Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

10970B

Networking with Windows Server®

Companion Content

Product Number: 10970B

Released: 02/2014

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.

b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.

c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.

e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.

f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.

g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.

h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.

i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.

j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.

k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.

n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.

o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. USE RIGHTS. The Licensed Content is licensed not sold. The Licensed Content is licensed on a ***one copy per user basis***, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

a. **If you are a Microsoft IT Academy Program Member:**
   i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   ii. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

   provided you comply with the following:
   iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
   iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
   v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
   vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member**:
i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
ii. For each license you acquire on behalf of an End User or Trainer, you may either:
    1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
    2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
    3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

    provided you comply with the following:
iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member**:

i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

ii. For each license you acquire on behalf of an End User or Trainer, you may either:

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,

iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,

v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,

viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,

ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and

x. you will only provide access to the Trainer Content to Trainers.

d. **If you are an End User:**

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

e. **If you are a Trainer.**

i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "*customize"* refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 **Redistribution of Licensed Content**. Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 **Third Party Notices**. The Licensed Content may include third party code tent that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code ntent are included for your information only.

2.5 **Additional Terms**. Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY. If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

c. **Pre-release Term**. If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE**. The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP**. Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS**. The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

7. **SUPPORT SERVICES**. Because the Licensed Content is "as is", we may not provide support services for it.

8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.

9. **LINKS TO THIRD PARTY SITES**. You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.

10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.

11. **APPLICABLE LAW.**
    a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.

12. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.
Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised July 2013

Module 1

Implementing IPv4 Services

Contents:

Lesson 1

Planning IPv4 Addressing

Contents:

Question and Answers

Understanding IPv4 Addresses and Address Types

Question: How is network communication affected if a default gateway is configured incorrectly?

Answer: A host with an incorrect default gateway will not be able to communicate with hosts on a remote network. To contact hosts outside the local network or network segment, a host must be able to contact a router that can provide the path to the destination IP. Communication on the local network is unaffected.

Creating Subnets in IPv4 Networks

Question: Does your organization use simple or complex networking?

Answer: Answers will vary. Most smaller organizations use simple networking to make configuration easier. Larger organizations with networking specialists are more likely to use complex networking.

Discussion: Planning Subnets

Question: How many subnets are required?

Answer: Five subnets are required. Four subnets are required for buildings, and one is required for the data center.

Question: How many bits are required to create that number of subnets?

Answer: Three bits are required, because three bits allow for 8 subnets.

Question: How many hosts are required on each subnet?

Answer: Each subnet must support 700 users and 14 printers, for a total of 714 hosts.

Question: How many bits are required to allow that number of hosts?

Answer: Ten bits are required to support up to 1,022 hosts.

Question: What is an appropriate subnet mask to meet these needs?

Answer: Several subnet masks can allow for the minimum number of networks and the minimum number of hosts:

- 255.255.224.0 (3 subnet bits, 13 host bits)
- 255.255.240.0 (4 subnet bits, 12 host bits)
- 255.255.248.0 (5 subnet bits, 11 host bits)
- 255.255.252.0 (6 subnet bits, 10 host bits)

Lesson 2

Managing and Troubleshooting IPv4 Connectivity

Contents:

Demonstration: How to Analyze Network Traffic by Using Microsoft Message Analyzer

Demonstration Steps

Capture network traffic with Microsoft Message Analyzer

Prepare to perform a packet capture

1. Sign in to LON-SVR2 as **Adatum\Administrator** with a password of **Pa$$w0rd**.
2. On the taskbar, click the **Windows PowerShell** icon.
3. At the Windows PowerShell command prompt, type **ipconfig /flushdns**, and then press Enter.
4. On the Start screen, click **Microsoft Message Analyzer**, and then click **Cancel** in the Microsoft Message Analyzer window.
5. In the navigation pane, click **Capture/Trace** and then, in the **Trace Scenarios** section, click **Firewall**.

Capture packets from a ping request

1. In Microsoft Message Analyzer, on the toolbar, click **Start With**.
2. At the Windows PowerShell command prompt, type **ping LON-DC1.adatum.com**, and then press Enter.
3. In Microsoft Message Analyzer, on the toolbar, click **Stop**.

Analyze the captured network traffic

1. In Microsoft Message Analyzer, in the results pane, select the first **ICMP** packet group.
2. In the result pane, click the plus icon (**+**) beside the selected packet group. Show that it includes both **Echo Request** and **Echo Reply** packets. This is a **ping** request.
3. View the source and destination IP addresses for each packet.

Filter the network traffic

1. On the Microsoft Message Analyzer toolbar, in the View Filter section, type the following into the box.

```
*DestinationAddress == 172.16.0.10
```

2. In the View Filter section, click **Apply Filter**. Explain that the packets have now been filtered to show only packets that match the filter.
3. Close Microsoft Message Analyzer without saving changes.

Lesson 3

Deploying Dynamic Host Configuration Protocol

Contents:

Demonstration: Creating and Configuring a DHCP Scope

Demonstration Steps

Install the DHCP server role

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the taskbar, click the **Server Manager** icon, and in **Server Manager**, click **Add roles and features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select the **DHCP Server** check box.
7. In the Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, wait until **Installation succeeded on LON-SVR1.Adatum.com** appears, and then click **Close**.
12. On the Server Manager dashboard, click **Tools**, and then click **DHCP**.
13. In the DHCP console, expand **lon-svr1.adatum.com**.
14. Right-click **lon-svr1.adatum.com**, and click **Authorize**.
15. In the DHCP console, right-click **lon-svr1.adatum.com**, and then click **Refresh**. Notice that the icons next to IPv4 and IPv6 change color from red to green, which means that DHCP server has been authorized in AD DS.

Create and configure a DHCP scope

1. In DHCP, in the navigation pane, click **lon-svr1.adatum.com**, expand **IPv4**, right-click **IPv4**, and then click **New Scope**.
2. In the New Scope Wizard, click **Next**.
3. On the **Scope Name** page, in the **Name** box, type **Branch Office**, and then click **Next**.
4. On the **IP Address Range** page, complete the page using the following information, and then click **Next**:
    - Start IP address: **172.16.0.100**
    - End IP address: **172.16.0.200**
    - Length: **16**
    - Subnet mask: **255.255.0.0**
5. On the **Add Exclusions and Delay** page, complete the page by using the following information:
    - Start IP address: **172.16.0.190**
    - End IP address: **172.16.0.200**
6. Click **Add**, and click **Next**.
7. On the **Lease Duration** page, click **Next**.

8. On the **Configure DHCP Options** page, click **Next**.
9. On the **Router (Default Gateway)** page, in the **IP address** box, type **172.16.0.1**, click **Add**, and then click **Next**.
10. On the **Domain Name and DNS Servers** page, click **Next**.
11. On the **WINS Servers** page, click **Next**.
12. On the **Activate Scope** page, click **Next**.
13. On the **Completing the New Scope Wizard** page, click **Finish**.

Create a Policy

1. In DHCP, in the navigation pane, click **lon-svr1.adatum.com**, expand **IPv4**, right-click **Policies**, and then click **New Policy**.
2. In the **Policy Name** field, type **Client1 Policy**, and then click **Next**.
3. On the **Configure Conditions for the policy** page, click **Add**.
4. In the Add/Edit Condition window, in the **Criteria** field, choose **MAC address**.
5. In the **Value** field, type **001DB7A63D11**, click **Add**, and then click **OK**.
6. In the DHCP Policy Configuration Wizard window, click **Next**.
7. On the **Configure settings for the policy** page, under **Available Options**, select **003 Router**, type **172.16.0.10** under IP address, click **Add**, and then click **Next** and then click **Finish**.

Note: Leave all virtual machines in their current state for the next demonstration.

Demonstration: Demonstration: Configuring a DHCP Relay Agent

Demonstration Steps

Install a DHCP relay agent

1. Switch to EU-RTR.
2. Sign in as **Adatum\Administrator** with the password of **Pa$$w0rd**.
3. In **Server Manager**, click **Tools**, and then click **Routing and Remote Access**.
4. In the navigation pane, expand **EU-RTR (local)**, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.
5. In the **Routing protocols** list, click **DHCP Relay Agent**, and then click **OK**.

Configure a DHCP Relay Agent

1. In the navigation pane, right-click **DHCP Relay Agent**, and then click **New Interface**.
2. In the **New Interface for DHCP Relay Agent** dialog box, click **Internal**, and then click **OK**.
3. In the **DHCP Relay Properties – Internal Properties** dialog box, click **OK**.
4. Right-click **DHCP Relay Agent**, and click **Properties**.
5. In the **DHCP Relay Agent Properties** dialog box, in the **Server address** box, type **172.16.0.10**, click **Add**, and then click **OK**.
6. Close Routing and Remote Access.

Lesson 4

Managing and Troubleshooting DHCP

Contents:

Demonstration: Configuring DHCP Failover

Demonstration Steps

1. Switch to LON-SVR1.
2. Open the DHCP management console, expand **LON-SVR1.Adatum.com**, right-click the **IPv4** node, and then click **Configure Failover**.
3. In the Configuration Failover Wizard, click **Next**.
4. On the **Specify the partner server to use for failover** page, in the **Partner Server** box, type **172.16.0.10**, and then click **Next**.
5. On the **Create a new failover relationship** page, in the **Relationship Name** box, type **Adatum**.
6. In the **Maximum Client Lead Time** field, set the hours to **0** and the minutes to **15**.
7. Ensure that the **Mode** field is set to **Load balance**.
8. Ensure the **Load Balance Percentage** is set to **50%**.
9. Check **State Switchover Interval**.
10. In the **Enable Message Authentication Shared Secret** box, type **Pa$$w0rd**, and then click **Next**.
11. Click **Finish**, and click **Close**.

Module Review and Takeaways

Review Question(s)

Question: You have just started as a server administrator for a small organization with a single location. The organization is using the 131.107.88.0/24 address range for the internal network. Is this a concern?

Answer: Yes, that is a concern because those are Internet-routable addresses. Most IPv4 networks use private addresses with NAT to allow access to the Internet. This organization will not be able to access the 131.107.88.0/24 network on the Internet.

Question: You are working for an organization that provides web hosting services to other organizations. You have a single /24 network from your ISP for the web hosts. You are almost out of IPv4 addresses and have asked ISP for an additional range of addresses. Ideally, you would like to supernet the existing network with the new network. Are there any specific requirements for supernetting?

Answer: Yes. To perform supernetting, the two networks must be consecutive. The networks must allow you to remove a single bit from the subnet mask and identify both as the same network.

Question: What are the two modes available when configuring DHCP Failover?

Answer: The two modes are hot standby and load balancing. Hot standby is commonly used for redundancy and load balancing is commonly used to scale a DHCP implementation to serve larger number of client computers.

Lab Review Questions and Answers

Lab A: Planning IPv4 Addressing

Question and Answers

Question: Why would A. Datum Corporation use separate IP address ranges for wired and wireless clients?

Answer: There could be several reasons, including the following:

- To be able to easily identify wired and wireless clients by IP address
- To filter traffic by IP address based on wired or wireless connection
- Wired and wireless networks typically use different physical infrastructure and, potentially, different IPv4 routing paths

Lab B: Implementing IPv4 Services

Question and Answers

Question: Why didn't you perform any configuration on NA-RTR for the wireless network subnets?

Answer: NA-RTR will not perform DHCP relay for the wireless connections. Each wireless access point in each branch location will be configured with DHCP relay to ensure that wireless clients receive appropriate addresses, according to the interface on which the DHCP request was received.

Question: Which Windows PowerShell cmdlet can you use to view the local routing table of a computer instead of using route print?

Answer: You can use the Get-NetRoute cmdlet to view the local routing table of a computer.

Module 2

Implementing Name Resolution by Using DNS

Contents:

Lesson 1

Implementing DNS Servers

Contents:

Demonstration: Installing the DNS Server Role

Demonstration Steps

1. Switch to LON-SVR1.
2. If necessary, on the taskbar, click **Server Manager**.
3. In Server Manager, in the navigation pane, click **Dashboard**, and then in the details pane, click **Add roles and features**.
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, in the **Roles** list, select the **DNS Server** check box.
8. In the **Add Roles and Features Wizard** dialog box, click **Add Features**.
9. On the **Select server roles** page, click **Next**.
10. On the **Select features** page, click **Next**.
11. On the **DNS Server** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.

Lesson 3

Configuring DNS Integration with AD DS

Contents:

Demonstration: Configuring AD DS Integrated Zones

Demonstration Steps

Promote LON-SVR1 as an additional domain controller

1. On LON-SVR1, in the Server Manager console, click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Domain Services**.
6. In the Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, when the **Installation succeeded** message displays, click **Close**.
11. In the Server Manager console, on the navigation page, click **AD DS**.
12. On the title bar where **Configuration required for Active Directory Domain Services at LON-SVR1** is displayed, click **More**.
13. On the **All Server Task Details and Notifications** page, click **Promote this server to a domain controller**.
14. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then click **Next**.
15. On the **Domain Controller Options** page, verify that the **Domain Name System (DNS) server** check box and the **Global Catalog (GC)** check box are selected. Type **Pa$$w0rd** in both boxes, and then click **Next**.
16. On the **DNS Options** page, click **Next**.
17. On the **Additional Options** page, click **Next**.
18. On the **Paths** page, click **Next**.
19. On the **Review Options** page, click **Next**.
20. On the **Prerequisites Check** page, click **Install**.

Note: The server will automatically restart as part of the procedure.

21. After LON-SVR1 restarts, sign in as **Adatum\Administrator**.

Create an Active Directory–integrated zone

1. On LON-DC1, open Server Manager.
2. Click **Tools**, and then click **DNS**.
3. In the DNS Manager console, click and then right-click **LON-DC1**, and then select **New Zone**.
4. In the New Zone Wizard, click **Next**.

5. On the **Zone Type** page, click **Primary zone**, ensure that the **Store the zone in Active Directory** option is selected, and then click **Next**.

Note: Point out that this option determines that that zone is in AD DS.

6. On the **Active Directory Zone Replication Scope** page, review the available options, and then without making any changes, click **Next**.
7. On the **Forward or Reverse Lookup Zone** page, select **Forward lookup zone**, and then click **Next**.
8. On the **Zone Name** page, in the **Zone name** box, type **Treyresearch.net**, and then click **Next**.
9. On the **Dynamic Update** page, review the available options, select **Allow only secure dynamic updates**, and then click **Next**.
10. On the **Completing the New Zone Wizard** page, click **Finish**.
11. In DNS Manager console, expand **Forward Lookup Zones**, click **Treyresearch.net**, and then review the records that are created automatically.

Create a record

1. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Treyresearch.net**.
2. Right-click **Treyresearch.net**, and then select **New Host (A or AAAA)**.
3. In the New Host window, in the **Name** box, type **www**; in the IP address box, type **172.16.0.100**; click **Add Host**; and then click **OK**.
4. Click **Done**.

Verify replication to a second DNS server

1. On **LON-SVR1**, in the **Server Manager** console, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **LON-SVR1**, expand **Forward Lookup Zones**, and then click **Treyresearch.net**.
3. Verify that the **www** resource record exists. It might take a couple of minutes for the record to appear, and you might have to refresh the console display.

Lesson 4

Configuring Advanced DNS Settings

Contents:

Demonstration: Configuring DNSSEC

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then in the drop-down list, click **DNS**.
2. In DNS, expand **LON-DC1**, expand **Forward Lookup Zones**, and then select and right-click **Adatum.com**.
3. On the menu, click **DNSSEC>Sign the Zone**.
4. In the **Zone Signing Wizard**, click **Next**.
5. Click **Customize zone signing parameters**, and then click **Next**.
6. On the **Key Master** page, click **The DNS server LON-DC1 is the Key Master**, and then click **Next**.
7. On the **Key Signing Key (KSK)** page, click **Next**.
8. On the **Key Signing Key (KSK)** page, click **Add**.
9. On the **New Key Signing Key (KSK)** page, click **OK**.
10. On the **Key Signing Key (KSK)** page, click **Next**.
11. On the **Zone Signing Key (ZSK)** page, click **Next**.
12. On the **Zone Signing Key (ZSK)** page, click **Add**.
13. On the **New Zone Signing Key (ZSK)** page, click **OK**.
14. On the **Zone Signing Key (ZSK)** page, click **Next**.
15. On the **Next Secure (NSEC)** page, click **Next**.
16. On the **Trust Anchors (TAs)** page, select the **Enable the distribution of trust anchors for this zone** check box, and then click **Next**.
17. On the **Signing and Polling Parameters** page, click **Next**.
18. On the **DNS Security Extensions** page, click **Next**, and then click **Finish**.
19. In DNS Manager, expand **Trust Points**, expand **com**, and then click **Adatum**. Ensure that the DNSKEY resource records exist, and that their status is valid.
20. In Server Manager, click **Tools**, and then in the drop-down list, click **Group Policy Management**.
21. In the Group Policy Management Console (GPMC), expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
22. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, and then click the **Name Resolution Policy** folder.
23. In the **Create Rules** section, in the **Suffix** box, type **Adatum.com** to apply the rule to the suffix of the namespace.
24. Select the **Enable DNSSEC in this rule** check box.
25. Select the **Require DNS clients to check that the name and address data has been validated by the DNS server** check box, and then click **Create**.
26. Close all open windows.

Lesson 5

Configuring DNS Resolution Between Zones

Contents:

Resources

What Is DNS Forwarding?

 **Best Practice:** Use a central forwarding DNS server for Internet name resolution. This security best practice can improve performance and simplify troubleshooting. You can locate the forwarding DNS server on a perimeter network, which ensures that no server within the network is communicating directly to the Internet.

Module Review and Takeaways

Review Question(s)

Question: If you have servers in a DNS zone with Internet-accessible domain names and IP addresses on both your local area network (LAN) and the Internet, how would you configure your DNS implementation to allow your clients to resolve the DNS names of these servers to the LAN-based IP address?

Answer: The ideal solution in this scenario would be to implement split DNS. You would configure a local area network (LAN)–based DNS server to host records for the zone in question, and then set up a conditional forwarder in your organization's DNS implementation to point to the LAN-based DNS server, which would resolve the host name to the LAN-based IP. Queries originating on the Internet would contact Internet-based DNS servers and resolve the host name to the Internet-based IP address.

Question: Why is it important to clear the DNS client resolver cache before testing a new DNS server configuration?

Answer: The DNS client resolver cache holds results of previous queries issued by the client, and it is checked before any other components in the DNS infrastructure. If a record for a host name has changed in the DNS server infrastructure, it will not be queried if a cached entry for that host name exists in the resolver cache.

Lab Review Questions and Answers

Lab: Planning and Implementing Name Resolution by Using DNS

Question and Answers

Question: What is the advantage of hosting Adatum.com as a secondary zone on SYD-SVR1?

Answer: The secondary zone is replicated from the master server (LON-DC1) and hosted locally. This means that SYD-SVR1 will have the same records as LON-DC1 and does need to contact LON-DC1 for name resolution for Adatum.com. SYD-SVR1 still needs to contact LON-DC1 periodically to check for newly created records, but name resolution for Adatum.com can be performed by SYD-SVR1 independently of LON-DC1.

Question: Why did you promote SYD-SVR1 to a domain controller?

Answer: When you host the DNS Server role on a domain controller, the DNS database is replicated to each Active Directory Domain Services domain controller in the domain, thereby creating automatic multimaster replication and redundancy for your DNS environment. It also ensures that every domain controller in your environment can resolve DNS queries, which is an important piece of Active Directory Domain Services functionality.

Module 3

Implementing IPv6

Contents:

Lesson 1

Overview of IPv6 Addressing

Contents:

Question and Answers

Understanding IPv6 Addresses

Question: Use the Calculator application on your computer to convert the following IPv6 address from binary to hexadecimal. Then, simplify the hexadecimal address by using zero compression.

Binary IPv6 address:

0010 0000 0000 0001 0000 1101 0001 0001 0010 0010 0011 0100 0000 0000 0000 0000

0000 0011 1011 1011 0000 0000 1010 1100 1011 1100 0011 1011 1010 1101 0110 1011

Answer: IPv6 address in hexadecimal format: 2001:0D11:2234:0000:03BB:00AC:CD39:AD6B

IPv6 address simplified by using zero compression: 2001:D11:2234::3BB:AC:CD39:AD6B

Demonstration: Configuring IPv6 Client Settings

Demonstration Steps

View IPv6 configuration by using IPconfig

1. On LON-DC1, click the Windows PowerShell icon on the taskbar.
2. At the Windows PowerShell command prompt, type **ipconfig**, and then press Enter.

   Notice that this returns a link-local IPv6 address.
3. Type **Get-NetIPAddress**, and then press Enter.

Configure IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**.
2. In the **Local Server Properties** dialog box, next to **Ethernet**, click **172.16.0.10, IPv6 Enabled**.
3. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
4. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.
6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::A**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **::1**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **OK**.
10. Close the **Network Connections** window.

Configure IPv6 on LON-SVR1

1. On LON-SVR1, in Server Manager, click **Local Server**.
2. In the **Local Server Properties** dialog box, next to Ethernet, click **172.16.0.11, IPv6 Enabled**.
3. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.

6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::15**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **OK**.
10. Close the **Network Connections** window.

Verify that IPv6 communication is functional

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell command prompt, type **ipconfig**, and then press Enter.

   Notice that both the link-local IPv6 address and the IPv6 address that you have configured are displayed.
3. At a command prompt, type **ping -6 lon-dc1**, and then press Enter.
4. Type **ping -4 lon-dc1**, and then press Enter.

Note: Leave all virtual machines in their current state for the subsequent demonstration.

Lesson 2

Implementing IPv6 and IPv4 Coexistence

Contents:

Demonstration: Configuring DHCP and DNS to Support IPv6

Demonstration Steps

Configure a scope and scope options in DHCP

1. On LON-DC1, on the taskbar, click the **Server Manager** icon, and then in the Server Manager window, in the top-right corner, click **Tools**, and then click **DHCP**.
2. In the DHCP console, in the navigation pane, expand **lon-dc1.adatum.com**, expand **IPv6**, right-click **IPv6**, and then click **New Scope**.
3. In the New Scope Wizard, click **Next**.
4. On the **Scope Name** page, in the **Name** box, type **Headquarters IPv6**, and then click **Next**.
5. On the **Scope Prefix** page, in the **Prefix** box, type **FD00:AAAA:BBBB:CCCC::B**, and then click **Next**.
6. On the **Add Exclusions** page, click **Next**.
7. On the **Scope Lease** page, click **Next**.
8. On the **Completing the New Scope Wizard** page, click **Finish**.

Configure DNS with an IPv6 host (AAAA) resource record

1. On LON-DC1, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Read the records listed for the zone and notice that LON-DC1 and LON-SVR1 have dynamically registered their IPv6 addresses with the DNS server.
4. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
5. In the New Host window, in the **Name** box, type **WebApp**.
6. In the **IP address** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **Add Host**.
7. Click **OK** to clear the success message.
8. Click **Done** to close the New Host window.

Verify name resolution for an IPv6 host (AAAA) resource record

1. On LON-SVR1, if necessary, open a Windows PowerShell command prompt.
2. At the Windows PowerShell command prompt, type **Test-NetConnection WebApp.adatum.com**, and then press **Enter**.

   The result should display **Ping Succeeded: True**.

Lesson 3

Transitioning from IPv4 to IPv6

Contents:

Resources

What Is PortProxy?

Additional Reading: For more information about IPv6 Transition Technologies, see IPv6 Transition Technologies at http://go.Microsoft.com/fwlink/?LinkID=112079&clcid=0x409

Module Review and Takeaways

Best Practices

Use the following best practices when implementing IPv6:

- Do not disable IPv6 on Windows Vista, Windows Server 2008, and newer Windows client and server operating systems.
- Enable coexistence of IPv4 and IPv6 in your organization rather than using transition technologies.
- Use unique local IPv6 addresses on your internal network.
- Use Teredo to implement IPv6 connectivity over the IPv4 Internet.

Review Question(s)

Question: What is the main difference between 6to4 and Teredo?

Answer: Both protocols allow IPv6 connectivity over the IPv4 Internet. However, only Teredo can provide connectivity through NAT.

Question: How can you provide a DNS server to an IPv6 host dynamically?

Answer: To provide a DNS server to an IPv6 host dynamically, you must use DHCPv6. You can use router advertisements to provide the network portion of an IPv6 address, but router advertisements cannot distribute DNS server IP addresses.

Question: Your organization is planning to implement IPv6 internally. After some research, you have identified unique local IPv6 addresses as the correct type of IPv6 addresses to use for private networking. To use unique local IPv6 addresses, you must select a 40-bit identifier that is part of the network. A colleague suggests using all zeros for the 40 bits. Why is this not a good idea?

Answer: The 40-bit organization identifier in a unique local IPv6 address should be randomly generated. This ensures the greatest likelihood that no two organizations are using the same organization identifier. If two organizations use the same organization identifier, the networks cannot be joined together after a merger.

Question: How many IPv6 addresses should an IPv6 node be configured with?

Answer: There is not specific number of IPv6 addresses that an IPv6 node should have; it depends on the configuration of the organization. Each IPv6 node has a link-local IPv6 address. In addition, it may also have a unique local IPv6 address for internal connectivity, and a global unicast IPv6 address for IPv6 Internet connectivity.

Lab Review Questions and Answers

Lab: Configuring and Evaluating IPv6 Transition Technologies

Question and Answers

Question: Did you configure IPv6 statically or dynamically in this lab?

Answer: You configured IPv6 dynamically in this lab. You added both IPv6 networks to the router, and the router advertisements configured LON-DC1 and LON-CL3 with the correct network address.

Question: Why did you not need to configure EU-RTR with the IPv4 address of the ISATAP router?

Answer: The default configuration for Windows client operating systems is set to resolve ISATAP by using DNS to locate the IPv4 address of the ISATAP router. EU-RTR used the default configuration.

Module 4

Implementing IPAM

Contents:

Lesson 2

Deploying IPAM

Contents:

Demonstration: Installing and Provisioning the IPAM Role

Demonstration Steps

Install IPAM

1. Sign in to LON-SVR2 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, in the results pane, click **Add roles and features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, select the **IP Address Management (IPAM) Server** check box.
8. In the **Add features that are required for IP Address Management (IPAM) Server** dialog box, click **Add Features**, and then click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. When the Add Roles and Features Wizard completes, close the wizard.

Configure IPAM

1. In the Server Manager navigation pane, click **IPAM**.
2. In the IPAM Overview pane, click **Connect to IPAM server**, select **LON-SVR2.Adatum.com**, and then click **OK**.
3. Click **Provision the IPAM server**.
4. In the Provision IPAM Wizard, click **Next**.
5. On the **Configure database** page, click **Next**.
6. On the **Select provisioning method** page, ensure that **Group Policy Based** is selected in the **GPO name prefix** box, type **IPAM**, and then click **Next**.
7. On the **Confirm the Settings** page, click **Apply**. Provisioning will take a few moments to complete.
8. When provisioning completes, click **Close**.
9. In the IPAM Overview pane, click **Configure server discovery**.
10. In the **Configure Server Discovery** dialog box, click **Add**, and then click **OK**.
11. In the IPAM Overview pane, click **Start server discovery**.

    Discovery might take 5–10 minutes to run. The yellow bar indicates when discovery is complete.
12. In the IPAM Overview pane, click **Select or add servers to manage and verify IPAM access**. Notice that the IPAM Access Status is **blocked** for LON-DC1. Scroll down to the **Details** view, and note the status report.

    The IPAM server has not yet been granted permission to manage LON-DC1 through Group Policy.
13. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**.
14. Open the Windows PowerShell command prompt, type the following command, and then press Enter.

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn
LON-SVR2.adatum.com –DelegatedGpoUser Administrator
```

15. When you are prompted to confirm the action, type **Y**, and then press Enter.

    The command will take a few moments to complete.

16. Close Windows PowerShell.
17. Switch to Server Manager.
18. In the IPv4 details pane, right-click **lon-dc1**, and then click **Edit Server**.
19. In the **Add or Edit Server** dialog box, in the **Manageability status** drop-down list, select **Managed**, and then click **OK**.

 **Note:** If a GPO error appears, switch the server back to **Unspecified**, and then restart LON-DC1 and LON-SVR2. Log back on to both servers as **Adatum\Administrator** with the password of **Pa$$w0rd**.

20. Switch to LON-DC1.
21. On the taskbar, click the **Windows PowerShell** icon.
22. At the Windows PowerShell command prompt, type **Gpupdate /force**, and then press Enter.
23. Close the Windows PowerShell window.
24. Switch back to LON-SVR2.
25. In Server Manager, right-click **LON-DC1**, and then click **Refresh Server Access Status**.
26. When completed, refresh IPv4 by clicking **Refresh**.

    It might take up to five minutes for the status to change. When the Data Retrieval Status displays the status as **Completed**, you may proceed.

27. In the IPAM Overview pane, click **Retrieve data from managed servers**.

    This action will take a few moments to complete.

Module Review and Takeaways

Question: What is the difference between an IP address block and an IP address range in IPAM?

Answer: An IP address block is a set of IP addresses that do not belong to a DHCP scope managed by IPAM. IP address ranges correspond to managed IP address space. You would typically create an IP address block to maintain inventory for a static IP range.

Question: Why would you reclaim an IP address in IPAM?

Answer: Typically you would reclaim an IP address from the list of available IP addresses because it has been allocated for use elsewhere in your environment, and is no longer an available IP address.

Question: Does IPAM provide any advantages if you are not centrally configuring or managing your IP addressing environment?

Answer: Yes. IPAM can still provide you with centralized monitoring of the IP addressing environment from a single console.

Lab Review Questions and Answers

Lab: Implementing IPAM

Question and Answers

Question: Why did you run the **Invoke-IpamGpoProvisioning** cmdlet?

Answer: You ran the **Invoke-IpamGpoProvisioning** cmdlet for setting the IPAM server permission to manage servers in the domain. When you run the command, it creates three GPOs that are linked to the domain. These GPOs apply permissions for management of DC, DNS, and DHCP servers in the domain.

Question: Why do only IP addresses and ranges from the Houston, Mexico City, and Portland locations appear in the IPAM console? Where are the IP addresses from the London, Toronto, and Sydney locations?

Answer: IPAM only displays IP address information for DHCP assigned IP addresses and address ranges. It does not specifically inventory, track, or manage statically assigned IP addresses.

Module 5

Implementing Remote Access

Contents:

Lesson 1

Remote Access Overview

Contents:

Demonstration: Installing and Managing the Remote Access Server Role

Demonstration Steps

Install the Remote Access server role

1. On LON-SVR1, switch to the Server Manager console, click **Manage**, and then click **Add Roles and Features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, click **Remote Access**, and then click **Next**.
6. On the **Select Features** page, click **Next**.
7. On the **Remote Access** page, click **Next**.
8. On the **Select role services** page, click **DirectAccess and VPN (RAS)**, and the in the **Add Roles and Features Wizard** dialog box, click **Add Features**.
9. Verify that **DirectAccess and VPN (RAS)** is selected, and on the **Select role services** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation finishes, click **Close**.

Manage the Remote Access server role

1. In the Server Manager console, in the upper-right part of the console, click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management console, review the options for configuring and managing remote access.
3. In the Server Manager console, in the upper-right part of the console, click **Tools**, and then click the **Routing and Remote Access**.
4. In the Routing and Remote Access console, review the options for configuring and managing remote access.

Lesson 2

Implementing DirectAccess by Using the Getting Started Wizard

Contents:

Question and Answers

How DirectAccess Works for Internal Clients

Question: How will you configure settings for different types of clients that need DirectAccess?

Answer: If you have clients that require secure remote access and you have internal computers that do not connect to the corporate network through the Internet, you might create separate computer groups for each of these clients, and then configure appropriate membership.

How DirectAccess Works for External Clients

Question: If you were using 6to4 instead of Teredo, would you need two IP addresses on the DirectAccess server?

Answer: No. DirectAccess first uses Teredo, and then tries 6to4. If 6to4 also fails, DirectAccess will then try HTTPS.

Demonstration: Running the Getting Started Wizard

Demonstration Steps

Create security group for DirectAccess client computers

1. On LON-DC1, on the task bar, click Server Manager.
2. In Server Manager, in the upper-right corner, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the Active Directory Users and Computers console tree, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **DA_Clients OU**, and then click **OK**.
5. In the Active Directory Users and Computers console tree, expand **Adatum.com**, right-click **DA_Clients OU**, click **New**, and then click **Group**.
6. In the **New Object - Group** dialog box, in the **Group name** box, type **DA_Clients**.
7. Under **Group scope**, ensure that **Global** is selected, and under **Group type**, ensure that **Security** is selected, and then click **OK**.
8. In the details pane, right-click **DA_Clients**, and then click **Properties**.
9. In the **DA_Clients Properties** dialog box, click the **Members** tab, and then click **Add**.
10. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.
11. In the **Enter the object names to select (examples)** box, type **LON-CL3**, and then click **OK**.
12. Verify that **LON-CL3** is displayed under **Members**, and then click **OK**.
13. Close the Active Directory Users and Computers console.

Configure DirectAccess by running the Getting Started Wizard

1. On EU-RTR, on the Start screen, click the **Server Manager** icon.
2. In Server Manager, click **Tools**, and then click **Remote Access Management**.
3. In the Remote Access Management console, under Configuration, click **DirectAccess and VPN**.
4. Click **Run the Getting Started Wizard**.

5. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
6. Verify that **Edge** is selected, in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** box, type **131.107.0.10**, and then click **Next**.
7. On the **Configure RemoteAccess** page, click the **here** link.
8. On the **Remote Access Review** page, verify that the two Group Policy Object (GPO) objects **Direct Access Server Settings** and **DirectAccess Client settings** are created.
9. Next to Remote Clients, click the **Change** link.
10. Select **Domain Computers (Adatum\Domain Computers)**, and then click **Remove**.
11. Click **Add**, type **DA_Clients**, click **OK**, ensure that the **Enable DirectAccess for mobile computers only** check box is cleared, and then click **Next**.
12. On the **Network Connectivity Assistant** page, click **Finish**.
13. On the **Remote Access Review** page, click **OK**.
14. On the **Configure Remote Access** page, click **Finish** to finish the wizard.
15. In the **Applying Getting Started Wizard Settings** dialog box, click **Close**.

Demonstration: Identifying the Getting Started Wizard Settings

Demonstration Steps

Review the configuration changes in the Remote Access Management console

1. On EU-RTR, switch to the Server Manager console, click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management console, in the left pane, click **DirectAccess and VPN**.
3. In the Remote Access Setup window, under the image of the client computer named **Step 1 Remote Clients**, click **Edit**.
4. In the DirectAccess Client Setup window, click **Deployment Scenario**, and review the default settings. Click **Select Groups**, and record the default settings. Click **Network Connectivity Assistant**, and then record the default settings.
5. Click **Cancel**, and then click **OK**.
6. In the Remote Access Setup window, under the image of the client computer named **Step 2 Remote Access Server**, click **Edit**.
7. In the Remote Access Server Setup window, click **Network Topology** and record the default settings. Click **Network Adapters**, and record the default settings. Click **Authentication**, and record the default settings.
8. Click **Cancel**, and then click **OK**.
9. In the Remote Access Setup window, under the image of the client computer named **Step 3 Infrastructure Servers**, click **Edit**.
10. In the Infrastructure Server Setup window, click **Network Location Server**, and record the default settings. Click **DNS**, and review the default settings. Click **DNS Suffix Search List**, and record the default settings. Click **Management**, and review the default settings.
11. Click **Cancel**, and then click **OK**.
12. In the Remote Access Setup window, under the image of the client computer named **Step 4 Application Servers**, click **Edit**.

13. In the DirectAccess Application Server Setup window, review the default settings, click **Cancel**, and then click **OK**.
14. Close all open windows.

Review the infrastructure changes in the Group Policy Management console

1. On EU-RTR, click the **Server Manager** icon, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management console, expand **Adatum.com**, and notice two new group policy objects are created: **DirectAccess Client Settings**, and **DirectAccess Server Settings**.
3. In the navigation pane, click the **DirectAccess Server Settings** GPO.
4. In the **Group Policy Management Console** dialog box, click **OK**, and then in the details pane, click the **Settings** tab.
5. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Settings** row, click the **show** link on the right side, and then in the **Windows Firewall with Advanced Security** row, click the **show** link.
6. Notice that there are three groups of firewall settings configured for the DirectAccess servers: **Global Settings**, **Inbound Rules**, and **Connection Security Settings**.
7. In the **Global Settings** row, click the **show** link, and then review the IPsec ICMP exception setting.
8. In the **Inbound Rules** row, click the **show** link, and then review the following settings:
   - **Core Networking – IPHTTPS (TCP-In)**. This rule allows the inbound Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) traffic to provide connectivity across HTTP proxies and firewalls.
   - **Domain Name Server (UDP-In)**, and **Domain Name Server (TCP-In)**. These rules allow traffic to the DNS64 server that is deployed on the Remote Access server. Notice the IPv6 address in the rules. It is the address of the **London_Network** adapter on EU-RTR, which can be verified by running the **ipconfig /all** command in the Windows PowerShell window
9. In the Connection Security Settings row, click the **show** link, and then in the Rules row, click the **show** link. Review the following settings:
   - **DirectAccess Policy-DaServerToCorpSimplified**. Review the IPv6 address prefixes, and compare them with the IPv6 address prefixes you recorded in step 7 of the previous section in this demonstration. Notice that they are the same prefixes configured in the Getting Started Wizard.
10. In the Rules row, click the **hide** link.
11. Under the Connection Security Settings row, in the First Authentication row, click the **show** link, and then review the Kerberos authentication setting.
12. Repeat step 11 for **Second Authentication**, **Key Exchange (Main Mode)**, and **Data Protection (Quick Mode)**.
13. In the navigation pane, click the **DirectAccess Client Settings** GPO.
14. In the **Group Policy Management Console** dialog box, click **OK**, and then in the details pane, click the **Settings** tab.
15. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, click the **show** link on the right side, then in the **Public Key Policies/Trusted Root Certification Authorities** row, click the **show** link, and then in the **Certificates** row, click on the **Show** link. Notice that the GPO is configuring the DirectAccess client computers to trust the self-signed certificates with the IP address of **131.107.0.10** and the name of **DirectAccess-NLS.Adatum.com**.

16. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, and in the Windows Firewall with Advanced Security row, click the **show** link.
17. Notice that there are three groups of firewall settings configured for the DirectAccess clients: **Global Settings**, **Outbound Rules**, and **Connection Security Settings**.
18. In the Global Settings row, click the **show** link, and then review the IPsec ICMP exception setting.
19. In the Outbound Rules row, click the **show** link, and then review the following settings:
    - **Core Networking – IP-HTTPS (TCP-Out)**. This rule allows the outbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
20. In the Connection Security Settings row, click the **show** link, and then in the Rules row, click the **show** link.
21. Review the three rules, and then compare the IPv6 address prefixes with the IPv6 address prefixes that you recorded in step 7 in the previous section of this demonstration. Notice that they are the same prefixes configured with the Getting Started Wizard.
22. In the Rules row, click the **hide** link.
23. Under the Connection Security Settings row, in the First Authentication row, click the **show** link, and then review the Kerberos authentication setting.
24. Repeat step 23 for **Second Authentication**, **Key Exchange (Main Mode)** and **Data Protection (Quick Mode)**.
25. Close the Group Policy Management Console.
26. On LON-DC1, click the **Server Manager** icon.
27. In Server Manager, click **Tools**, and then click **DNS**.
28. In the Domain Name System (DNS) Manager console, in the navigation pane, expand **Forward Lookup Zones**, expand **Adatum.com**, and then review the **A** and **AAAA** records for the following hosts: **directaccess-corpConnectivityHost**, **DirectAccess-NLS**, and **directaccess-WebProbeHost**. These records are created by the Getting Started Wizard.

Lesson 3

Implementing and Managing an Advanced DirectAccess Infrastructure

Contents:

Demonstration: Modifying the DirectAccess Infrastructure

Demonstration Steps

Configure the Remote Access server role

1. On EU-RTR, in Server Manager, on the **Tools** menu, click **Remote Access Management**.
2. In the Remote Access Management window, click **Direct Access and VPN**.
3. On **Step 1**, click **Edit** to select which clients will use DirectAccess.
4. On the **Deployment Scenario** page, click **Next**.
5. Under Select Groups, click **Next**.
6. On the **Network Connectivity Assistant** page, under the Resource column, delete the existing record by right-clicking on the arrow and then clicking **Delete**.
7. On the **Network Connectivity Assistant** page, under the Resource column, double-click the empty row.
8. In the Configure Corporate Resources for NCA window, verify that **HTTP** is selected, and then in the box next to **HTTP**, type **https://lon-svr1.adatum.com**. Click **Validate**, and then click **Add**.
9. On the **Network Connectivity Assistant** page, click **Finish**.
10. On **Step 2**, click **Edit**.
11. On the **Network Topology** page, verify that **Edge** is selected, type **131.107.0.10**, and then click **Next**.
12. On the **Network Adapters** page, ensure that the **Use a self-signed certificate created automatically by DirectAccess** check box is selected, verify that **CN=131.107.0.10** is used as a certificate to authenticate IP-HTTPS connections, and then click **Next**.
13. On the **Authentication** page, click **Use computer certificates**, click **Browse**, click **AdatumCA**, and then click **OK**.
14. Click **Enable Windows 7 client computers to connect via DirectAccess**, and then click **Finish**.
15. In the Remote Access Setup pane, under **Step 3**, click **Edit**.
16. On the **Network Location Server** page, select **The network location server is deployed on a remote web server (recommended)**, type **https://lon-svr1.adatum.com**, click **Validate**, and then click **Next**.
17. On the **DNS** page, click **Next**.
18. On the **DNS Suffix Search List** page, click **Next**.
19. On the **Management** page, click **Finish**.
20. Under **Step 4**, click **Edit**.
21. On the **DirectAccess Application Server Setup** page, click **Finish**.
22. Click **Finish** to apply the changes.
23. In the **Remote Access Review** page, click **Cancel**.

 **Note:** The DirectAccess configuration is not applied, because additional prerequisites need to be configured, such as AD DS configuration, firewall settings, and certificate deployment.

Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

Demonstration Steps

Verify DirectAccess Group Policy configuration settings for Windows 8 clients

1. Switch to LON-CL3.
2. Restart LON-CL3, and then sign in again as **Adatum\Administrator** with the password of **Pa$$w0rd**. Open the **Command Prompt** window, and then type the following commands, and pressing **Enter** at the end of each line.

```
gpupdate /force
gpresult /R
```

3. Verify that **DirectAccess Client Settings GPO** displays in the list of Applied Policy objects for the Computer Settings.

Move the client computer to the Internet virtual network

1. Switch to LON-CL3.
2. To move the client from the intranet to the public network, on LON-CL3, at the command prompt, type the following command, and then press Enter.

```
control
```

3. In Control Panel, under **Network and Internet** section, click **View network status and tasks**.
4. In Network and Sharing Center, click **Change adapter settings**.
5. Right-click **London_Network**, and then click **Disable**.
6. Right-click **Internet**, and then click **Enable**.
7. Close the Network Connections window.

Verify connectivity to the DirectAccess server

1. On LON-CL3, open a Command Prompt window.
2. At the command prompt, type the following command, and then press Enter:

```
ipconfig
```

   Notice the IP address that starts with 2002. This is IP-an HTTPS address.

3. At the command prompt, type the following command, and then press Enter.

```
Netsh name show effectivepolicy
```

Monitoring DirectAccess connectivity

1. Switch to EU-RTR.
2. On EU-RTR, open the Remote Access Management console, and then in the left pane, click **Dashboard**.
3. Review the information in the central pane, under the DirectAccess and VPN Client Status.
4. In the left pane, click **Remote Client Status**, and then in the central pane, review the information under the **Connected Clients** list.

   If no information appears under the **Connected Clients** list, restart **LON-CL3** and repeat step 4.

5. In the left pane, click **Reporting**, and then in the central pane, click **Configure Accounting**.
6. In the Configure Accounting window, under Select Accounting Method, click **Use inbox accounting**, click **Apply**, and then click **Close**.
7. In the central pane, under Remote Access Reporting, review the options for monitoring historical data.
8. Close the **Remote Access Management** console, and in the dialog box click **Yes**.

Lesson 4

Implementing VPN

Contents:

Demonstration: Configuring VPN

Demonstration Steps

Review the default VPN configuration

1. Switch to EU-RTR.
2. In Server Manager, on the **Tools** menu, click **Remote Access Management**.
3. In the Remote Access Management console, click **DirectAccess and VPN**, and then in the Tasks pane, under the VPN section, click **Enable VPN**.
4. In the **Enable VPN** dialog box, click **OK**, and then click **Close**.
5. Close the **Remote Access Management** console.
6. In Server Manager, on the **Tools** menu, click **Routing and Remote Access**.
7. In the Routing and Remote Access console, expand **EU-RTR**, right-click **Ports**, and then click **Properties**.
8. In the **Port Properties** dialog box, click **WAN Miniport (SSTP)**, and then click **Configure**. In the **Maximum ports** box, type **5**, and then click **OK**.
9. In the **Routing and Remote Access** message box, click **Yes**.
10. Repeat Step 7 for the following ports:
    - IKEv2
    - PPTP
    - L2TP
11. To close the **Ports Properties** dialog box, click **OK**.
12. Right-click **EU-RTR**, click **Properties**, and then on **General** tab, verify that IPv4 Remote Access Server is selected.
13. Click **Security**, and then verify that Certificate 131.107.0.10 is selected for SSL Certificate Binding.
14. Click **Authentication Methods**, verify that **EAP** is selected as the authentication protocol, and then click **OK**.
15. Click the **IPv4** tab, and verify that VPN server is configured in **IPv4 address assignment** with **Dynamic Host Configuration Protocol (DHCP)**.
16. To close the **EU-RTR Properties** dialog box, click **OK**.

Verify certificate requirements for IKEv2 and SSTP

1. Switch to EU-RTR.
2. On the Start screen, type **mmc**, and then press Enter.
3. In the MMC, click **File**, and then click **Add or Remove Snap-in**.
4. In Add or Remove Snap-in, click **Certificates**, click **Add**, click **Computer Account**, and then click **Next**.
5. Verify that **Local computer** is selected, and then click **Finish**.
6. To close the Add or Remove Snap-in, click **OK**.
7. In MMC, expand **Certificates** (Local Computer), expand **Personal**, and then click **Certificates**.

8. Notice that certificate 131.107.0.10 has **Intended Purpose** for **Server Authentication** (this is required for SSTP and IKEv2 VPN connectivity).
9. Close the console without saving the changes.

Configure the Remote Access server

1. On EU-RTR, in Server Manager, on the **Tools** menu, click **Network Policy Server**.
2. In the Network Policy Server console, expand **Policies**, and then click **Network Policies**.
3. In the details pane, right-click the policy at the top of the list, and then click **Disable**.
4. In the details pane, right-click the policy at the bottom of the list, and then click **Disable**.
5. In the navigation pane, right-click **Network Policies**, and then click **New**.
6. In the New Network Policy Wizard, in the **Policy name** box, type **VPN Policy**.
7. In the **Type of network access server** list, click **Remote Access Server(VPN-Dial up)**, and then click **Next**.
8. On the **Specify Conditions** page, click **Add**.
9. In the **Select condition** dialog box, click **Windows Groups**, and then click **Add**.
10. In the **Windows Groups** dialog box, click **Add Groups**.
11. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** box, type **IT**, and then click **OK**.
12. Click **OK** again to close the dialog box, and then click **Next**.
13. On the **Specify Access Permission** page, click **Access granted**, and then click **Next**.
14. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
15. To add EAP Types, click **Add**.
16. On the **Add EAP** page, click **EAP-MSCHAP v2**, and then click **OK**.
17. To add EAP Types, click **Add**.
18. On the **Add EAP** page, click **Microsoft: Smart Card or other certificate**, click **OK**, and then click **Next**.
19. On the **Configure Constraints** page, click **Next**.
20. On the **Configure Settings** page, click **Next**.
21. On the **Completing New Network Policy** page, click **Finish**.

Demonstration: How to Create a Connection Profile

Demonstration Steps

Install the CMAK feature

1. If necessary, on LON-CL3, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.
2. Pause your mouse pointer in the lower-left of the taskbar, and then click **Start**.
3. On the Start screen, type **Control Panel**, and then press Enter.
4. In Control Panel, click **Programs**, and then click **Programs and Features**.
5. In Programs, click **Turn Windows features on or off**.

6. In Windows Features, select the **RAS Connection Manager Administration Kit (CMAK)** check box, and then click **OK**.
7. Click **Close**.

Create a connection profile

1. In Control Panel, click **Control Panel Home**.
2. In the **View by** list, click **Large icons**.
3. Click **Administrative Tools**, and then double-click **Connection Manager Administration Kit**.
4. In the Connection Manager Administration Kit Wizard, click **Next**.
5. On the **Select the Target Operating System** page, click **Windows Vista or above**, and then click **Next**.
6. On the **Create or Modify a Connection Manager profile** page, click **New profile**, and then click **Next**.
7. On the **Specify the Service Name and the File Name** page, in the **Service name** text box, type **Adatum HQ**, in the **File name** box, type **Adatum**, and then click **Next**.
8. On the **Specify a Realm Name** page, click **Do not add a realm name to the user name**, and then click **Next**.
9. On the **Merge Information from Other Profiles** page, click **Next**.
10. On the **Add Support for VPN Connections** page, select the **Phone book from this profile** check box.
11. In the **VPN server name or IP address** text box, type **131.107.0.10**, and then click **Next**.
12. On the **Create or Modify a VPN Entry** page, click **Next**.
13. On the **Add a Custom Phone Book** page, clear the **Automatically download phone book updates** check box, and then click **Next**.
14. On the **Configure Dial-up Networking Entries** page, click **Next**.
15. On the **Specify Routing Table Updates** page, click **Next**.
16. On the **Configure Proxy Settings for Internet Explorer** page, click **Next**.
17. On the **Add Custom Actions** page, click **Next**.
18. On the **Display a Custom Logon Bitmap** page, click **Next**.
19. On the **Display a Custom Phone Book Bitmap** page, click **Next**.
20. On the **Display Custom Icons** page, click **Next**.
21. On the **Include a Custom Help File** page, click **Next**.
22. On the **Display Custom Support Information** page, click **Next**.
23. On the **Display a Custom License Agreement** page, click **Next**.
24. On the **Install Additional Files with the Connection Manager profile** page, click **Next**.
25. On the **Build the Connection Manager Profile and Its Installation Program** page, click **Next**.
26. On the **Your Connection Manager Profile is Complete and Ready to Distribute** page, click **Finish**.

Examine the created profile

1. On the desktop, on the taskbar, click the **File Explorer** icon.

2. In File Explorer, expand drive **C**, expand **Program Files**, expand **CMAK**, expand **Profiles**, expand **Windows Vista and above**, and then click **Adatum**.
3. In the details pane, review the files that display. These are the files that you must distribute.
4. Close all open windows.

Lesson 6

Implementing Web Application Proxy

Contents:

Demonstration: Publishing a Secure Website

Demonstration Steps

Install the Web Application Proxy role

1. Switch to EU-RTR.
2. On the **Start** screen, click **Server Manager**.
3. On the **Dashboard** page, click **Add roles and features**.
4. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**, on the **Select installation type** page, click **Next**, and then on the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **Remote Access**, click **Web Application Proxy**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

Obtain a certificate for the ADFS1 farm

1. On the Start screen, type **cmd**, and press Enter.
2. In the Command Prompt window, type **mmc**, and then press Enter.
3. In the MMC console, on the **File** menu, click **Add/Remove Snap-In**.
4. In **Add or Remove Snap-ins**, click **Certificates**, click **Add**, click **Computer account**, and then click **Next**.
5. Verify that **Local Computer** is selected, click **Finish**, and then click **OK**.
6. In the MMC, expand **Certificates (local Computer)**, expand **Personal**, and then click **Certificates**.
7. Right-click **Certificates**, click **All Tasks**, and then click **Request new Certificate**.
8. On the **Before You Begin** page, click **Next**.
9. On the **Select Certificate Enrollment Policy** page, click **Next**.
10. On the **Request Certificates** page, click **Adatum Web Certificate**, and then click **More information is required to enroll for this certificate. Click here to configure settings.**
11. In the **Subject Name** section, in the **Type** drop-down list, click **Common Name**, in the **Value** box type **adfs1.adatum.com**, and then click **Add**.
12. In the **Alternative name** section, in the **Type** drop-down list, click **DNS**, in the **Value** box type **adfs1.adatum.com**, and then click **Add**.
13. In the **Alternative name** section, in the **Type** drop-down list, click **DNS**, in the **Value** box type **enterpriseregistration.adatum.com**, and then click **Add**.
14. In the **Alternative name** section, in the **Type** drop-down list, click **DNS**, in the **Value** box type **lon-svr1.adatum.com**, and then click **Add**.
15. Click **OK** to close the **Certificate Properties** dialog box.
16. Click **Enroll** to proceed with Certificate Enrollment.
17. Click **Finish** to close the **Certificate Properties** dialog box.

Configure Web Application Proxy

1. In Server Manager, from the **Tools** menu, click **Remote Access Management**.
2. In the Remote Access Management console, in the navigation pane, click **Web Application Proxy**.
3. In the middle pane, click **Run the Web Application Proxy Configuration Wizard**.
4. In the Web Application Proxy Configuration Wizard, on the **Welcome** page, click **Next**.
5. On the **Federation Server** page, perform the following steps:
   a. In the **Federation service name** box, type **adfs1.adatum.com**.
   b. In the **User name** and **Password** boxes, type **Administrator** and **Pa$$w0rd**, and then click **Next**.
6. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, click **adfs1.adatum.com**, and then click **Next**.
7. On the **Confirmation** page, review the settings. If required, you can copy the Windows PowerShell cmdlet to automate additional installations. Click **Configure**.
8. On the **Results** page, verify that the configuration is successful, and then click **Close**.

Publish a sample web application

1. On the Web Application Proxy server, in the Remote Access Management console, in the navigation pane, click **Web Application Proxy**, and then in the Tasks pane, click **Publish**.
2. In the Publish New Application Wizard, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Pass-through**, and then click **Next**.
4. On the **Publishing Settings** page, perform the following steps:
   a. In the **Name** box, type **LON-SVR1 Web**.
   b. In the **External URL** box, type **https://lon-svr1.adatum.com**.
   c. In the **External certificate** list, click **adfs1.adatum.com**.
   d. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed, and then click **Next**. Note that this value is entered automatically when you enter the external URL.
5. On the **Confirmation** page, review the settings, and then click **Publish**. You can also opt to copy the Windows PowerShell command to set up additional published applications.
6. On the **Results** page, ensure that the application published successfully, and then click **Close**.

Disable DirectAccess on a client computer

1. Switch to LON-CL3.
2. On the Start screen, type **control**, and then press Enter.
3. In Control Panel, click **System**.
4. In the System window, under **Computer name, domain and workgroup settings**, click **Change Settings**.
5. In the **System Properties** dialog box, click **Change**.
6. In the **Computer Name/Domain Changes** dialog box, under **Member of** section, in the **Workgroup** box, type **Workgroup**, and then click **OK**.
7. In the **Computer Name/Domain Changes** dialog box, click **OK**.

8. If a **Windows Security** dialog box appears, in the **Username** box, type **Administrator**, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
9. In the **Welcome to the WORKGROUP workgroup** dialog box, click **OK**.
10. To restart the computer, click **OK**.
11. Click **Close** to close **System Properties** dialog box.
12. Click **Restart Now**.

Verify access to the internal website from the client computer

1. On LON-CL3, sign in with the username **Admin** and the password **Pa$$w0rd**.
2. On the Start screen, click the **Internet Explorer** tile.
3. In Internet Explorer, in the address bar, type **https://lon-svr1.adatum.com/**, and then press Enter.
4. In Internet Explorer, click the **Continue to this website (not recommended)** message.

   Note: This is expected behavior, since in this lab environment, the LON-SVR1 certificate is not trusted by LON-CL3. In a real world scenario, a trusted certificate should be used by the published server.
5. Verify that the sample application opens.
6. If you are unable to connect to **https://lon-svr1.adatum.com**, perform the following steps:
   a. On LON-CL3, open the Registry Editor window by running the **regedit.exe** tool. In the Registry Editor window, expand **HKLM**, expand **Software**, expand **Policies**, expand **Microsoft**, expand **Windows NT**, expand **DNSClient**, and then expand **DNSPolicyConfig**. Notice the three entries starting with **DA**.
   b. In the Registry Editor window, in the navigation pane, delete each of the entries starting with **DA**, and then close the Registry Editor window.
   c. Restart LON-CL3, and then perform steps 1 to 4 again, to verify the connectivity to the default IIS 8.0 webpage on LON-SVR1.
   d. Open File Explorer.
   e. In File Explorer, in the address bar, type **\\lon-svr1\Labfiles**, and then press Enter. Notice that you are unable to open the folder.

Module Review and Takeaways

Best Practices

- Although DirectAccess was present in previous Windows 7 and Windows 2008 R2 editions, Windows 8 introduces new features for improved manageability, ease of deployment, and improved scale and performance.
- You can monitor the DirectAccess environment by using Windows PowerShell and GUI tools, along with Network Connectivity Assistant on the client side.
- DirectAccess can now access IP4 servers on your network, and your servers do not require IPv6 addresses to be implemented through DirectAccess, because your DirectAccess server acts as a proxy.
- For ease of deployment, you do not need to have IP addresses on the Internet-facing network. Therefore, this is a good scenario for proof of concept. However, if you are concerned about security and if you want to integrate with NAP, you still need two public addresses.
- Consider integrating DirectAccess with your existing Remote Access solution. Windows Server 2012 can implement a DirectAccess server behind the NAT device, which is the most common remote access solution for organizations.

Review Question(s)

Question: What remote access solutions can you deploy by using Windows Server 2012 R2?

Answer: In Windows Server 2012 R2, you can deploy the following remote access solutions: DirectAccess, VPN, Routing, and Web Application Proxy.

Question: What are the main benefits of using DirectAccess for providing remote connectivity?

Answer: The main benefits of using DirectAccess for providing remote connectivity are as follows:

- Always-on connectivity. When the user is connected to the Internet, the user is also connected to the intranet.
- Users have the same experience regardless of whether they are connected locally or remotely.
- Bidirectional access. When the client computer is accessing the intranet, the computer is also connected and managed.
- Improved security. Administrators can set and control the intranet resources that are accessible through DirectAccess.

Question: How do you configure DirectAccess clients?

Answer: To configure DirectAccess clients, use Group Policy. When you use the Configure Remote Access Wizard to configure DirectAccess, two GPOs are created and linked to the domain. These two GPOs define DirectAccess-related settings, and are applied to the DirectAccess clients.

Question: How does a DirectAccess client determine if it is connected to the intranet or the Internet?

Answer: When you configure the DirectAccess server, you need to determine the computer that will be a network location server. The network location server should be a highly-available web server. Based on the response from this web server, the DirectAccess client determines if it is connected to the intranet or the Internet.

Question: What is the use of an NRPT?

Answer: NRPT stores a list of DNS namespaces and their corresponding configuration settings. These settings define the DNS server to contact, and the DNS client behavior for that namespace.

Question: What type of remote access solutions can you provide by using VPN in Windows Server 2012?

Answer: You can configure the following remote access solutions by using VPN in Windows Server 2012:

- Secure remote access to internal network resources for users located on the Internet. The users act as VPN clients that are connecting to Windows Server 2012, which acts as a VPN server.
- Secure communication between network resources that are located on different geographical locations or sites. This solution is called site-to-site VPN. In each site, Windows Server 2012 acts as a VPN server that encrypts communication between the sites.

Question: What type of applications can you publish by using Web Application Proxy in Windows Server 2012 R2?

Answer: Web Application Proxy in Windows Server 2012 R2 is a role service that you can use for publishing web applications. You can choose between two types of preauthentication for web applications:

- Active Directory Federation Services (AD FS) preauthentication, which uses AD FS for web applications that use claims-based authentication.
- Pass-through preauthentication, where a user connects to the web application through Web Application Proxy, and the web application authenticates the user.

Tools

Tool	Use for	Where to find it
Remote Access Management console	Managing DirectAccess and VPN	Server Manager/Tools
Routing and Remote Access console	Managing VPN and routing	Server Manager/Tools
Remote Access Getting Started Wizard	A graphical tool that simplifies DirectAccess configuration	Server Manager/Tools/Remote Access Management console
Web Application Proxy	Publishing web applications	Server Manager/Tools
Dnscmd.exe	A command-line tool used for DNS management	Run from command-line
Services.msc	Helps in managing Windows services	Server Manager/Tools
Gpedit.msc	Helps in editing the Local Group Policy	Run from command-line
IPconfig.exe	A command-line tool that displays the current TCP/IP network configuration	Run from command-line
DNS Manager console	Helps in configuring name resolution	Server Manager/Tools
Mmc.exe	Creates customized MMC for managing operating system roles, features, and	Run from command-line

Tool	Use for	Where to find it
	settings.	
Gpupdate.exe	Helps in managing Group Policy application	Run from command-line
Active Directory Users and Computers	Useful for configuring group membership for client computers that will be configured with DirectAccess	Server Manager/Tools

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You have configured DirectAccess, but users are complaining about connectivity issues. You want to troubleshoot those issues more efficiently.	Basic troubleshooting experience is integrated in Network Connectivity assistance, so educate users how to access it and to determine what is preventing the client computer from communicating with the DirectAccess server.
The DirectAccess client tries to connect to the DirectAccess server by using IPv6 and IPsec with no success.	If you are using Teredo as the IPv6 transition technology, verify whether you have two public addresses on the external network adapter of the DirectAccess server. This is required for establishing two IPsec tunnels.

Lab Review Questions and Answers

Lab A: Implementing DirectAccess by Using the Getting Started Wizard

Question and Answers

Question: Why did you create the DA_Clients group?

Answer: You created the DA_Clients group to apply DirectAccess security settings to the computers that are a member of this security group.

Question: How will you configure IPv6 address for client computers running Windows 8 to use DirectAccess?

Answer: Global unicast IPv6 addresses are generated automatically based on the network infrastructure. As a result, Windows 8 clients can connect to the company intranet and to the Internet by using DirectAccess, without requiring you to configure IPv6 addresses.

Lab B: Deploying an Advanced DirectAccess Solution

Question and Answers

Question: Why did you make the CRL available on the Edge server?

Answer: You made the CRL available on the Edge server so that the DirectAccess clients connecting through the Internet can access the CRL.

Question: Why did you install a certificate on the client computer?

Answer: Without a certificate, the DirectAccess server cannot identify and authenticate the client.

Lab C: Implementing VPN

Question and Answers

Question: In the lab, you configured the VPN server to allocate an IP address configuration by using a static pool of addresses. Is there a way for automatic IP configuration?

Answer: Yes, you could use a DHCP server on the internal network to allocate addresses.

Question: Why was DirectAccess not working when you removed LON-CL3 from the Adatum.com domain?

Answer: DirectAccess works only for domain-joined computers.

Lab D: Implementing Web Application Proxy

Question and Answers

Question: Where should you deploy the Web Application Proxy server?

Answer: You should deploy the Web Application Proxy server between the corporate network and the Internet.

Question: What is required for clients to access a published web application?

Answer: For clients to access a published web application, they must be able to resolve the external address of the application that is published by Web Application Proxy.

Module 6

Implementing Network Security

Contents:

Lesson 1

Managing Windows Firewall with Advanced Security

Contents:

Demonstration: Configuring Firewall Rules

Demonstration Steps

Allow ICMP traffic on LON-SVR1

1. Switch to LON-SVR1.
2. In Server Manager, click **Tools**, and then click **Windows Firewall with Advanced Security**.
3. In Windows Firewall with Advanced Security, click and then right-click **Inbound Rules**, and then click **New Rule**.
4. In the **New Inbound Rule Wizard** dialog box, click **Custom**, and then click **Next**.
5. On the **Program** page, click **Next**.
6. On the **Protocols and Ports** page, in the **Protocol type** list, click **ICMPv4**, and then click **Next**.
7. On the **Scope** page, click **Next**.
8. On the **Action** page, click **Allow the connection if it is secure**, and then click **Next**.
9. On the **Users** page, click **Next**.
10. On the **Computers** page, click **Next**.
11. On the **Profile** page, click **Next**.
12. On the **Name** page, in the **Name** box, type **ICMPv4 allowed**, and then click **Finish**.

Demonstration: Configuring Firewall Rules by Using GPOs

Demonstration Steps

Create an organizational unit

1. Switch to LON-DC1.
2. In the Server Manager window, click **Tools,** and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** console, in the navigation pane, right-click **Adatum.com**, point to **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **Member Servers**, and then click **OK**.
5. Right-click the **Member Servers** organizational unit, click **New**, and then click **Group**.
6. In the New Object – Group window, in the **Group Name** box, type **Application Servers**, and then click **OK**.
7. In the **Active Directory Users and Computers** console, in the navigation pane, click the **Member Servers** organizational unit; in the details pane, right-click **Application Servers** group; and then click **Properties**.
8. In the Application Servers Properties window, click the **Members** tab, and then click **Add**.
9. In Select Users, Contacts, Computers, Service Accounts, or Groups, click **Object Types**, select the **Computers** check box, and then click **OK**.
10. In the **Enter the object names to select** box, type **LON-SVR1**, and then click **OK** twice.

Configure Windows Firewall settings by using the new Group Policy Object (GPO)

1. On LON-DC1, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.

2. In the Group Policy Management Console, expand **Forests: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Group Policy Objects**, and then click **New**.
3. In the New GPO window, in the **Name** box, type **Application Servers GPO**, and then click **OK**.
4. In the Group Policy Management Console, expand **Group Policy Objects**, right-click **Application Servers GPO**, and then click **Edit**.
5. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Windows Firewall with Advanced Security**, and then click **Windows Firewall with Advanced Security - LDAP://CN={GUID}**.
6. In the Group Policy Management Editor, click **Inbound Rules**.
7. Right-click **Inbound Rules**, and then click **New Rule**.
8. In the New Inbound Rule Wizard, on the **Rule Type** page, click **Custom**, and then click **Next**.
9. On the **Program** page, click **Next**.
10. On the **Protocol and Ports** page, in the **Protocol type** list, click **TCP**.
11. In the **Local port** list, click **Specific Ports**; in the text box, type **8080**, and then click **Next**.
12. On the **Scope** page, click **Next**.
13. On the **Action** page, click **Allow the connection**, and then click **Next**.
14. On the **Profile** page, clear the **Private** and **Public** check boxes, and then click **Next**.
15. On the **Name** page, in the **Name** box, type **Application Server Department Firewall Rule**, and then click **Finish**.
16. Close the Group Policy Management Editor.

Link the GPO to the organizational unit

1. On LON-DC1, in the Group Policy Management Console, right-click **Member Servers**, and then click **Link an Existing GPO**.
2. In the Select GPO window, in **Group Policy objects** list, click **Application Servers GPO**, and then click **OK**.

Lesson 2

Configuring IPsec and Connection Security Rules

Contents:

Demonstration: Configuring Connection Security Rules

Demonstration Steps

Create a server–to-server rule on connecting servers

1. On LON-SVR1, in **Windows Firewall with Advanced Security**, click and then right-click **Connection Security Rules**, and then click **New Rule**.
2. In the New Connection Security Rule Wizard, click **Server-to-server**, and then click **Next**.
3. On the **Endpoints** page, click **Next**.
4. On the **Requirements** page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
5. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
6. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication methods**, click **Add**.
7. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.
8. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
9. On the **Authentication Method** page, click **Next**.
10. On the **Profile** page, click **Next**.
11. On the **Name** page, in the **Name** box, type **Adatum-Server-to-Server**, and then click **Finish**.

Create a server to server rule on LON-CL1

1. Switch to LON-CL1.
2. If required, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.
3. On the Start screen, type **Windows Firewall**, click **Windows Firewall**.
4. In Windows Firewall, click **Advanced settings**.
5. Click and then right-click **Connection Security Rules**, and then click **New Rule**.
6. In the New Connection Security Rule Wizard, click **Server-to-server**, and then click **Next**.
7. On the **Endpoints** page, click **Next**.
8. On the **Requirements** page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
9. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
10. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication methods**, click **Add**.
11. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.
12. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
13. On the **Authentication Method** page, click **Next**.
14. On the **Profile** page, click **Next**.
15. On the **Name** page, in the **Name** box, type **Adatum-Server-to-Server**, and then click **Finish**.

Test the rule

1. On the taskbar, click **Start**.
2. On the Start screen, type **cmd.exe**, and then press Enter.
3. At the command prompt, type **ping 172.16.0.11**, and then press Enter.
4. Switch to Windows Firewall with Advanced Security.
5. Expand **Monitoring**, expand **Security Associations**, and then click **Main Mode**.
6. In the right pane, double-click the listed item.
7. View the information in Main Mode, and then click **OK**.
8. Click **Quick Mode**.
9. In the right pane, double-click the listed item.
10. View the information in Quick Mode, and then click **OK**.

Lesson 3

Implementing Isolation Zones

Contents:

Demonstration: Implementing a Domain Isolation Zone

Demonstration Steps

Create a new GPO for the application of the domain isolation policy

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Right-click **Adatum.com**, point to **New**, and then click **Organizational Unit**.
3. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **Domain Isolation OU**, and then click **OK**.
4. In the navigation pane, click **Computers**.
5. Right-click **LON-SVR1**, and then click **Move**.
6. In the **Move** dialog box, click **Domain Isolation OU**, and then click **OK**.
7. Right-click **LON-SVR2**, and then click **Move**.
8. In the **Move** dialog box, click **Domain Isolation OU**, and then click **OK**.
9. In Server Manager, click **Tools**, and then click **Group Policy Management**.
10. In the Group Policy Management Console, expand **Forests: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Group Policy Objects**, and then click **New**.
11. In the New GPO window, in the **Name** box, type **Domain Isolation Policy**, and then click **OK**.

Create a firewall connection security rule for the domain isolation policy

1. In the Group Policy Management Console, right-click **Domain Isolation Policy**, and then click **Edit**.
2. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Windows Firewall with Advanced Security**, and then click **Windows Firewall with Advanced Security - LDAP://CN={GUID}**.
3. In the Group Policy Management Editor, click **Connection Security Rules**.
4. Right-click **Connection Security Rules**, and then click **New Rule**.
5. On the **Rule Type** page, click **Isolation**, and then click **Next**.
6. On the **Requirements** page, click **Require authentication for inbound connections and request authentication for outbound connections**, and then click **Next**.
7. On the **Authentication Method** page, click **Computer (Kerberos V5)**, and then click **Next**.
8. On the **Profile** page, clear both the **Private** and **Public** check boxes, and then click **Next**.
9. On the **Name** page, in the **Name** box, type **Domain Isolation**, and then click **Finish**.
10. Close the Group Policy Management Editor.

Link the GPO to the domain

1. In the Group Policy Management Console, right-click **Domain Isolation OU**, and then click **Link an Existing GPO**.
2. In the Select GPO window, in the **Group Policy objects** list, click **Domain Isolation Policy**, and then click **OK**.

Refresh the group policy on both servers

1. Restart LON-SVR1 and LON-SVR2.
2. Sign in to both servers as **Adatum\Administrator** with the password **Pa$$w0rd**.

3. Switch to LON-SVR1, and on the taskbar, click **Start**.
4. Type **cmd.exe**, and then press Enter.
5. At the command prompt, type **gpupdate /force**, and then press Enter.
6. Switch to LON-SVR2, and on the taskbar, click **Start**.
7. Type **cmd.exe**, and then press Enter.
8. At the command prompt, type **gpupdate /force**, and then press Enter.

Test the application of the domain isolation policy

1. Switch to LON-SVR2.
2. At the command prompt, type **net share C=C:**, and then press Enter.
3. Switch to LON-SVR1.
4. On the taskbar, click **File Explorer**.
5. In File Explorer, in the address bar, type **\\lon-svr2\c**, and then press Enter.
6. Click **Start**, and then type **Windows Firewall with Advanced Security** and press Enter.
7. In Windows Firewall with Advanced Security, expand **Monitoring**, expand **Security Associations**, and then click **Main Mode**.
8. In the right pane, double-click the listed item.
9. View the information in Main Mode, and then click **OK**.
10. Click **Quick Mode**.
11. In the right pane, double-click the listed item.
12. View the information in Quick Mode, and then click **OK**.

Module Review and Takeaways

Review Question(s)

Question: What are the recommended uses for IPsec?

Answer: The recommended uses for IPsec are the following:

- Packet filtering
- Securing host-to-host traffic
- Securing traffic to servers
- Layer Two Tunneling Protocol (L2TP)
- Site-to-site (gateway-to-gateway) tunneling
- Enforcing logical networks

Question: You need to ensure that traffic passing between a computer in the perimeter network and one deployed in the internal network is encrypted and authenticated. The computer in the perimeter is not a member of your AD DS forest. What authentication methods could you use if you attempted to establish an IPsec rule between these two computers?

Answer: You cannot use Kerberos because the perimeter computer is not in the forest. Therefore, you could use certificates or a preshared key.

Lab Review Questions and Answers

Lab: Implementing Network Security

Question and Answers

Question: What was your approach to the firewall and isolation planning exercise?

Answer: Answers will vary.

Module 7

Implementing Network Access Protection

Contents:

Lesson 1

Implementing NPS

Contents:

Question and Answers

What Is a Connection Request Policy?

Question: Identify the scenarios that would require custom connection policies.

Answer: Examples include a scenario in which policies exist with different realm names for RADIUS authentication and authorization, or in which you require a different accounting server.

Demonstration: Installing the NPS Role Service

Demonstration Steps

Install the NPS Role Service

1. Switch to LON-DC1.
2. If necessary, on the taskbar, click **Server Manager**.
3. In Server Manager, in the details pane, click **Add roles and features**.
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select the **Network Policy and Access Services** check box.
8. Click **Add Features**, and then click **Next** twice.
9. On the **Network Policy and Access Services** page, click **Next**.
10. On the **Select role services** page, verify that the **Network Policy Server** check box is selected, and then click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. Verify that the installation was successful, and then click **Close**.

Register NPS in AD DS

1. In Server Manager, click **Tools**, and then click **Network Policy Server**.
2. In Network Policy Manager, in the navigation pane, right-click **NPS (Local)**, and then click **Register server in Active Directory**.
3. In the **Network Policy Server** message box, click **OK**.
4. In the subsequent **Network Policy Server** dialog box, click **OK**.
5. Leave the Network Policy Server console window open.

Demonstration: Configuring a RADIUS Client

Demonstration Steps

1. Switch to EU-RTR.
2. In Server Manager, click **Tools**, and then click **Routing and Remote Access**.
3. In the **Routing and Remote Access** console, right-click **EU-RTR (local)**, and then click **Disable Routing and Remote Access**.
4. In the dialog box, click **Yes**.

5. In the **Routing and Remote Access** console, right-click **EU-RTR (local)**, and then click **Configure and Enable Routing and Remote Access**.
6. Click **Next**, select **Remote access (dial-up or VPN)**, and then click **Next**.
7. Select the **VPN** check box, and then click **Next**.
8. Click the network interface called **Internet**. Clear the **Enable security on the selected interface by setting up static packet filters** check box, and then click **Next**.
9. On the **Network Selection** page, in the **Network interfaces** list, click **London_Network**, and then click **Next**.
10. On the **IP Address Assignment** page, select **From a specified range of addresses**, and then click **Next**.
11. On the **Address Range Assignment** page, click **New**. Type **172.16.0.100** next to **Start IP address**, and type **172.16.0.110** next to **End IP address**, and then click **OK**, and then click **Next**.
12. On the **Managing Multiple Remote Access Servers** page, click **Yes, setup this server to work with a RADIUS server**, and then click **Next**.
13. On the **RADIUS Server Selection** page, in the **Primary RADIUS server** box, type **LON-DC1**.
14. In the **Shared secret** box, type **Pa$$w0rd**, and then click **Next**.
15. Click **Finish**.
16. In the **Routing and Remote Access** dialog box, click **OK**.
17. If prompted again, click **OK**.

Demonstration: Configuring a Connection Request Policy

Demonstration Steps

1. Switch to the LON-DC1 computer.
2. Switch to the Network Policy Server console.
3. In Network Policy Server, expand **Policies**, and then click **Connection Request Policies**.

   Notice the presence of the Virtual Private Network (VPN) Connections policies. The wizard created these automatically when you specified the NPS role service of this server.
4. Right-click **Connection Request Policies**, and then click **New**.
5. In the **New Connection Request Policy** Wizard, in the **Policy name** box, type **Adatum VPN**.
6. In the **Type of network access server** list, click **Remote Access Server (VPN-Dial up)**, and then click **Next**.
7. On the **Specify Conditions** page, click **Add**.
8. In the **Select condition** dialog box, select **NAS Port Type**, and then click **Add**.
9. In the **NAS Port Type** dialog box, select the **Virtual (VPN)** check box, click **OK**, and then click **Next**.
10. On the **Specify Connection Request Forwarding** page, click **Next**.
11. On the **Specify Authentication Methods** page, click **Next**.
12. On the **Configure Settings** page, click **Next**.
13. On the **Completing Connection Request Policy Wizard** page, click **Finish**.

14. In the **Connection Request Policies** list, if necessary right-click **Adatum VPN**, and then click **Move Up**.
15. Ensure that the Adatum VPN policy has a processing order of **1**. If not, repeat step 14.

Lesson 3

Configuring NAP

Contents:

Demonstration: Configuring NAP with DHCP Enforcement

Demonstration Steps

Configure NPS as a NAP Health Policy Server

1. Switch to LON-DC1.
2. Switch to Network Policy Server.
3. In the navigation pane, expand **Network Access Protection**, expand **System Health Validators**, expand **Windows Security Health Validator**, and then click **Settings**.
4. In the right pane, under **Name**, double-click **Default Configuration**.
5. In the navigation pane, click **Windows 8/Windows 7/Windows Vista**.
6. In the details pane, clear all check boxes except the **A firewall is enabled for all network connections** check box.
7. Click **OK** to close the **Windows Security Health Validator** dialog box.

Configure Health Policies

1. In the navigation pane, expand **Policies**.
2. Right-click **Health Policies**, and then click **New**.
3. In the **Create New Health Policy** dialog box, under **Policy name**, type **Compliant**.
4. Under **Client SHV checks**, verify that the **Client passes all SHV checks** check box is selected.
5. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, and then click **OK**.
6. Right-click **Health Policies**, and then click **New**.
7. In the **Create New Health Policy** dialog box, under **Policy Name**, type **Noncompliant**.
8. Under **Client SHV checks**, select **Client fails one or more SHV checks**.
9. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, and then click **OK**.

Configure Network Policies for Compliant Computers

1. In the navigation pane, under **Policies**, click **Network Policies**.

   Disable the two default policies found under **Policy Name** by right-clicking the policies and then clicking **Disable**.
2. Right-click **Network Policies**, and then click **New**.
3. On the **Specify Network Policy Name and Connection Type** page, under **Policy name**, type **Compliant-Full-Access**, and then click **Next**.
4. On the **Specify Conditions** page, click **Add**.
5. In the **Select condition** dialog box, double-click **Health Policies**.
6. In the **Health Policies** dialog box, under **Health policies**, select **Compliant**, and then click **OK**.
7. On the **Specify Conditions** page, click **Next**.
8. On the **Specify Access Permission** page, click **Next**.
9. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box, and then click **Next**.

10. Click **Next** again.
11. On the **Configure Settings** page, click **NAP Enforcement**. Verify that **Allow full network access** is selected, and then click **Next**.
12. On the **Completing New Network Policy** page, click **Finish**.

Configure Network Policies for Noncompliant Computers

1. Right-click **Network Policies**, and then click **New**.
2. On the **Specify Network Policy Name And Connection Type** page, under **Policy name**, type **Noncompliant-Restricted**, and then click **Next**.
3. On the **Specify Conditions** page, click **Add**.
4. In the **Select condition** dialog box, double-click **Health Policies**.
5. In the **Health Policies** dialog box, under **Health policies**, select **Noncompliant**, and then click **OK**.
6. On the **Specify Conditions** page, click **Next**.
7. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then click **Next**.
8. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box, and then click **Next**.
9. Click **Next** again.
10. On the **Configure Settings** page, click **NAP Enforcement**, and then click **Allow limited access**.
11. Clear the **Enable auto-remediation of client computers** check box.
12. Click **Next**, and then click **Finish**.

Configure the DHCP Server Role for NAP

1. In Server Manager, click **Tools**, and then click **DHCP**.
2. In DHCP, expand **LON-DC1.Adatum.com**, expand **IPv4**, right-click **Scope [172.16.0.0] Adatum**, and then click **Properties**.
3. In the **Scope [172.16.0.0] Adatum Properties** dialog box, click the **Network Access Protection** tab, click **Enable for this scope**, and then click **OK**.
4. In the navigation pane, under **Scope [172.16.0.0) Adatum**, click **Policies**.
5. Right-click **Policies**, and then click **New Policy**.
6. In the **DHCP Policy Configuration Wizard**, in the **Policy Name** box, type **NAP Policy**, and then click **Next**.
7. On the **Configure Conditions for the policy** page, click **Add**.
8. In the **Add/Edit Condition** dialog box, in the **Criteria** list, click **User Class**.
9. In the **Operator** list, click **Equals**.
10. In the **Value** list, click **Default Network Access Protection Class**, and then click **Add**.
11. Click **OK**, and then click **Next**.
12. On the **Configure settings for the policy** page, click **No**, and then click **Next**.
13. On the subsequent **Configure settings for the policy** page, in the **Vendor class** list, click **DHCP Standard Options**.
14. In the **Available Options** list, select the **006 DNS Servers** check box.

15. In the **IP address** box, type **172.16.0.10**, and then click **Add**.
16. In the **Available Options** list, select the **015 DNS Domain Name** check box.
17. In the **String value** box, type **restricted.adatum.com**, and then click **Next**.
18. On the **Summary** page, click **Finish**.
19. Close DHCP.

Configure Client NAP Settings

1. Switch to the LON-CL1 computer, and then sign in as **Adatum\administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **napclcfg.msc**, and then press Enter.
3. In **NAPCLCFG – [NAP Client Configuration (Local Computer)]**, in the navigation pane, click **Enforcement Clients**.
4. In the results pane, right-click **DHCP Quarantine Enforcement Client**, and then click **Enable**.
5. Close **NAPCLCFG – [NAP Client Configuration (Local Computer)]**.
6. On the taskbar, click **Start**.
7. On the Start screen, type **Services.msc**, and then press Enter.
8. In **Services**, in the results pane, double-click **Network Access Protection Agent**.
9. In the **Network Access Protection Agent Properties (Local Computer)** dialog box, in the **Startup type** list, click **Automatic**.
10. Click **Start**, and then click **OK**.
11. On the taskbar, click **Start**.
12. On the Start screen, type **gpedit.msc**, and then press Enter.
13. In the console tree, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Security Center**.
14. Double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**.
15. Close the console window.
16. Point to the lower-right corner of the taskbar, and then click **Settings**.
17. In the **Settings** list, click **Control Panel**.
18. In Control Panel, click **Network and Internet**.
19. In **Network and Internet**, click **Network and Sharing Center**.
20. In **Network and Sharing Center**, in the left pane, click **Change adapter settings**.
21. Right-click **London_Network**, and then click **Properties**.
22. In the **London_Network Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
23. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Obtain an IP address automatically**.
24. Click **Obtain DNS server address automatically**, and then click **OK**.
25. In the **London_Network Properties** dialog box, click **OK**.

Test NAP

1. On the taskbar, click **Start**.
2. On the Start screen, type **cmd.exe**, and then press Enter.
3. At the command prompt, type the following command, and then press Enter.

```
Ipconfig
```

4. Switch to **Services**.
5. In **Services**, in the results pane, double-click **Windows Firewall**.
6. In the **Windows Firewall Properties (Local Computer)** dialog box, in the **Startup type** list, click **Disabled**.
7. Click **Stop**, and then click **OK**.
8. In the notification area, click the **Network Access Protection** pop-up warning. Review the information in the **Network Access Protection** dialog box, and then click **Close**.

 **Note:** You might not receive a warning in the notification area, depending on the point at which your computer becomes noncompliant.

9. At the command prompt, type the following command, and then press Enter.

```
Ipconfig
```

10. Notice that the computer has a subnet mask of **255.255.255.255** and a Domain Name System (DNS) suffix of **restricted.Adatum.com**.
11. After you complete the demonstration, revert all virtual machines.

Lesson 4

Configuring IPsec Enforcement for NAP

Contents:

Demonstration: Configuring NAP Enforcement with IPsec

Demonstration Steps

Configure the CA and the required certificate

1. Switch to LON-DC1.
2. On the Start screen, type **certsrv.msc**, and then press Enter.
3. In the left pane, expand **AdatumCA**.
4. Right-click **Certificate Templates**, and then click **Manage**.
5. In the **Certificate Templates Console**, right-click **Workstation Authentication**, and then click **Duplicate Template**.
6. On the **General** tab, in **Template display name** box, type **Adatum Health Certificate**.
7. On the **Subject Name** tab, click **Supply in the request**, and then click **OK** to close the **Certificate Templates** warning.
8. On the **Extensions** tab, click **Application Policies**, and then click **Edit**.
9. In the **Edit Application Policies Extension** dialog box, click **Add**, select **System Health Authentication**, and then click **OK** twice to return to the **Properties of New Template** dialog box.
10. Click **OK** to close the **Properties of New Template** dialog box, and then close the **Certificate Templates Console**.
11. In the **certsrv - [Certification Authority(Local)\AdatumCA\Certificate Templates]** console, right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**.
12. Select **Adatum Health Certificate**, and then click **OK**.
13. In the Certification Authority console, in the left pane, right-click **AdatumCA**, and then click **Properties**.
14. On the **Security** tab, click **Add**.
15. Click **Object Types**, select the **Computers** check box, and then click **OK**.
16. On the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** box, type **LON-SVR2**, and then click **OK**.
17. On the **Security** tab, click **LON-SVR2**, select **Allow** for the **Read**, **Issue and Manage Certificates**, **Manage CA**, and **Request Certificates** check boxes, and then click **OK**.
18. Close the Certification Authority console.
19. On the taskbar, right-click **Windows PowerShell**, and then click **Run as Administrator**.
20. At the command prompt, type **Certutil -setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE**, and then press Enter.
21. At the command prompt, type **net stop certsvc**, and then press Enter.
22. At the command prompt, type **net start certsvc**, and then press Enter.

Install the Network Policy and Access Services role

1. Switch to LON-SVR2.
2. On the taskbar, click **Start**.
3. On the Start screen, type **mmc.exe**, and then press Enter.

4. On the **File** menu, click **Add/Remove Snap-in**.
5. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, and then click **Finish**.
6. In the **Add or Remove Snap-ins** dialog box, click **OK**.
7. In the console, expand **Certificates**, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
8. In the **Certificate Enrollment** dialog box, click **Next**.
9. On the **Select Certificate Enrollment Policy** page, click **Active Directory Enrollment Policy**, and then click **Next**.
10. Select the **Computer** check box, and then click **Enroll**.
11. Verify that the status of certificate installation is **Succeeded**, and then click **Finish**.
12. Close the Console1 window.
13. When prompted to save console settings, click **No**.
14. In Server Manager, in the Dashboard, click **Add roles and features**.
15. Click **Next** three times to get to the server role selection page.
16. On the **Select server roles** page, select **Network Policy and Access Services**, click **Add Features**, and then click **Next**.
17. Click **Next** twice.
18. On the **Select role services** page, select the **Network Policy Server** and the **Health Registration Authority** check boxes, click **Add Features**, and then click **Next**.
19. On the **Certification Authority** page, click **Use an existing remote CA**, and then click **Select**; on the **Select Certification Authority** page, select **AdatumCA**; click **OK**; and then click **Next**.
20. On the **Authentication requirements** page, click **Yes, require requestors to be authenticated as members of a domain**, and then click **Next**.
21. On the **Server Authentication Certificate** page, select the **LON-SVR2.Adatum.com** certificate that appears in the list, and then click **Next**.
22. Click **Next** twice.
23. On the **Confirm installation selections** page, click **Install**.
24. On the **Installation progress** page, verify that the installation was successful, and then click **Close**.

Configure the HRA

1. On LON-SVR2, in Server Manager, click **Tools**.
2. Click **Health Registration Authority**.
3. In the left pane, expand **Health Registration Authority (Local Computer)**, and then click **Certification Authority**.
4. In the details pane, confirm that **LON-DC1.Adatum.com\AdatumCA** is listed.
5. In the left pane, right-click **Certification Authority**, and then click **Properties**.
6. In the **Certification Authorities Properties** dialog box, click **Use enterprise certification authority**, and in **Authenticated compliant certificate template** and **Anonymous compliant certificate template**, select the **AdatumHealthCertificate** template.

7. Verify that the validity period for certificates approved by this Health Registration Authority is set to **4** hours, and then click **OK**.
8. Close the Health Registration Authority window.

Configure health policies

1. On LON-SVR2, in Server Manager, click **Tools**, and then click **Network Policy Server**.
2. In the details pane, click **Configure NAP**.
3. On the **Select Network Connection Method For Use with NAP** page, in **Network connection method,** select the **IPsec with Health Registration Authority (HRA)** check box, and then click **Next**.
4. On the **Specify NAP Enforcement Servers Running HRA** page, click **Next**.
5. On the **Configure Machine Groups** page, click **Next**.
6. On the **Define NAP Health Policy** page, clear the **Enable auto-remediation of client computers** check box, and then click **Next**.
7. Click **Finish**.
8. In the navigation pane, expand **Network Access Protection**, expand **System Health Validators**, expand **Windows Security Health Validator**, and then click **Settings**.
9. In the details pane, double-click **Default Configuration**.
10. In the **Windows Security Health Validator** window, clear all check boxes.
11. Select the **A firewall is enabled for all network connections** check box, and then click **OK**.
12. In the navigation pane, expand **Policies**, and then click **Health Policies**. Observe the two policies created.
13. Click **Network Policies**. Observe the two new policies.
14. Click **Connection Request Policies**. Observe the new policy.

 **Note:** Mention to the students that you are showing them only a subset of the procedure. Inform them that they will have an opportunity to perform the complete procedure during the lab.

Module Review and Takeaways

Question: Can you use the remote access NAP solution alongside the IPsec NAP solution? What benefit would this scenario provide?

Answer: Yes. You can use one or all of the NAP solutions in an environment. One benefit is that this solution would use IPsec to secure communication on the intranet, and not just the tunnel between the Internet host and the Remote Access server.

Question: On a client computer, what steps must you perform to ensure that the client's health is assessed?

Answer: You must perform the following steps to ensure that it can be assessed for health:

1. Enable the NAP enforcement client.
2. Enable the Security Center.
3. Start the NAP agent service.

Lab Review Questions and Answers

Lab A: Implementing NAP with VPN Enforcement

Question and Answers

Question: What role services must you deploy to support NAP?

Answer: You must deploy the NPS role service and, where required, Active Directory Certificate Services (AD CS). If you are implementing DHCP enforcement, you must deploy a DHCP server. VPN enforcement requires the Remote Access role and the DirectAccess and VPN (RAS) role service. If you are considering deploying NAP with IPsec enforcement, you must also deploy a Health Registration Authority (HRA) and Certificate Authority (CA).

Module 8

Implementing Networking for Branch Offices

Contents:

Lesson 1

Networking Features and Considerations for Branch Offices

Contents:

Question and Answers

Scenarios for Branch Offices

Question: Do these branch office scenarios apply to your organization? Does your organization experience any other branch office–related scenarios?

Answer: Answers will vary. This question is designed to encourage discussion in the classroom about real-life branch office scenarios. Have students describe their branch office scenarios and identify the issues they are experiencing in delivering applications and services to those branch offices.

Lesson 2

Implementing DFS for Branch Offices

Contents:

Question and Answers

Scenarios for Implementing DFS

Question: Why should you avoid using DFS to replicate high volume, transaction-based databases?

Answer: Databases with high-volume transactions typically leave several database files open in order to process the transactions. DFS cannot replicate files if they are held open by an application. Therefore, if you use DFS to replicate a high-volume, transaction-based database, the replicated copies of the database will not be consistent with the data.

Considerations for Implementing DFS

Question: You need to use DFS to ensure that a file share hosted on a file server running Windows Server 2008 R2 is replicated to another file server running Windows Server 2008 R2 in a branch office. The file share contains several virtual hard disk files that contain slightly different versions of the same base operating system image. Would Data Deduplication be effective in this situation?

Answer: Although Data Deduplication would work well with the data being replicated, you cannot use Data Deduplication in this scenario, because it is not available in Windows Server 2008 R2.

Demonstration: Demonstration: Configuring DFS Namespaces and Replication

Demonstration Steps

Install the DFS Replication role service

1. Switch to LON-SVR1.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, expand **File and Storage Services(installed)**, expand **File and iSCSI Services**, and then select the **DFS Namespaces** check box.
7. In the Add Roles and Features pop-up window, click **Add Features**.
8. Select the **DFS Replication** check box, and then click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation completes, click **Close**.
12. Repeat steps 1–11 for **TOR-SVR1**.

Create a new namespace

1. Switch to LON-SVR1.
2. In Server Manager, click **Tools**, and then click **DFS Management**.
3. In the **DFS Management** console, click **Namespaces**.
4. Right-click **Namespaces**, and then click **New Namespace**.
5. In the New Namespace Wizard, on the **Namespace Server** page, under **Server**, type **LON-SVR1**, and then click **Next**.

6. On the **Namespace Name and Settings** page, in the **Name** box, type **Research**, and then click **Next**.
7. On the **Namespace Type** page, ensure that both **Domain-based namespace** and **Enable Windows Server 2008 mode** are selected, and then click **Next**.
8. On the **Review Settings and Create Namespace** page, click **Create**.
9. On the **Confirmation** page, verify that the create namespace task is successful, and then click **Close**.
10. In the console, expand the **Namespaces** node, and then click **\\Adatum.com\Research**. Review the four tabs in the details pane.
11. In the console, right-click **\\Adatum.com\Research**, and then click **Properties**. Review the options on the **General**, **Referrals**, and **Advanced** tabs.
12. Click **OK** to close the **\\Adatum.com\Research Properties** dialog box.

Create a new folder and folder target

1. In the **DFS Management** console, right-click **\\Adatum.com\Research**, and then click **New Folder**.
2. In the **New Folder** dialog box, in the **Name** box, type **Proposals**.
3. In the **New Folder** dialog box, in the **Folder targets** section, click **Add**.
4. In the **Add Folder Target** dialog box, type **\\LON-SVR1\Proposal_docs**, and then click **OK**.
5. In the **Warning** dialog box, click **Yes** to create the shared folder.
6. In the **Create Share** dialog box, configure the following, and then click **OK**:
   - Local path of shared folder: **C:\Proposal_docs**
   - Shared folder permissions: **Administrators have full access; other users have read and write permissions**
7. In the **Warning** dialog box, click **Yes** to create the folder.
8. Click **OK** to close the **New Folder** dialog box.
9. In the console, expand **\\Adatum.com\Research**, and then click **Proposals**.

   Notice that currently there is only one **Folder Target**. To provide redundancy, a second folder target can be added with **DFS Replication** configured.
10. To test the namespace, open File Explorer, in the address bar, type **\\Adatum.com\Research**, and then press Enter.

    The Proposals folder is displayed.

Create a new folder target for replication

1. Switch to LON-SVR1.
2. In the **DFS Management** console, right-click the **Proposals** folder, and then click **Add Folder Target**.
3. In the **New Folder Target** dialog box, under **Path to folder target**, type **\\TOR-SVR1\Proposal_docs**, and then click **OK**.
4. In the **Warning** dialog box, click **Yes** to create the shared folder.
5. In the **Create Share** dialog box, in the **Local path of shared folder** box, type **C:\Proposal_docs**.
6. In the **Shared folder permissions** box, select the **Administrators have full access; other users have read and write permissions** check box, and then click **OK**.
7. In the **Warning** dialog box, click **Yes** to create the folder.

8. In the **Replication** dialog box, click **Yes** to create a replication group. The Replicate Folder Wizard starts.

Create a new replication group

1. In the **DFS Management** console, in the Replicate Folder Wizard, on the **Replication Group and Replicated Folder Name** page, accept the default settings, and then click **Next**.
2. On the **Replication Eligibility** page, note that LON-SVR1 and TOR-SVR1 are both eligible as DFS Replication members, and then click **Next**.
3. On the **Primary Member** page, select **LON-SVR1** as the primary member, and then click **Next**.
4. On the **Topology Selection** page, leave the default selection of **Full mesh**, which will replicate all data between all members of the replication group.

   If you had three or more members within the replication group, you can also choose **Hub and spoke**, which allows you to configure a publication scenario in which data is replicated from a common hub to the rest of the members. You can also choose **No topology**, which allows you to configure the topology at a later time.
5. After reviewing all the selections, click **Next**.
6. On the **Replication Group Schedule and Bandwidth** page, leave the default selection of **Replicate continuously using the specified bandwidth**, and then configure the setting to use **Full bandwidth**. Note that you can also choose a specific schedule to replicate during specified days and times. Click **Next**.
7. On the **Review Settings and Create Replication Group** page, click **Create**.
8. On the **Confirmation** page, ensure that all tasks are successful, and then click **Close**. Take note of the **Replication Delay** warning, and then click **OK**.
9. In the console, expand **Replication**.
10. Under **Replication**, click **Adatum.com\research\proposals**. Click and review each of the tabs in the details pane.

Lesson 3

Implementing BranchCache for Branch Offices

Contents:

Demonstration: Demonstration: Configuring BranchCache

Demonstration Steps

Add BranchCache for the Network Files Role Service

1. On LON-DC1, in Server Manager, click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (Installed)**, expand **File and iSCSI Services**, select the **BranchCache for Network Files** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation completes, click **Close**.

Enable BranchCache for the Server

1. On LON-DC1, click the Start screen.
2. On the Start screen, type **gpedit.msc**, and then press Enter.
3. Expand **Computer Configuration**, expand **Administrative Templates**, expand **Network**, click **Lanman Server**, and then double-click **Hash Publication for BranchCache**.
4. In the **Hash Publication for BranchCache** dialog box, click **Enabled**.
5. In the **Options** box, under **Hash publication actions**, select **Allow hash publication only for shared folder on which BranchCache is enabled**, and then click **OK**.
6. Close the Local Group Policy Editor.

Enable BranchCache for a File Share

1. On the taskbar, click the **File Explorer** icon.
2. In the File Explorer window, click **Local Disk (C:)**.
3. On the Quick Access Toolbar located on the upper-left side of the window, click **New Folder**, type **Share**, and then press Enter.
4. Right-click **Share**, and then click **Properties**.
5. In the **Share Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
6. In the **Advanced Sharing** dialog box, click **Share this folder**, and then click **Caching**.
7. In the **Offline Settings** dialog box, select the **Enable BranchCache** check box, and then click **OK**.
8. In the **Advanced Sharing** dialog box, click **OK**, and then click **Close**.
9. Close all open windows.

Module Review and Takeaways

Question: Why does DFS-R make a more efficient replication platform than file replication service (FRS)?

Answer: DFS-R uses an advanced delta-based heuristic, which only replicates modified portions of the file system, whereas file replication service (FRS) always replicates the complete file. DFS-R also uses RDC to reduce replication-based network traffic.

Question: How does BranchCache differ from the DFS?

Answer: BranchCache caches only files that users in a remote location have accessed. DFS replicates files between the head office and a remote location so that all files exist in both locations.

Question: Why would you want to implement BranchCache in hosted cache mode instead of distributed cache mode?

Answer: When you use the distributed cache mode, the cache is distributed to all computers running Windows 8. However, it is likely that computers or laptops that are running Windows 8 might be shut down or removed from the office. This means that a cached file might not be available, which will force the file to be downloaded across the WAN link again. However, if the hosted cache mode is used, the computer running Windows Server 2012 that is hosting the cache would make cached files available even if client computers are shut down or removed from the office.

Lab Review Questions and Answers

Lab: Implementing Networking for Branch Offices

Question and Answers

Question: What are the benefits of hosting a namespace on several namespace servers?

Answer: Hosting a namespace on several namespace servers increases availability if a namespace server fails. Users will still be able to access the namespace by using one of the remaining namespace servers. If a namespace is hosted on a single server, and that server becomes unavailable, clients will not be able to use namespace links to access shared folders on the network.

Question: In this lab, you moved SYD-SVR1 to its own organizational unit. Why?

Answer: The client configuration settings were configured in the Default Domain Policy, which is linked to the root of the domain. Those Group Policy settings prevent the hosted cache mode from being configured on SYD-SVR1. By moving SYD-SVR1 to its own organizational unit, you could block inheritance of Group Policy to that organizational unit, and prevent those settings from applying to SYD-SVR1.

Question: When would you consider implementing BranchCache into your own organization?

Answer: Answers will vary, but BranchCache is important only if you have a branch office or a location that is connected to your organization's headquarters with a low bandwidth link.

Module 9

Implementing Networking Infrastructure for File and Data Services

Contents:

Lesson 1

Implementing iSCSI

Contents:

Demonstration: Configuring an iSCSI Target and iSCSI Initiator

Demonstration Steps

Add the iSCSI Target Server Role Service

1. On LON-SVR2, in Server Manager, click **Manage**, and then click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File And Storage Services (Installed)**, expand **File and iSCSI Services**, select the **iSCSI Target Server** check box.
6. In the **Add Roles and Features** dialog box, click **Add Features**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. When the installation completes, click **Close**.

Create Two iSCSI Virtual Disks and an iSCSI Target

1. On LON-SVR2, in Server Manager, in the navigation pane, click **File and Storage Services**.
2. In the File and Storage Services pane, click **iSCSI**.
3. In the iSCSI Virtual Disks pane, click **Tasks**, and then in the **Tasks** drop-down list box, click **New iSCSI Virtual Disk**.
4. In the New iSCSI Virtual Disk Wizard, on the **Select iSCSI virtual disk location** page, under **Storage location**, click drive **C**, and then click **Next**.
5. On the **Specify iSCSI virtual disk name** page, type **iSCSIDisk1**, and then click **Next**.
6. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**; in the drop-down list, ensure **GB** is selected; and then click **Next**.
7. On the **Assign iSCSI target** page, click **New iSCSI target**, and then click **Next**.
8. On the **Specify target name** page, in the **Name** box, type **LON-SVR2**, and then click **Next**.
9. On the **Specify access servers** page, click **Add**.
10. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**; in the **Type** drop-down list, click **IP Address**; in the **Value** box, type **172.16.0.12**; and then click **OK**.
11. On the **Specify access servers** page, click **Next**.
12. On the **Enable Authentication** page, click **Next**.
13. On the **Confirm selections** page, click **Create**.
14. On the **View results** page, wait until the creation completes, and then click **Close**.
15. In the iSCSI Virtual Disks pane, click **Tasks**, and then in the **Tasks** drop-down list, click **New iSCSI Virtual Disk**.

16. In the New iSCSI Virtual Disk Wizard, on the **Select iSCSI virtual disk location** page, under **Storage location**, click drive **C**, and then click **Next**.
17. On the **Specify iSCSI virtual disk name** page, type **iSCSIDisk2**, and then click **Next**.
18. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**; in the drop-down list, ensure **GB** is selected; and then click **Next**.
19. On the **Assign iSCSI target** page, click **lon-svr2**, and then click **Next**.
20. On the **Confirm selections** page, click **Create**.
21. On the **View results** page, wait until the creation completes, and then click **Close**.

Connect to the iSCSI Target

1. On LON-SVR2, in Server Manager, click the **Tools** menu, and then click **iSCSI Initiator**.
2. In the **Microsoft iSCSI** message box, click **Yes**.
3. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, type **LON-SVR2**, and then click **Quick Connect**.
4. In the Quick Connect window, in the **Discovered targets** section, click **iqn.1991-05.com.microsoft:LON-SVR2-lon-svr2-target**, and then click **Done**.
5. In the **iSCSI Initiator Properties** dialog box, click **OK** to close the dialog box.

Verify the Presence of the iSCSI Drive

1. On LON-SVR2, in Server Manager, on the **Tools** menu, click **Computer Management**.
2. In the Computer Management console, under the **Storage** node, click **Disk Management**.

   Notice that the new disks are added. However, they all are currently offline and not formatted.
3. Close the Computer Management console.

Lab Review Questions and Answers

Lab: Implementing File and Data Networking Infrastructure

Question and Answers

Question: When you configured MPIO, both network adapters in each machine were connected to the same virtual network. In a physical environment, how can you make the MPIO connection between LON-SVR1 and LON-SVR2 more robust?

Answer: You can make the connection more robust by connecting each of the two network cards in each server to separate network switches. This would remove a switch as a single point of failure. If one of the switches that is connected fails, the connection will still be active through the network adapters connected to the other switch.

Question: Why is MPIO important for business-critical applications and services?

Answer: MPIO provides an easily configurable and automatic failover method to provide network redundancy through multiple network paths. This is extremely important when portions of your network might be susceptible to failure.

Module 10

Implementing and Managing Networking in Hyper-V

Contents:

Lesson 1

Creating and Using Hyper-V Virtual Switches

Contents:

Question and Answers

Types of Virtual Switches

Question: Can a virtual machine access the Internet if it is connected to an internal virtual switch?

Answer: If a virtual machine is connected to an internal virtual switch, in general, its connectivity is limited to:

- The Hyper-V host itself.
- Other virtual machines that are running on the same Hyper-V host and are connected to the same internal virtual switch

However, If the Hyper-V host has Internet connectivity and is configured to perform Network Address Translation (NAT), the virtual machine could also have Internet connectivity. To enable the Hyper-V host to use NAT, you need to configure the Routing and Remote Access Service on the host. You might use this option if the Hyper-V host is directly attached to the Internet, and the virtual machines are using private IP addresses.

What Is VLAN Tagging?

Question: Why is it that you can configure VLAN IDs for external and internal virtual switches, but not for a private virtual switch?

Answer: With external and internal virtual switches, the network adapter from the parent partition is connected to the virtual switch. But private virtual switches enable connectivity only to virtual machines, and no network adapter from the parent partition is connected to the private virtual switch. This is why you cannot configure VLAN ID for private virtual switch.

Question: Can two virtual machines on different hosts communicate with each other if you configure VLANs?

Answer: Yes, as long as the VLANs are configured on the virtual machine settings and on the physical network infrastructure.

Dynamic Switch Ports

Question: Is there any default Ethernet resource pool in Hyper-V?

Answer: When you install Hyper-V, there is a default Ethernet resource pool created, which is called primordial. You can view the resource pools by running the **Get-VMResourcePool** cmdlet. If you want to use an Ethernet resource pool, you should first create the pool.

Demonstration: Using Virtual Switch Manager

Demonstration Steps

1. On LON-HOST1, on the Start screen, start Hyper-V Manager.
2. In Hyper-V Manager, in the Actions pane, click **Virtual Switch Manager**.

   The Virtual Switch Manager for LON-HOST1 window opens.
3. In the Virtual Switch Manager for LON-HOST1 window, confirm that in the **Virtual Switches** section, only one virtual switch is listed and its name is **External Network**.
4. In the right pane, in the **Create virtual switch** section, click **Private**, and then click **Create Virtual Switch**.
5. In the Virtual Switch Manager for LON-HOST1 window, in the **Name** box, type **Private Switch**, and then click **OK**.

6. In **Hyper-V Manager**, right-click **10970B-LON-PROD1**, and then click **Settings**.
7. In the Settings for 10970B-LON-PROD1 window, in the left pane, click **Network Adapter**; in the **Virtual Switch** drop-down list, click **Private Switch**; and then click **OK**.
8. In **Hyper-V Manager**, right-click **10970B-LON-TEST1**, and then click **Settings**.
9. In the Settings for 10970B-LON-TEST1 window, in the left pane, click **Network Adapter**; in the **Virtual Switch** drop-down list, click **Private Switch**; and then click **OK**.
10. On LON-PROD1, on the Start screen, type **Windows PowerShell**. Right-click **Windows PowerShell**, and then click **Run as administrator**.
11. In the Windows PowerShell window, run the following command.

    ```
    ping 10.0.0.16
    ```

    Confirm that four replies are returned. (LON-TEST1 has IP address 10.0.0.16.)
12. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-PROD1**, and then click **Settings**.
13. In the Settings for 10970B-LON-PROD1 window, in the left pane, click **Network Adapter**; in the **Virtual Switch** drop-down list, click **External Network**; and then click **OK.**
14. On LON-PROD1, in the Windows PowerShell window, run the following command.

    ```
    ping 10.0.0.16
    ```

    Confirm that this time, the destination host is unreachable because LON-PROD1 is connected on a different virtual switch from LON-TEST1.

Demonstration: Configuring and Using VLANs

Demonstration Steps

1. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-TEST1**, and then click **Settings**.
2. In the Settings for 10970B-LON-TEST1 window, in the left pane, click **Network Adapter**; in the **Virtual Switch** drop-down list, click **External Network**; and then click **OK**.
3. On LON-PROD1, in the Windows PowerShell window, run the following command.

    ```
    ping 10.0.0.16
    ```

    If four replies are returned, you can confirm that LON-PROD1 and LON-TEST1 have network connectivity.
4. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-PROD1**, and then click **Settings**.
5. In the Settings for 10970B-LON-PROD1 window, in the left pane, click **Network Adapter**, and in right pane, click **Enable virtual LAN identification**. Verify that **2** is specified as **VLAN ID**, and then click **OK**.
6. On LON-PROD1, in Windows PowerShell, run the following command.

    ```
    ping 10.0.0.16
    ```

    Confirm that destination host is now not reachable, because LON-PROD1 is connected to different VLAN as LON-TEST1.
7. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-TEST1**, and then click **Settings**.

8. In the Settings for 10970B-LON-TEST1 window, in the left pane, click **Network Adapter**, and in the right pane, click **Enable virtual LAN identification**. Verify that **2** is specified as **VLAN ID**, and then click **OK.**
9. On LON-PROD1, in Windows PowerShell, run the following command.

```
ping 10.0.0.16
```

   Confirm that four replies are returned, which confirms that LON-PROD1 and LON-TEST1 have network connectivity, because now they are connected to the same VLAN.

Lesson 2

Configuring Advanced Hyper-V Networking Features

Contents:

Question and Answers

Virtual Switch Extensibility

Question: Can you write Hyper-V virtual switch extensions in Windows PowerShell?

Answer: You can use virtual switch extensions to process or inspect any network packet in the virtual switch, and therefore, you must compile and install them on the Hyper-V host. You can use Windows PowerShell to enable and manage virtual switch extensions but not to develop new extensions.

Advanced Network Adapter Features

Question: How can you monitor network traffic when you enable the port mirroring mode for a network adapter?

Answer: When you enable port mirroring in source mirroring mode, the Hyper-V virtual switch copies network traffic from the port to which the network adapter is connected, to the virtual switch port where the network adapter with mirroring mode destination is connected. You will still need to install and use network monitoring application in the virtual machine to be able to monitor network traffic.

Additional Network Adapter Configuration Options

Question: Do you need to enable DHCP Guard Protection on each virtual machine that you want to protect from obtaining TCP/IP configuration from the rogue DHCP server?

Answer: No, you do not have to enable DHCP Guard Protection on each virtual machine that you want to protect from obtaining TCP/IP configuration from the rogue DHCP server. You should enable this protection only on virtual machines in which the (potentially) rogue DHCP server is installed. When DHCP Guard Protection is enabled on a virtual machine, DHCP in that virtual machine will not be able to provide TCP/IP settings to other systems on the network. DHCP Guard Protection settings have no effect on whether the virtual machine can obtain TCP/IP settings.

What Are VMQ and dVMQ?

Question: Is VMQ beneficial when a virtual machine has to perform complex calculation and database searches?

Answer: VMQ enables efficient transfer of the incoming network traffic to a virtual machine. If a virtual machine is performing calculations on locally available data and it is not transferring large amounts of data over a network, then it is not benefiting from VMQ functionality. The same is true for database searches. However, virtual machines can benefit from using VMQ when you have to transfer large amounts of network traffic such as the results of database searches from different computers or when you have to access a network shared folder to copy files.

NIC Teaming in Virtual Machines

Question: Is there any special hardware requirement if you want to use NIC Teaming in virtual machines?

Answer: You can enable and use NIC Teaming in virtual machines regardless of the model, network speed, and configuration of the network adapters, or the manufacturer of the network adapter. This means that there are no special hardware requirements to use NIC Teaming in virtual machines. But if you want to have redundancy, a virtual machine should have at least two network adapters in a NIC team.

Demonstration: Configuring Network Adapter Advanced Features

Demonstration Steps

1. On LON-PROD1, on the desktop, on the taskbar, click **File Explorer**. The **This PC** window opens.
2. In the **This PC** navigation pane, expand **This PC**, expand **Local Disk (C:)**, and then click **Windows**.
3. In the details pane, right-click the **Inf** folder, and then click **Copy**.
4. In the Windows window, in the address bar, click the arrow, type **\\10.0.0.16\share**, and then press Enter.
5. In the **share** window, right-click in the details pane, and then click **Paste**.

   A window that shows the progress of the copy process is displayed. Note the copy speed and how long the process takes.
6. When the copy process is complete, right-click the **Inf** folder, click **Delete**, and then in the **Delete Folder** dialog box, click **Yes**.
7. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-PROD1**, and then click **Settings**.
8. In the Settings for 10970B-LON-PROD1 window, in the left pane, click **Network Adapter**; in the details pane, click **Enable bandwidth management**; in the **Minimum bandwidth** box, type **10**; in the **Maximum bandwidth** box, type **10**; and then click **OK**.
9. On LON-PROD1, in the Share window, right-click in the details pane, and then click **Paste**.

   A window that shows the progress of the copy process is displayed. Confirm that copy process takes longer to complete than it did before you configured bandwidth management.
10. On LON-PROD1, in Windows PowerShell, run the following cmdlet to configure LON-PROD1 to obtain an IP address automatically from a DHCP server.

    ```
    Set-NetIPInterface –InterfaceAlias Ethernet –dhcp enabled
    ```
11. On LON-PROD1, in Windows PowerShell, run the following commands.

    ```
    ipconfig /release
    ipconfig /renew
    ```

    By running these commands, you renewed TCP/IP settings on LON-PROD1. As the output shows, TCP/IP settings were obtained successfully.
12. On LON-HOST1, in Hyper-V Manager, right-click **10970B-LON-DC1B**, and then click **Settings**.
13. In the Settings for 10970B-LON-DC1B window, in the left pane, expand **Legacy Network Adapter**; click **Advanced Features**; in the right pane, select the **Enable DHCP guard** check box, and then click **OK**.
14. On LON-PROD1, in Windows PowerShell, run the following commands.

    ```
    ipconfig /release
    ipconfig /renew
    ```

Note: This time, it takes considerably longer than it did before you configured DHCP guard, and LON-PROD1 is not able to obtain TCP/IP settings. When you enable DHCP guard on the virtual machine where a rogue DHCP server is running, you cannot get TCP/IP settings from that virtual machine.

Lab Review Questions and Answers

Lab: Creating and Configuring Virtual Machine Networks

Question and Answers

Question: Can you connect a virtual machine that is running on Hyper-V to an external Hyper-V virtual switch that you created on different Hyper-V host?

Answer: You can connect a virtual machine only to Hyper-V virtual switches that are created on the Hyper-V host on which that virtual machine is running. You cannot connect a virtual machine that is running on one Hyper-V host to a virtual switch that was created on another Hyper-V host.

Question: Can you add a virtual network adapter to the parent partition by using Hyper-V Manager?

Answer: The parent partition is a virtual machine in which you can manage and monitor Hyper-V and in which device drivers for accessing Hyper-V physical hardware are installed. You can add virtual network adapters to a parent partition just as you can add them to other virtual machines, but you cannot do so by using Hyper-V Manager. You can do this only by using the **Add-VMNetworkAdapter** Windows PowerShell cmdlet with the **ManagementOS** parameter.

Question: Can you change an internal virtual switch to an external virtual switch?

Answer: Yes, you can change an internal virtual switch to an external virtual switch. By doing so, virtual machines that were limited in connectivity to other virtual machines connected to the same internal virtual switch will also have access to the external network, as will the Hyper-V host on which internal virtual switch was created. But when you change the switch type, you will not be able to enable SR-IOV, because you can enable this option only when virtual switch is created.

Question: Is DHCP guard enabled by default? Where can you change this setting and why would you use it?

Answer: The DHCP guard option is disabled by default. You can change this option on the Advanced Features settings page of the network adapter, and you should enable it on the network adapters of the virtual machine, where a potentially rogue DHCP server could be installed. When the DHCP guard option is enabled, the DHCP server in the virtual machine on which this option is enabled will not be able to lease TCP/IP settings on the network.

Module 11

Virtualizing Your Network Infrastructure

Contents:

Lesson 1

Implementing Hyper-V Network Virtualization

Contents:

Question and Answers

What Is Network Virtualization Generic Routing Encapsulation?

Question: Does a virtual machine customer address change when you move the virtual machine between Hyper-V hosts?

Answer: When you move a virtual machine, its customer address stays the same. The only thing that changes is its provider address, which is the address of the Hyper-V host on which it is running. You must update the network virtualization configuration on the Hyper-V hosts so that Hyper-V hosts are aware of the move.

What Are Network Virtualization Policies?

Question: Why are network virtualization policies needed when using network virtualization?

Answer: Network virtualization policies define on which Hyper-V host the virtual machines are running. Hyper-V consults network virtualization policies when it needs to form an NVGRE–encapsulated packet and send it on a physical network.

Resources

What Is Network Virtualization Generic Routing Encapsulation?

Additional Reading: For more information about network virtualization, go to the following website:
http://go.microsoft.com/fwlink/?LinkID=331220

Demonstration: Configuring Network Virtualization

Demonstration Steps

1. On LON-PROD1, on the Start screen, search for and start Windows PowerShell.
2. In the Windows PowerShell window, run the following three commands.

```
ping 10.0.0.16
ping 10.0.0.25
ping 10.0.0.26
```

3. Confirm that four replies are returned for each command.

   This confirms that LON-PROD1 has connectivity with LON-TEST1, LON-PROD2, and LON-TEST2.

4. On LON-HOST1, on the taskbar, click **Windows PowerShell**.
5. In the Windows PowerShell window, run the following cmdlet.

```
Get-VMNetworkAdapter –VMName 10970B-LON-PROD1 | fl
```

6. Confirm that the **VirtualSubnetId** property has the value **0**, which means that virtual subnets are not used.
7. In the Windows PowerShell window, run the following cmdlet.

```
Get-NetAdapter
```

8. For the Ethernet 2 adapter, under the **ifIndex** column, write down the index number.
9. On LON-HOST2, in the Windows PowerShell window, run the following cmdlet.

```
Get-NetAdapter
```

10. For the Ethernet 2 adapter, under the **ifIndex** column, write down the index number.
11. On LON-HOST1, on the desktop, on the taskbar, click **File Explorer**.

    The PC window is displayed.
12. In the This PC pane, expand **Local Disk (C:)**, and then click **Labfiles**.
13. In the details pane, right-click **ConfigureNW1.ps1** file, and then click **Edit**.

    The **ConfigureNW1.ps1** file opens in Windows PowerShell Integrated Scripting Environment (ISE).
14. Review the Windows PowerShell script to see how network virtualization is configured. Also, review the variables, which are defined at the start of the script.
15. In Windows PowerShell ISE, click **Run Script** on the toolbar. (Alternatively, you can press F5.)
16. Type the number of the index for Ethernet 2 on LON-HOST1, and then press Enter.
17. Type the number of the index for Ethernet 2 on LON-HOST2, and then press Enter.
18. On LON-HOST1, in Windows PowerShell ISE, in the console (lower pane), run the following cmdlet.

```
Get-VMNetworkAdapter –VMName 10970B-LON-PROD1 | fl
```

19. Confirm that the **VirtualSubnetId** property has the value **5001**, which was configured by the Windows PowerShell script.
20. On LON-PROD1, in Windows PowerShell, run the following three commands.

```
ping 10.0.0.16
ping 10.0.0.25
ping 10.0.0.26
```

21. Confirm that four replies are returned only from IP **10.0.0.25**, which confirms that LON-PROD1 has connectivity with LON-PROD2 but does not have connectivity with LON-TEST1 and LON-TEST2, because LON-TEST1 and LON-TEST2 are on different virtual network (which is sharing the same physical network).

Lab Review Questions and Answers

Lab: Creating and Configuring Virtual Machine Networks

Question and Answers

Question: Is there any better way to configure network virtualization than using Windows PowerShell?

Answer: When you are limited to Windows Server 2012 R2, Windows PowerShell is the only tool that you can use for configuring network virtualization. But if you can use additional tools such as System Center 2012 R2 Virtual Machine Manager, configuring network virtualization is considerably easier, and you can use the graphical tool for that.