

   D. **Correct**. You have to make a DHCP exclusion to ensure that the Remote Access server doesn't give a remote client the same IP address as an internal one.

   E. **Incorrect**. This would use DHCP, and the address assigned to the remote client would not be controlled by the Remote Access server.

   F. **Correct**. Enables the Remote Access server to control the assignment of IP addresses for remote VPN clients.

Objective 3.4: Thought experiment

1. Three choices are available: physical smart cards, virtual smart cards, and OTPs.

2. Physical smart cards are expensive and complicated to deploy, but can be easily integrated into the VPN strategy. You have to ensure that all users have a smart card reader, and provide a solution to reset the smart cards, and so on.

3. Virtual smart cards require only a TPM, and it is already company policy to require a TPM and BitLocker on all company mobile devices because they routinely work with sensitive data. With a TPM already assured, using virtual smart cards is a compelling solution. It does not, however, solve the issue of remote users who are on non-TPM desktop computers, and those users need to be addressed. However, the new corporate desktop specification includes at least two desktop options that have a TPM, so rolling that out to remote users should be a priority.

4. OTPs are simple and easy to use, require only a smartphone app for users to generate their password, and need no extra hardware for desktop users. However, they require deploying RADIUS servers, and do nothing to address desktop remote users who do not have a TPM and BitLocker, so you'd likely want to consider upgrading them even though you didn't plan to use virtual smart cards.

5. You should require two-factor authentication of VPN as well as DirectAccess, and deploy the same solution across both. Also consider removing PPTP and L2TP as VPN protocols.

Objective 3.4: Review

1. **Correct answer:** A
   - **A.** **Correct**. The Quick Start Wizard defaults to selecting the Enable DirectAccess for Mobile Computers Only option.
   - **B.** **Incorrect**. By clearing the Enable DirectAccess for Mobile Computers Only check box, DirectAccess is allowed for both mobile and non-mobile devices.
   - **C.** **Incorrect**. By adding the Home Computers and Mobile Computers security groups, both home users' and mobile users' computers are enabled for DirectAccess.
   - **D.** **Incorrect**. Only answer A is a possible cause of only mobile computers being able to connect via DirectAccess.
   - **E.** **Incorrect**. Only answer A is a possible cause of only mobile computers being able to connect via DirectAccess.
2. **Correct answers:** B, C
   - **A.** **Incorrect**. DirectAccess can be installed with a single network adapter.
   - **B.** **Correct**. Windows Server must be installed on the server.
   - **C.** **Correct**. The Remote Access role must be installed on the server.
   - **D.** **Incorrect**. Only a single public IP address is required.
   - **E.** **Incorrect**. With a single network adapter, DirectAccess can be installed behind a NAT device. If the edge device were decommissioned, you'd also need to add an additional network adapter, but you would have additional options for DirectAccess protocols.
   - **F.** **Incorrect**. Incorrect because A, D, and E are incorrect.
   - **G.** **Incorrect**. Incorrect because B and C are correct.

3. **Correct answer:** B

   A. **Incorrect.** Using the Quick Start Wizard would not have created a configuration that was affected by the number of actual users on the system.

   B. **Correct.** By selecting Use Force Tunneling, you have forced all remote traffic through the company's network connection. This actually causes a double load on the Internet connection, since remote users have to first connect inbound, and then outbound through the company's Internet connection. The extra load wasn't particularly noticeable for a few test users, but with many remote users you are now saturating the Internet connection, causing a general slowdown.

   C. **Incorrect.** This would have no effect on Internet connection speed for users.

   D. **Incorrect.** Since answer B is a possible answer, this can't be correct.

This page intentionally left blank

This page intentionally left blank

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z