Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20741B

Networking with Windows Server 2016

Companion Content

Product Number: 20741B

Released: 02/2017

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

Planning and implementing an IPv4 network

Contents:

Lesson 1

Planning IPv4 addressing

Contents:

Question and Answers

Question: Select the subnet mask to create the smallest networks that will allow 172.168.32.223 and 172.168.35.19 to be on the same network.

( ) /20

( ) /21

( ) /22

( ) /23

( ) /24

Answer:

( ) /20

( ) /21

(√) /22

( ) /23

( ) /24

Feedback:

Option 1 and option 2 would place both addresses in the same network, but would make the networks much larger than necessary. Option 4 and option 5 would force both addresses to be on separate networks.

Question: What is the decimal equivalent of the correct subnet mask for the previous question?

Answer: 255.255.252.0

Overview of IPv4 settings

Question: Convert the following values

Binary	Dotted decimal notation
00001010 00001110 00011011 00100000	
	172.16.34.22
	192.168.87.19
10101100 00010000 01100010 00010111	
11000000 10101000 01010111 00111000	
	10.17.22.99

Answer:

Binary	Dotted decimal notation
00001010 00001110 00011011 00100000	10.14.27.32
10101100 00010000 00100010 00010110	172.16.34.22

Binary	Dotted decimal notation
11000000 10101000 01010111 00010011	192.168.87.19
10101100 00010000 01100010 00010111	172.16.98.23
11000000 10101000 01010111 00111000	192.168.87.56
00001010 00010001 00010110 01100011	10.17.22.99

Defining subnets

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

Answer: A host with an incorrect default gateway is unable to communicate with hosts on a remote network. Communication on the local network, however, remains unaffected.

Question: Does your organization use simple or complex networking?

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

Discussion: Determining IPv4 notation and translation

Question: Which of the following addresses are classful and which are classless?

- 10.14.27.32/8
- 172.16.34.22/26
- 192.168.87.19 Subnet mask 255.555.555.0
- 172.16.98.23 Subnet mask 255.240.0.0
- 192.168.87.56/24
- 10.17.22.99/12

Answer:

- 10.14.27.32/8 (classful)
- 172.16.34.22/26 (classless)
- 192.168.87.19 Subnet mask 255.555.555.0 (classful)
- 172.16.98.23 Subnet mask 255.240.0.0 (classless)
- 192.168.87.56/24 (classful)
- 10.17.22.99/12 (classless)

Question: Identify the network ID for each of the following addresses.

- 10.25.12.100/24
- 10.25.12.100/16
- 172.168.20.66/24
- 172.168.20.66/26
- 192.168.52.98 Subnet mask 255.255.255.0
- 192.168.52.98 Subnet mask 255.255.255.240

Answer:

- 10.25.12.100/24 (network ID 10.25.12.0)
- 10.25.12.100/16 (network ID 10.25.0.0)
- 172.168.20.66/24 (network ID 172.168.20.0)
- 172.168.20.66/26 (network ID 172.168.20.64)
- 192.168.52.98 Subnet mask 255.255.255.0 (network ID 192.168.52.0)
- 192.168.52.98 Subnet mask 255.255.255.240 (network ID 192.168.52.96)

Question: For the network in which each of these addresses reside, Identify the first usable address and the broadcast address.

- 10.25.12.100/24
- 10.25.12.100/16
- 172.168.20.66/24
- 172.168.20.66/26
- 192.168.52.98 Subnet mask 255.255.255.0
- 192.168.52.98 Subnet mask 255.255.255.240

Answer:

- 10.25.12.100/24 (First usable address 10.25.12.1, broadcast address 10.25.12.255)
- 10.25.12.100/16 (First usable address 10.25.12.1, broadcast address 10.25.255.255)
- 172.168.20.66/24 (First usable address 172.168.20.1, broadcast address 172.168.20.255)
- 172.168.20.66/26 (First usable address 172.168.20.65, broadcast address 172.168.20.127)
- 192.168.52.98 Subnet mask 255.255.255.0 (first usable address 192.168.52.1, broadcast address 192.168.52.255)
- 192.168.52.98 Subnet mask 255.255.255.240 (first usable address 192.168.52.97, broadcast address 192.168.52.111)

Discussion: Creating a subnetting scheme for a new office

Question: How many subnets are required?

Answer: Five subnets are required in this scenario. Of these, four subnets are required for buildings, and one is required for the data center. These are the minimum number for subnets required by the scenario requirements.

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

Answer: Subnets are calculated by using the formula 2^n, where *n* is the number of bits. As seen in the chart below, three bits are required to create five subnets, because two bits only provide for 4 subnets and three bits allow for eight subnets. Because printers in this scenario have networking capability, you need to assign IP addresses to them.

Subnet bits	Formula	Subnets
1	2^1	2
2	2^2	4

Subnet bits	Formula	Subnets
3	2^3	8
4	2^4	16
5	2^5	32
6	2^6	64

Question: How many available hosts are required on each subnet?

Answer: Because each subnet must support up to 700 users and 14 printers, 714 usable addresses should be available on each subnet.

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

Answer: The number of usable hosts depends on the number of bits. The formula is (2^n)-2, where n is the number of bits. 9 hosts bits provide for 510 hosts, ((2^9) – 2 = 510). Ten bits ((2^10) – 2 = 1022) provides up to 1,022 hosts.

Question: What is an appropriate subnet mask that would satisfy these requirements?

Answer: Several subnet masks would 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

Configuring an IPv4 host

Contents:

Question and Answers

Question: What would be the best way to configure IP addresses for a branch office that has only 50 desktop computers?

> **Answer:** Answers could vary. Some students could suggest static IP addresses, as desktop systems generally do not roam between locations, and the network does not include a server for use as a DHCP server. Others might suggest using DHCP and sending DHCP requests to a DHCP in the home network.

Question: How would your answer change if there were a mix of laptops and desktop computers?

> **Answer:** Answers could vary. The students who suggested DHCP likely would not change their answer. However, students that suggested static addresses will likely suggest DHCP to support laptop roaming.

Configurable IPv4 settings

Question: Do any computers or devices in your organization have static IP addresses?

> **Answer:** In most cases, servers have static IP addresses. Other network devices such as printers also typically have static IP addresses.

Tools for configuring IPv4

Question: If you want to assign multiple IPv4 addresses to a server, which tool should you use?

> **Answer:** The simplest tool to accomplish this task would be the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, Advanced TCP/IP settings tab.

Resources

 **Additional Reading:** For more information, review "Net TCP/IP Cmdlets in Windows PowerShell," at: http://aka.ms/L50hb6

Demonstration: Configuring IPv4

Demonstration Steps

Configuring IPv4 by using the user interface

1. On **LON-SVR1**, click the **Start** button, and then click **Settings**.
2. In the **Settings** window, click **Network & Internet**.
3. In the **Network & Internet** window, in the navigation pane, click **Ethernet**.
4. In the **Network & Internet** window, in the results pane, click **Network and Sharing Center**.
5. In the **Network and Sharing Center** window, in the navigation pane, click **Change adapter settings**.
6. Right-click **London_Network**, and then click **Properties**.
7. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
8. Change the **IP address** to **172.16.0.111**, and then click **OK**.
9. Close all open windows.

Configuring IPv4 by using Windows PowerShell

1. Click the **Start** button, and then click **Windows PowerShell**.

2. Verify that the IP address was changed by typing the following command, and then pressing Enter:

```
Get-NetIPAddress -InterfaceAlias “London_Network”
```

3. Remove the IP address by typing the following command, and then pressing Enter:

```
Remove-NetIPAddress -InterfaceAlias “London_Network” -IPAddress 172.16.0.111
```

4. When prompted to **Confirm**, type **y**, and then press Enter.
5. When prompted to **Confirm**, type **y**, and then press Enter.
6. Verify that the IP address was changed by typing the following command, and then pressing Enter:

```
Get-NetIPAddress -InterfaceAlias “London_Network”
```

7. Note the IP address assigned to the interface.
8. Add the **172.16.0.11** IP address to the **Ethernet** interface by typing the following command, and then pressing Enter:

```
New-NetIPAddress -InterfaceAlias “London_Network” -IPAddress 172.16.0.11 -
PrefixLength 24
```

9. Close all open windows, and then minimize all virtual machines.

Lesson 3

Managing and troubleshooting IPv4 network connectivity

Contents:

Question and Answers

Question: What is the result of applying the wrong subnet mask to a system?

Answer: Communications will be disrupted.

Question: If a client complains that they are unable to connect to a server, which of the following steps would help you to resolve the problem?

( ) Restart the server.

( ) Verify that the client has a valid IP address.

( ) Verify that the client received the proper APIPA address.

( ) Check the IP configuration of the servers to which the client is trying to connect.

( ) All of the above.

Answer:

( ) Restart the server.

(√) Verify that the client has a valid IP address.

( ) Verify that the client received the proper APIPA address.

( ) Check the IP configuration of the servers to which the client is trying to connect.

( ) All of the above.

IPv4 troubleshooting methodology

Question: What additional steps might you use to troubleshoot network connectivity problems?

Answer: Answers will vary. Some students might monitor firewalls if the problem is related to Internet connectivity. Students also might use application logs when troubleshooting connectivity to a specific program.

Resources

What is Microsoft Message Analyzer?

Reference Links: For more information about Microsoft Message Analyzer, see the "Microsoft Message Analyzer Operating Guide" at: http://aka.ms/Jzc3pk
To download Microsoft Message Analyzer, go to https://aka.ms/e89var

Demonstration: Troubleshooting IPv4

Demonstration Steps

Using Get-NetIPAddress and ipconfig

1. On **LON-SVR1**, click the **Start** button, and then click **Windows PowerShell**.
2. Click the **Start** button, type **cmd**, right-click **Command Prompt**, and click **Run as Administrator**.
3. On **LON-SVR1**, right-click the taskbar, and then click **Show windows side by side**.
4. In the Windows PowerShell window, type the following command, and then press Enter:

```
Get-NetIPAddress -InterfaceAlias "London_Network"
```

5. In the Administrator: command prompt window, type the following command, and then press Enter:

```
ipconfig
```

6. Discuss the similarities and differences in the output of each command.

Using Test-NetConnection and ping

1. On **LON-SVR1**, in the Windows PowerShell window, type the following command, and then press Enter:

```
Test-NetConnection 172.16.0.1
```

2. In the Administrator: command prompt window, type the following command, and then press Enter:

```
Ping 172.16.0.1
```

3. Discuss the similarities and differences between the output of each command.

Using Test-NetConnection –TraceRoute and tracert

1. On **LON-SVR1**, in the Windows PowerShell window, type the following command, and then press Enter:

```
Test-NetConnection -TraceRoute 172.16.18.20
```

2. In the command prompt window, type the following command, and then press Enter:

```
Tracert 172.16.18.20
```

3. Discuss the similarities and differences between the output of each command.

Demonstration: Using Microsoft Message Analyzer

Demonstration Steps

Start a new Capture/Trace in Microsoft Message Analyzer

1. Connect to **LON-SVR2**, if you have not already done so.
2. Sign in as **Adatum\Administrator** with a password of **Pa55w.rd**.
3. Click **Start**, and then click the **Windows PowerShell** icon.
4. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Clear-DnsClientCache
```

5. Click **Start**, expand **Microsoft Message Analyzer**, and then click **Microsoft Message Analyzer**.
6. In the navigation pane, click **Start Local Trace**.

Capture packets from a ping request

1. On the taskbar, click the Windows PowerShell icon.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Test-NetConnection LON-DC1.adatum.com
```

3. Wait for the command to complete, and then on the taskbar, click the **Microsoft Message Analyzer** icon.
4. In Microsoft Message Analyzer, on the toolbar, click **Stop**.

Analyze the captured network traffic

1. In Microsoft Message Analyzer, in the results pane, under the **Module** column, select the first **ICMP** packet group.
2. In the results pane, click the plus sign '**+**' next to the selected packet group.
3. Show that the packet group includes both the **Echo Request** and the **Echo Reply** packets, as a result of the ping request that was executed when running the **Test-NetConnection** cmdlet.
4. Review 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, in the **Filter** box, type the following command, and then click **Apply**:

```
*DestinationAddress == 172.16.0.10
```

2. Verify that only packets that match the filter display.
3. Close **Microsoft Message Analyzer** without saving.

Module Review and Takeaways

Best Practices

When implementing IPv4, use the following best practices:

- Allow for growth when planning IPv4 subnets. This ensures that you do not need to change your IPv4 configuration scheme.
- Define purposes for specific address ranges and subnets. This enables you to identify hosts based on their IP address easily, and to use firewalls to increase security.
- Use dynamic IPv4 addresses for clients. It is much easier to manage the IPv4 configuration for client computers by using DHCP, than with manual configuration.
- Use static IPv4 addresses for servers. When servers have a static IPv4 address, it is easier to identify where services are located on the network.

Review Questions

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, this is a concern because those are Internet routable addresses. Most IPv4 networks use private addresses with NAT to allow access to the Internet. If this organization does not own the 131.107.88.0/24 network, they will not be able to access resources on the 131.107.88.0/24 network on the Internet because all clients will consider those addresses local.

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 your 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. Additionally, the networks must allow you to remove a single bit from the subnet mask and identify both as the same network.

Question: You have installed a new web-based program that runs on a nonstandard port number. A colleague is testing access to the new web-based program, and indicates that he cannot connect to it. What are the most likely causes of his problem?

> **Answer:** When a server program runs on a nonstandard port, you need to provide the client program with the port number to which it should be connecting, such as http://servername:port. It is also possible that your colleague is attempting to connect using http, when he should be using https.

Tools

The following table lists the tools that this module references.

Tool	Use to	Where to find it
Microsoft Message Analyzer	Capture and analyze network traffic	Download from the Microsoft website
Get-NetIPAddress	Obtain a list of IP addresses that are configured for interfaces	Windows PowerShell

Tool	Use to	Where to find it
Test-NetConnection	Display the following: • Results of a DNS lookup • Listing of IP interfaces • Option to test a TCP connection • IPsec rules • Confirmation of connection establishment	Windows PowerShell
Ipconfig	View network configuration	Command prompt
Ping	Verify network connectivity	Command prompt
Tracert	Verify network path between hosts	Command prompt
Pathping	Verify network path and reliability between hosts	Command prompt
Route	View and configure the local routing table	Command prompt
Telnet	Test connectivity to a specific port	Command prompt
Netstat	View network connectivity information	Command prompt
Resource Monitor	View network connectivity information	Tools in Server Manager
Windows Network Diagnostics	Diagnose a problem with a network connection	Properties of the network connection
Event Viewer	View network-related system events	Tools in Server Manager

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
IP conflicts	In most cases, computers that are running Windows operating systems display a message when they have an IP conflict with another network device. However, some network devices do not. When performing a packet capture, duplicate TCP acknowledgements can be an indication that two devices have the same IP address, and that both are responding to connection attempts. To prevent IP conflicts, clearly document which IPv4 addresses are in use on your network, and do not assign new IPv4 addresses without checking the documentation.

Common Issue	Troubleshooting Tip
Multiple default gateways defined	On hosts with multiple network cards, only one should have a default gateway defined. Windows Server is designed to function with only a single default gateway. When multiple default gateways are defined, network communication can be unpredictable. You can verify that only a single default gateway is configured by using the **Get-NetRoute** cmdlet.
Incorrect IPv4 configuration	Incorrect IPv4 configuration information is most commonly a result of a manual configuration error. To ensure that this does not affect a production environment, you should test network connectivity thoroughly for any new servers that you place into production. You should also perform testing after making any network configuration changes.

Lab Review Questions and Answers

Lab A: Planning an IPv4 network

Question and Answers

Question: How many default gateways will be required?

Answer: Each subnet requires a default gateway. Using seven subnets will require seven default gateways.

Question: What other factors would you take into consideration when designing a network?

Answer: Answers will vary. Possible considerations include the distribution of the offices. For example, you might want to use only two subnets for the wired connections in Houston, but the facilities might be laid out in such a way that using only two subnets is not possible.

Lab B: Implementing and troubleshooting an IPv4 network

Question and Answers

Question: When troubleshooting an issue, what is the first step you should take?

Answer: Answers will vary. Many people take different approaches to troubleshooting. One very important first step is to duplicate the issue.

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 DHCP

Contents:

Lesson 1

Overview of the DHCP server role

Contents:

Question and Answers

Question: If there are multiple DHCP severs responding to client requests, how does the client choose which DHCP offer to accept?

Answer: The client has no preference. It will accept the first offer it receives.

Question: All Windows-based operating systems are configured to be DHCP clients after the initial installation of the operating system.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

Even server operating systems start off as DHCP clients. If you want a static address, you must configure one.

Lesson 2

Deploying DHCP

Contents:

Question and Answers

Question: Any domain administrator can authorize a DHCP server.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Only an enterprise administrator can authorize a DHCP server.

Question: In case of a conflict between DHCP options, which level takes precedence?

( ) Server level

( ) Class level

( ) Scope level

( ) Client reservation level

Answer:

( ) Server level

( ) Class level

( ) Scope level

(√) Client reservation level

Feedback:

Options assigned to client reservations override any conflicting options.

Resources

Allocating and managing IPv4 addresses with DHCP

 **Additional Reading:** For more information about DHCP server cmdlets in Windows PowerShell, refer to: "DHCP Server Cmdlets in Windows PowerShell" at: http://aka.ms/Blsmzw

 **Additional Reading:** For additional Windows PowerShell cmdlets for DHCP that were added in Windows Server 2012 R2, refer to: "What's New in DHCP" at: http://aka.ms/Hfgoye

Demonstration: Installing a DHCP server, and performing post-installation tasks

Demonstration Steps

Install the DHCP server role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Click **Start**, and then click the **Server Manager** tile.
3. On the **Server Manager** dashboard, click **Add roles and features**.
4. On the **Before you begin** page, click **Next**.

5. On the **Select installation type** page, click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select **DHCP Server**.
8. In the **Add Roles and Features Wizard**, click **Add Features**, and then click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **DHCP Server** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**. The installation will take a few minutes to complete.
12. After the installation succeeds, click **Close**.

Perform the post-installation tasks

1. Click the (orange triangle) **Notifications** icon in the top menu bar, and then click the **Complete DHCP configuration** link.
2. In the **DHCP Post-Install configuration wizard**, on the **Description** page, read the text, and then click **Next**.
3. On the **Authorization** page, click **Commit**.
4. Read the text on the **Summary** page, and then click **Close**.
5. In **Server Manager**, click **Tools**, and then click **Services**.
6. Select the **DHCP Server** service, and then click the **Restart** link.
7. Close the **Services** management console.

Demonstration: Configure a DHCP server

Demonstration Steps

Create a DHCP scope

1. On **LON-SVR1**, in Server Manager, click **Tools**, and then click **DHCP**.
2. In the left pane, click to select **lon-svr1.adatum.com**. This will open the **IPv4** node.
3. Click to select the **IPv4** node. In the **Actions** pane, click **More Actions**, and then click **New Scope**.
4. In the **New Scope Wizard**, click **Next**.
5. On the **Scope Name** page, in the **Name** text box, type **Adatum**, and then click **Next**.
6. On the **IP Address Range** page, in the **Start IP address** text box, type **10.0.0.100**, and then in the **End IP address** text box, type **10.0.0.150**.

 **Note:** Note that the **subnet mask** field fills in automatically to match the default subnet mask for a class **A** address range.

7. Change the subnet mask to **255.255.255.0**, and then click **Next**.
8. On the **Add Exclusions and Delay** page, click **Next**.
9. On the **Lease Duration page**, change the value in the **Days** field to **1** Day, and then click **Next**.
10. On the **Configure DHCP Options** page, click **No, I will configure these options later**, click **Next**, and then click **Finish**.

Note: Note that the **Scope** folder has a red downward arrow on it, which indicates that the scope is not activated.

Configure DHCP options

1. Expand the **IPv4** node, and then expand the **Scope [10.0.0.0] Adatum** folder.
2. Click to select the **Scope Options** folder. Right-click the folder, and then click **Configure Options**.
3. In the **Scope Options** dialog box, select **003 Router**. In the **IP address** text box, type **10.0.0.1**, and then click **Add**.
4. Select **006 DNS Servers**. In the **IP address** text box, type **172.16.0.10**, click **Add**, and then click **OK**.
5. Right-click the **Scope [10.0.0.0] Adatum** folder, and then click **Activate**.
6. Note that the **red downward arrow** icon no longer appears on the **Scope** folder.

Create a DHCP reservation

1. Click to select the **Reservations** folder. Right-click the folder, and then click **New Reservation**.
2. In the **New Reservation** dialog box, in the **Reservation name** text box, type **Sales Printer**.
3. In the **IP address** text box, type **10.0.0.120**.
4. In the **MAC address** text box, type **00-14-6D-01-73-6B**, click **Add**, and then click **Close**.

Lesson 3

Managing and troubleshooting DHCP

Contents:

Question and Answers

Question: How can you prevent ranges of subnet addresses from being assigned to clients?

> **Answer:** Configure exclusions to prevent one or more of the subnet's address ranges from being assigned.

Question: The maximum time difference that can exist between two DHCP servers in a failover relationship is five minutes.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:**
>
> The maximum time difference that can exist between two DHCP servers in a failover relationship is only one minute.

Resources

Advanced options for configuring DHCP

 **Additional Reading:** For more information on DHCP policies for devices, refer to: "Using DHCP policies to set different lease durations for different device types" at: http://aka.ms/ljz5m7

Demonstration: Configure DHCP failover

Demonstration Steps

1. On **LON-DC1**, in Server Manager, click **Tools**, and then from the drop-down list box, click **DHCP**.
2. In the **DHCP** console, expand **lon-dc1.adatum.com**, select and then right-click **IPv4**, and then click **Configure Failover**.
3. In the **Configure Failover Wizard**, click **Next**.
4. On the **Specify a partner server to use for failover** page, in the **Partner Server** text box, type **172.16.0.11**, and then click **Next**.
5. On the **Create a new failover relationship** page, in the **Relationship Name** text box, type **Adatum**.
6. In the **Maximum Client Lead Time** field, set the **hours** to **0**, and then set the **minutes** to **15**.
7. Ensure that the **Mode** is set to **Load balance**.
8. Ensure that the **Load Balance Percentage** is set to **50%**.
9. Select the **State Switchover Interval** check box. Leave the default value of **60** minutes.
10. In the Enable Message Authentication Shared Secret text box, type Pa55w.rd, and then click Next.
11. Click **Finish**, and then click **Close**.
12. Switch to **LON-SVR1**.
13. Refresh the **IPv4** node, expand the node, and then expand **Scope [172.16.0.0] Adatum**.
14. Click **Address Pool**, and then point out that the address pool is configured.

15. Click **Scope Options**, and then point out that the scope options are configured.
16. Close the **DHCP** console on both **LON-DC1** and **LON-SVR1**.

Module Review and Takeaways

Best Practices

The following are best practices when you are working with DHCP:

- Configure DHCP failover relationships to provide high availability.
- Ensure lease durations are appropriate. We typically recommend shorter lease durations for wireless networks, due to the transient nature of wireless clients.
- Create reservations for devices that need IP addresses that will not change.
- Enable DHCP auditing to track trends and history.
- Enable name protection.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Clients are unable to obtain IP addresses	Check that the scope has available addresses and that the server is online.

Lab Review Questions and Answers

Lab: Implementing DHCP

Question and Answers

Question: Why do the scopes created in the lab start at 172.16.x.2 and not 172.16.x.1?

Answer: The default gateway will use the 172.16.x.1 address in all cases.

Question: What is the default location of the DHCP database?

Answer: The default location of the DHCP database is the **%systemroot%\System32\Dhcp** folder.

Module 3

Implementing IPv6

Contents:

Lesson 1

Overview of IPv6 addressing

Contents:

Question and Answers

Overview of IPv6 addressing

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

Lesson 2

Configuring an IPv6 host

Contents:

Question and Answers

Question: The servers in your organization are configured for IPv6 and receive IPv6 addresses from a DHCPv6 server. You need to add an IPv6 address to the interface on one of your servers. What should you do?

Answer: If you use the **New-NetIPAddress** cmdlet to add an IPv6 address to an interface on which DHCP is already enabled, DHCP is automatically disabled. As a result, you will need to either:

- Use the **Set-NetIPInterface** cmdlet to disable DHCP configuration on the interface, and then use **Set-NetIPAddress** and **New-NetIPAddress** to configure the IPv6 addresses on the interface.
- Use **New-NetIPAddress** to disable DHCP configuration on the interface, and then use **New-NetIPAddress** to configure the additional IPv6 address on the interface.

Resources

Tools for configuring IPv6

 **Additional Reading:** For more information, refer to Net TCP/IP Cmdlets in Windows PowerShell at: https://aka.ms/ysn3pb

 **Additional Reading:** For more information on using Netsh, refer to the list of Netsh commands for configuring IPv6 at: http://aka.ms/Dley4n

Demonstration: Configuring IPv6

Demonstration Steps

View IPv6 configuration by using IPconfig

1. On LON-DC1, if necessary, open a **Windows PowerShell** command prompt.
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 **London_Network**, click **172.16.0.10, IPv6 Enabled**.
3. In the Network Connections window, right-click **London_Network**, 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** text box, type **FD00:AAAA:BBBB:CCCC::A**
7. In the **Subnet prefix length** text box, type **64**.
8. In the **Preferred DNS server** text box, type **::1**, and then click **OK**.
9. In the **London_Network Properties** dialog box, click **Close**.

10. Close the **Network Connections** window. If the **Network** page opens, click **Yes**.

Configure IPv6 on LON-SVR1

1. On LON-SVR1, open **Server Manager**, and then click **Local Server**.
2. In the **Local Server Properties** dialog box, next to **London_Network**, click **172.16.0.11**, **IPv6 Enabled**.
3. In the **Network Connections** window, right-click **London_Network**, and then click **Properties**.
4. In the **London_Network 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** text box, type **FD00:AAAA:BBBB:CCCC::15**.
7. In the **Subnet prefix length** text box, type **64**.
8. In the **Preferred DNS server** text box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **OK**.
9. In the **London_Network Properties** dialog box, click **Close**.
10. Close the **Network Connections** window.

Verify that IPv6 communication is functional

1. On LON-SVR1, click **Start**, and then click **Windows PowerShell**.
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 next demonstration in this module.

Demonstration: Configuring DHCP for 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 upper-right corner, click **Tools**, and then click **DHCP**.
2. In the DHCP console, in the navigation pane, expand **LON-DC1.adatum.com**, expand **IPv6**, select and then 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 **fd00:0000:0000:0000::**, and then click **Next**.
6. On the **Add Exclusions** page, type the following, click **Add**, and then click **Next**:
   - Start IPv6 Address: **0000:0000:0000:0000**
   - End IPv6 Address: **0000:0000:0000:00ff**

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-SVR1 has dynamically registered its IPv6 address 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** text box, type **WebApp.**
6. In the **IP address** text 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, from the **Start** menu, click **Windows PowerShell**.
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 4

Transitioning from IPv4 to IPv6

Contents:

Resources

What is ISATAP?

Additional Reading:

- For more information about network transition cmdlets in Windows PowerShell, refer to "Network Transition Cmdlets in Windows PowerShell" at: http://aka.ms/Vzxldt
- For more information about Netsh commands for Interface ISATAP, refer to "Netsh commands for Interface ISATAP" at: http://aka.ms/E5u3fk

What Is 6to4?

Additional Reading: For more information about Netsh commands for Interface 6to4, refer to "Netsh commands for Interface 6to4" at: http://aka.ms/Qqqgu7

What is Teredo?

Additional Reading: For more information about Netsh commands for Interface Teredo, refer to "Netsh commands for Interface Teredo" at: http://aka.ms/Tsgd7b

What is PortProxy?

Additional Reading: For more information about IPv6 Transition Technologies, refer to "IPv6 Transition Technologies" at http://aka.ms/E8c95o

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 Windows 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 Questions

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 that you use 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 generated randomly. 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 no specific number of IPv6 addresses that an IPv6 node should have. It depends on the organization's configuration. Each IPv6 node has a link-local IPv6 address. In addition, it might 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 the LON-DC1 and LON-CL1 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 the 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 DNS

Contents:

Lesson 1

Implementing DNS servers

Contents:

Question and Answers

Categorize Activity

Question: Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Contains a database of host names and IP addresses
2	Has both forward and reverse lookup categories
3	Is run by the DNS client service
4	Responds to client requests
5	Contains resource records
6	Generates client requests
7	If it does not have the needed mapping information, forwards requests to other DNS servers
8	Scope for replication
9	Facilitates the caching of resolved mappings in a local client cache for future use

Category 1		Category 2		Category 3
DNS server		DNS zones		DNS resolver

Answer:

Category 1		Category 2		Category 3
DNS server		DNS zones		DNS resolver
Contains a database of host names and IP addresses Responds to client requests If it does not have the needed mapping information, forwards requests to other DNS servers		Has both forward and reverse lookup categories Contains resource records Scope for replication		Is run by the DNS client service Generates client requests Facilitates the caching of resolved mappings in a local client cache for future use

Resources

Tools and techniques for troubleshooting name resolution

Additional Reading: For more information on the parameters for the **Get-DnsServerStatistics** cmdlet, refer to: "Get-DnsServerStatistics" at: http://aka.ms/U9442y

Reference Links: To download the Dnslint.exe package, refer to: "Description of the DNSLint utility" at: http://aka.ms/Vw9oyv

Demonstration: Installing and configuring the DNS role

Demonstration Steps

Install the DNS Server role

1. On **TOR-SVR1**, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Click **Start**, and then 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** dialog box, 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, ensure **TOR-SVR1.adatum.com** is selected in the **Server Pool** area, and then 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**.
13. After you have installed the role, click **Close**.

Enable Pings

1. On TOR-SVR1, in Server Manager, click **Tools**, and then click **Windows Firewall with Advanced Security**.
2. In the **Windows Firewall with Advanced Security** console, select **Inbound Rules**.
3. In the **Inbound Rules** details pane, scroll down and right-click the **File and Print Sharing (Echo Request - ICMPv4-In)** item, and click **Enable Rule**.
4. Right-click and enable the item named **File and Print Sharing (Echo Request – ICMPv6-In).**
5. Close the **Windows Firewall with Advanced Security** console.
6. Click the **Start** button, and in the Start menu, click **Windows PowerShell**.
7. In **Windows PowerShell**, type the following cmdlet, and then press Enter:

```
Ping 172.16.0.10
```

8. You should get four replies.
9. Close **Windows PowerShell**.
10. Switch to **LON-DC1**, and then click the **Start** button, and in the Start menu, click **Windows PowerShell**.
11. In **Windows PowerShell**, type the following cmdlet, and then press Enter:

```
Ping 172.16.18.20
```

12. You should get four replies.
13. Close **Windows PowerShell**.

Configure the DNS Server role

1. On **TOR-SVR1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **TOR-SVR1**, select and right-click **TOR-SVR1**, and then click **Properties**.
3. In the **TOR-SVR1 Properties** dialog box, click the **Forwarders** tab.
4. On the **Forwarders** tab, click **Edit**. In the **Edit Forwarders** window, in the **<Click here to add an IP addresses or DNS name>** text box, type **172.16.0.10**, and then press Enter. In a few minutes the IP address will resolve, and you will get a green check mark beside the address.

Note: If you receive another entry in the **IP address** column with red X that says **The requested name** and in the **Validated** column says **No IPv6 address**, then select the entry and then click the **Delete** button.

Click **OK**.

5. In the **TOR-SVR1 Properties** window, click **OK**.
6. In the **DNS console** tree, select and then right-click **Forward Lookup Zones**, and then click **New Zone**.
7. In the **New Zone Wizard** that opens, click **Next**.
8. On the **Zone Type** page, click **Next**.
9. On the **Zone Name** page, in the **Zone name** text box, type **Contoso.com**, and then click **Next**.
10. On the **Zone File** page, click **Next**.
11. On the **Dynamic update** page, click **Next**.
12. On the **Completing the New Zone Wizard** page, click **Finish**.
13. In the console tree, expand **Forward Lookup Zones**, double-click **Contoso.com**, right-click **Contoso.com**, and then select **New Host (A or AAAA)**.
14. In the **New Host** window, in the **Name** text box, type **ATL-SVR1**, in the **IP address** text box, type **172.16.18.125**, and then click **Add Host**.
15. In the **DNS** pop-up window, click **OK**, and then in the **New Host** window, click **Done**.

Demonstration: Troubleshooting name resolution

Demonstration Steps

Use Windows PowerShell cmdlets to troubleshoot DNS

1. On **LON-CL1**, on the **Taskbar**, in the **Search** text box, type **PowerShell**, and then in the list that is returned, click **Windows PowerShell.**
2. In the **Windows PowerShell** console, type the following cmdlets, and press Enter after each command:

```
Get-DnsClientServerAddress
Clear-DnsClientCache
```

   Note that the DNS Server address assigned to London_Network IPv4 is **172.16.0.10**. This is **LON-DC1**.

3. Note the entries labeled **London_Network** in the InterfaceAlias column, and the entry labeled **IPv4** in the Address Family column. In the Interface Index column, note the Interface Index number that is in the same row as London_Network and IPv4. Note this number. You will use this specific Interface Index number in a later step.
4. In the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
Resolve-DnsName lon-dc1
```

   Note the address returned. Do not close Windows PowerShell.

5. Right-click **Start**, and then click **Control Panel**.
6. In the **Control Panel** window, click the **Network and Internet** hyperlink.
7. On the **Network and Internet** page, click the **Network and Sharing Center** hyperlink.
8. On the **Network and Sharing Center** page, click the **London_Network** hyperlink.
9. In the **London_Network Status** window, click **Details**.
10. In the **Network Connections Details** pop-up window, note the information shown, and then click **Close**.
11. On the **London_Network Status** page, click **Properties**.
12. Scroll down to the **This connection uses the following items** section, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
13. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons, click **OK**, and then click **Close** twice.
14. Switch to the **Windows PowerShell** console, type the following cmdlets, pressing Enter after each cmdlet, where *X* is the Interface Index number you wrote down in step 3:

```
Ipconfig /release
Set-DnsClientServerAddress –InterfaceIndex X -ResetServerAddresses
Clear-DnsClientCache
Get-DnsClientServerAddress
```

Note: Note that there is no IP address for IPv4.

15. On **LON-DC1**, click the **Start** icon and select **Windows PowerShell**.

16. In the **Windows PowerShell** console (on **LON-DC1**), type the following command, and then press Enter:

```
Net start DHCPServer
```

17. Return to **LON-CL1**, and in the **Windows PowerShell** console (on **LON-CL1**), type the following command, and then press Enter:

```
Ipconfig /renew
```

18. In the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
Get-DnsClientServerAddress
```

Note: Note that there is now an address for IPv4.

19. In the **Windows PowerShell** console, type the following cmdlet, press Enter, and then note the address that displays:

```
Resolve-DnsName lon-dc1
```

20. Return to the **Network and Sharing Center** window, and then click the **London_Network** hyperlink.
21. On the **London_Network Status** page, click **Properties**.
22. On the **London_Network Properties** page, scroll down to the **This connection uses the following items** section, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
23. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Use the following IP address** and enter the following:
    - IP address: **172.16.0.50**
    - Subnet mask: **255.255.0.0**
    - Default gateway: **172.16.0.1**
    - Preferred DNS server: **172.16.0.10**
24. Click **OK**, and then click **Close** twice.

Note: If a Networks pane opens, click Yes.

25. To display the output of the following cmdlets, in the **Windows PowerShell** console, type each of the following cmdlets, and press Enter after each cmdlet:

```
Get-DnsClientCache
Clear-DnsClientCache
Get-DnsClientCache
Get-DnsClientGlobalSetting
Register-DnsClient
```

26. Close the **Windows PowerShell** and **Network and Sharing Center** windows.

Use command line tools to troubleshoot DNS

1. On **LON-CL1**, on the **Taskbar**, in the **Search** text box, type **cmd**, in the list that is returned, right-click **Command Prompt**, and then click **Run as administrator**.

2. In the **Command Prompt** window, type the following command, and then press Enter:

```
ipconfig /all
```

3. Review the output that displays, and note the **DNS server** section.
4. In the **Command Prompt** window, type the following command, and then press Enter.

```
nslookup
```

Note: You should see the address of the DNS server from step 3 above returned. Note the **>** prompt, which means that you are in the nslookup prompt.

5. In the **Command Prompt** window, type the following command, and then press Enter.

```
lon-cl1
```

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

```
exit
```

Note: Do not close any open Windows.

7. Switch to **LON-DC1**.
8. On the **Taskbar**, in the **Search** text box, type **cmd**, then in the list that is returned, right-click **Command Prompt**, and then click **Run as administrator**.
9. At the command prompt, type the following command, and then press Enter:

```
dnscmd /?
```

Note: Use the output to review some of the dsncmd options available. Do not spend much time here because the second DNS server has not been set up.

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

```
ipconfig /displaydns
```

Note: Note the output values that display.

11. At the command prompt, type the following, and press Enter after each line:

```
ipconfig /flushdns
ipconfig /displaydns
```

Note: Note that the output values are gone.

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

```
ping LON-CL1
```

Note: Note that the ping command returned the FQDN of **LON-CL1**. Point out to the students that this is an indicator that the DNS name resolution occurred even before the ping packet was generated.

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

```
ipconfig /displaydns
```

Note: Note that information on the LON-CL1 DNS resource record is displayed.

14. Close all open windows.

Demonstration: Testing the DNS server

Demonstration Steps

Test the DNS server

1. On **TOR-SVR1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, expand **TOR-SVR1**, select and right-click **TOR-SVR1**, and then click **Properties**.
3. Click the **Advanced** tab. On this tab, you can configure options including securing the cache against pollution.
4. Click the **Root Hints** tab. On this tab, you can see the configuration for the root hints servers.
5. Click the **Debug Logging** tab, and then select the **Log packets for debugging** check box. On this tab, you can configure debug logging options.
6. Clear the **Log packets for debugging** check box, and then click the **Event Logging** tab.
7. Click **Errors and Warnings**.
8. Click the **Monitoring** tab. You can perform simple and recursive tests against the server by using the **Monitoring** tab. Select the **A simple query against this DNS server** check box, and then click **Test Now**.
9. In the **TOR-SVR1 Properties** window, click **OK**.
10. Click **Start**, and then click **Windows PowerShell**.
11. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
nslookup -d2 LON-DC1.Adatum.com
```

12. Review the information provided by Nslookup. It provides detailed debugging information.
13. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Test-DnsServer -IpAddress 172.16.18.20
```

14. Observe the results.
15. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Get-DNSServerDiagnostics
```

16. Observe the results.
17. Leave Windows PowerShell open.

Use audit and analytic event logging

1. On **TOR-SVR1**, in **Server Manager,** click **Tools**, and then click **Event Viewer**.
2. Maximize the **Event Viewer** console, and then wait a few seconds for the Overview and Summary information to load.
3. In the console tree, expand **Applications and Service Logs**, expand **Microsoft**, expand **Windows**, and then click **DNS-Server**.
4. Right-click **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**. The analytical log will be displayed.
5. Right-click **Analytical**, and then click **Properties**.
6. Under **When maximum event log size is reached**, select **Do not overwrite events (Clear logs manually)**, select **Enable logging**, and then click **OK**. In the **Do you want to enable this log** window, click **OK**.
7. Return to the **Windows PowerShell** console.
8. In the **Windows PowerShell** console, type the following commands, and then press Enter after each line:

```
Nslookup
Server tor-svr1
ATL-SVR1.contoso.com
```

9. Return to Event Viewer, and under **DNS-Server**, click **Analytical**.
10. Right-Click **Analytical**, and then click **Refresh**.
11. The details pane of Event Viewer should now populate with several events. Expand a few of them, explaining what they tell you. You should identify the event that returned the successful query for the address of **ATL-SVR1.contoso.com** that you did in step 8 above.
12. Close all open windows. Do not sign out.

Use Windows PowerShell to configure global DNS settings

1. On **LON-CL1**, in the search box on the taskbar, type **PowerShell**, and in the returned list, click **Windows PowerShell Desktop app**.
2. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Resolve-DnsName atl-svr1.contoso.com
```

   After a moment, you should get an error, explaining that the command timed out. This is because the Contoso domain is not reachable, even though you added it as a DNS zone on **TOR-SVR1**.

3. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**.
4. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Add-DnsServerConditionalForwarderZone –name “Contoso.com” –MasterServers 172.16.18.20
–PassThru
```

5. Review the information provided. Note that Contoso.com is listed as a forwarder.

6. Return to **LON-CL1.**
7. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Clear-DNSClientCache
```

8. In the **Windows PowerShell** console, type the following command, and then press Enter:

```
Resolve-DnsName atl-svr1.contoso.com
```

   You should receive the following response:

```
atl-svr1.contoso.com                           A      3600  Answer     172.16.18.125
```

9. Explain that this message means that the DNS zone for contoso.com has been successfully added to the DNS server on the Adatum.com zone as a conditional forwarder.

Lesson 2

Configuring zones in DNS

Contents:

Question and Answers

Question: A DNS server is authoritative for a zone if:

( ) It is set to Authoritative in the DNS Server Properties.

( ) It hosts the resource records in the zone file that is named for the zone.

( ) It has multiple CNAME resource records.

( ) It is set to Authoritative in the Zone Properties.

( ) It is set to the secondary zone server.

Answer:

( ) It is set to Authoritative in the DNS Server Properties.

(√) It hosts the resource records in the zone file that is named for the zone.

( ) It has multiple CNAME resource records.

( ) It is set to Authoritative in the Zone Properties.

( ) It is the secondary zone server.

Lesson 3

Configuring name resolution between DNS zones

Contents:

Question and Answers

Question: A stub zone consists of which of the following? (Choose two answers.)

( ) The IP address of one or more master servers that you can use to update the zone.

( ) Resource records not contained in a DNS server's zone.

( ) A cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.

( ) Requests for all Internet names forwarded to a DNS server at an Internet service provider (ISP).

( ) The delegated zone's Start of Authority resource record, NS resource records, and A resource records.

Answer:

(√) The IP address of one or more master servers that you can use to update the zone.

( ) Resource records not contained in a DNS server's zone.

( ) A cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.

( ) Requests for all Internet names forwarded to a DNS server at an Internet service provider (ISP).

(√) The delegated zone's Start of Authority resource record, NS resource records, and A resource records.

Lesson 4

Configuring DNS integration with AD DS

Contents:

Question and Answers

What are Active Directory–integrated zones?

Question: Are there any disadvantages to storing DNS information in AD DS?

> **Answer:** If you want to replicate DNS data to other non-Microsoft DNS servers, you should not store it in AD DS.

Demonstration: Configuring AD DS–integrated zones

Demonstration Steps

Promote a server as a domain controller

1. On **TOR-SVR1**, open **Server Manager**, 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, ensure that **TOR-SVR1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Domain Services**.
6. When the **Add Roles and Features Wizard** window appears, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, when the **Installation succeeded** message 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 TOR-SVR1** is visible, click **More**.
13. On the **All Server Task Details and Notifications** page, click **Promote this server to a domain controller**.
14. In the **Active Directory Domain Services Configuration Wizard**, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then click **Next**.
15. On the **Domain Controller Options** page, ensure the **Domain Name System (DNS) server** and **Global Catalog (GC)** are both selected.
16. In the **Password** and **Confirm Password** text boxes, type **Pa55w.rd**, and then click **Next**.
17. On the **DNS Options** page, click **Next**.
18. On the **Additional Options** page, click **Next**.
19. On the **Paths** page, click **Next**.
20. On the **Review Options** page, click **Next**.
21. On the **Prerequisites Check** page, click **Install**.
22. On the **You're about to be signed out** app bar, click **Close**.

Note: The server automatically restarts as part of the procedure.

23. After **TOR-SVR1** restarts, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

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

Note: Point out that this option determines that the 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** text 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 click **New Host (A or AAAA)**.
3. In the **New Host** window, in the **Name** text box, type **www**, in the **IP address** text 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 **TOR -SVR1**, open **Server Manager**, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **TOR-SVR1**, expand **Forward Lookup Zones**, and then click **TreyResearch.net**.
3. Verify that the **www** resource record exists. It might take few minutes for the record to appear, and you might have to refresh the console display.

Lesson 5

Configuring advanced DNS settings

Contents:

Resources

DNS policies

Additional Reading: For more information on DNS sinkholes, refer to: "Applying Filters on DNS Queries using Windows DNS Server Policies" at: http://aka.ms/Efxdlc

Demonstration: Configuring the GlobalNames zone

Demonstration Steps

1. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**.
2. To create an Active Directory–integrated forward lookup zone named **Fabrikam.com**, at the Windows PowerShell command prompt, type the following cmdlet, and then press Enter:

```
Add-DnsServerPrimaryZone –Name Fabrikam.com –ReplicationScope Forest
```

3. To enable support for GlobalName zones, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Set-DnsServerGlobalNameZone –AlwaysQueryServer $true
```

4. To create an Active Directory-integrated forward lookup zone named **GlobalNames**, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Add-DnsServerPrimaryZone –Name GlobalNames –ReplicationScope Forest
```

5. Close the **Windows PowerShell** window.
6. From the **Taskbar**, restore the **DNS Manager** console.
7. In the **DNS Manager** console, click **Action**, and then click **Refresh**.
8. In the **DNS Manager** console, expand **Forward Lookup Zones**, click the **Fabrikam.com** zone, right-click **Fabrikam.com**, and then click **New Host (A or AAAA)**.
9. In the **New Host** dialog box, in the **Name** text box, type **App1**.

Note: The **Name** text box uses the parent domain name if it is left blank.

10. In the **IP address** text box, type **172.16.0.200**, and then click **Add Host**.
11. Click **OK**, and then click **Done**.
12. Select and then right-click the **GlobalNames** zone, and then click **New Alias (CNAME)**.
13. In the **New Resource Record** dialog box, in the **Alias name** text box, type **App1**.
14. In the **Fully qualified domain name (FQDN) for target host** text box, type **App1.Fabrikam.com**, and then click **OK**.
15. Close DNS Manager.

Demonstration: Configuring DNS policies

Demonstration Steps

Create www.adatum.com Host record and test resolution

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In **DNS Manager** console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then select **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Alias (CNAME)...**.
4. In the **New Resource Record** window, in the **Alias name** text box, type **www**, and in the **Fully qualified domain name (FQDN) for target host** text box, type **LON-DC1.adatum.com**, and then click **OK**.
5. Switch to **TOR-SVR1**.
6. On **TOR-SVR1**, right-click **Start**, and then click **Windows PowerShell**.
7. In the **Windows PowerShell** console, type the following two commands, and press Enter after each command:

```
ipconfig /flushdns
nslookup www.adatum.com
```

8. Verify that the last command returns the IP address **172.16.0.10**.

Note: You may receive a reply that looks like the following:

```
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  172.16.0.10
Name:    lon-dc1.adatum.com
Addresses:  fd00::10
     172.16.0.10
Aliases: www.adatum.com
```

Explain to the students that the first half of the output looks like an error, but it is normal behavior if there is no reverse lookup zone. There is no reverse lookup zone on LON-DC1, and the nslookup on the client passes the query to the preferred DNS server found in the TCP/IP properties, which is this case is 172.16.0.10. The query does not have a host name to pass with the server IP address, and therefore reports with the DNS request time out and Server: Unknown line.

9. Switch to **LON-CL1**.
10. Right-click the **Start** icon and select **Command Prompt (Admin)**.
11. In the **Administrator: Command Prompt** console, type the following two commands, and press Enter after each command:

```
ipconfig /flushdns
nslookup www.adatum.com
```

12. Verify that the name resolves to an IP address **172.16.0.10**.

Configure DNS Policy

Note: There is a text file located on **LON-DC1** in **E:\Labfiles\Mod04** named **ConfigurePolicies.txt**. This file has all the below mentioned cmdlets that you can copy and paste into Windows PowerShell to eliminate excessive typing.

1. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**.
2. At the Windows PowerShell command prompt, type the following cmdlets, and then press Enter after each cmdlet:

```
Add-DnsServerClientSubnet -Name "UKSubnet" -IPv4Subnet "172.16.0.0/24"
Add-DnsServerClientSubnet -Name "CanadaSubnet" -IPv4Subnet "172.16.18.0/24"
Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "UKZoneScope"
Add-DnsServerZoneScope -ZoneName "Adatum.com" -Name "CanadaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www" -IPv4Address
"172.16.0.41" -ZoneScope "UKZoneScope"
Add-DnsServerResourceRecord -ZoneName "Adatum.com" -A -Name "www" -IPv4Address
"172.16.18.17" -ZoneScope "CanadaZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "UKPolicy" -Action ALLOW -ClientSubnet
"eq,UKSubnet" -ZoneScope "UKZoneScope,1" -ZoneName "Adatum.com"
Add-DnsServerQueryResolutionPolicy -Name "CanadaPolicy" -Action ALLOW -ClientSubnet
"eq,CanadaSubnet" -ZoneScope "CanadaZoneScope,1" -ZoneName Adatum.com
```

3. Switch **to LON-CL1**.
4. To test that the above changes worked, in Administrator Command Prompt window, type the following commands, and press Enter after each one:

```
Ipconfig /flushdns
Nslookup www.adatum.com
```

5. You should get the result of **172.16.0.41**.
6. On the host computer, in the **Hyper-V Manager** console, right-click **20741B-LON-CL2** and select **Settings**.
7. In the **Settings for 20741B-LON-CL2** window, select the **Network Adapter**, **London_Network**.
8. In the details pane, in the **Virtual switch** drop down, select **NA_WAN**, and then click **OK**.
9. Right-click **20741B-LON-CL2** and select **Start**, and then right-click **20741B-LON-CL2** again and then select **Connect**.
10. When the **20741B-LON-CL2** virtual machine completes start up, sign in as **Adatum\Administrator** with a password of **Pa55w.rd**.
11. On the Notification area of the Taskbar, right-click the Network icon, and select **Open Network and Sharing Center**.
12. In the **Network and Sharing Center** window, click the **London_Network** hyperlink, and then in the **London_Network Status** dialog box, click **Properties**.
13. In the **London_Network Properties**, select the **Internet Protocol Version 4 (TCP/IPv4)** item, and then click **Properties**.
14. In the **Internet Protocol Version 4 (TCP/IPv4) Properties**, change the **IP address** field to **172.16.18.51**, and the **Default gateway** field to **172.16.18.1**, then click **OK** twice and then **Close**.
15. **Start**, and then, in the list of Apps, scroll down and click **Windows PowerShell** folder, and then click **Windows PowerShell** item.

16. In the **Windows PowerShell** window, type the cmdlets, and press Enter after each one:

```
Ipconfig /flushdns
Nslookup www.adatum.com
```

17. You should get a result of **172.16.18.17**.
18. In the **20741B-LON-CL2 on *host* Virtual Machine Connection** window, click the **Revert** icon.

Demonstration: Configuring DNSSEC

Demonstration Steps

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then select and right-click **Adatum.com**.
3. On the context menu, click **DNSSEC**, and then click **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 **Enable the distribution of trust anchors for this zone**, 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 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** text box, type **Adatum.com** to apply the rule to the suffix of the namespace.
24. Select **Enable DNSSEC in this rule**, select the **Require DNS clients to check that the name and address data has been validated by the DNS server**, and then click **Create**.
25. Close all open windows.

Module Review and Takeaways

Best Practices

When you implement DNS, use the following best practices:

- Always use host names instead of NetBIOS names.
- Use forwarders rather than root hints.
- Be aware of potential caching issues when you troubleshoot name resolution.
- Use Active Directory–integrated zones instead of primary and secondary zones.
- Use GlobalNames zone when you must have single-name entities.
- Use DNS policies to fine-tune client name resolution and zone transfers.

Review Questions

Question: You are troubleshooting DNS name resolution from a client computer. What must you remember to do before each test?

Answer: You should clear the resolver cache before starting to troubleshoot.

Question: You are deploying DNS servers into an Active Directory domain, and your customer requires that the infrastructure be resistant to single points of failure. What must you consider when planning the DNS configuration?

Answer: You should deploy more than one AD DS domain controller with the DNS Server role installed.

Question: What benefits do you realize by using forwarders?

Answer: Forwarders are used when your local DNS server cannot resolve a query from the client using its own local zones. You usually configure forwarders to resolve Internet names. However, you also can use forwarders to optimize performance, to optimize Internet link usage on your local DNS server, and to enhance security.

Tools

Name of tool	Used for	Where to find it
DNS Manager console	Manage DNS server role	Administrative Tools
Nslookup	Troubleshoot DNS	Command-line tool
Ipconfig	Troubleshoot DNS	Command-line tool
Windows PowerShell cmdlets	Manage and troubleshoot DNS	Windows PowerShell
DNS Policies	Various scenarios involving client name resolution aspects and zone transferring	Windows PowerShell
WDK: Includes Tracelog.exe	Event tracing for Windows (ETW) consumer applications	You can "Download the WDK, WinDbg, and associated tools" at: http://aka.ms/Dbocr6

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Clients sometimes cache invalid DNS records.	Clear the DNS cache.
DNS Server performs slowly.	Use the Performance Monitor to measure the load on DNS.

Lab Review Questions and Answers

Lab A: Planning and implementing name resolution by using DNS

Question and Answers

Question: Can you install the DNS Server role on a server that is not a domain controller? If yes, are there any limitations?

Answer: Yes, you can install the DNS server role on a server that is not a domain controller. However, you cannot create Active Directory–integrated zones on a DNS server that is not a domain controller.

Question: What is the most common way to carry out Internet name resolution on a local DNS?

Answer: Organizations typically configure their local DNS with a forwarder. That forwarder is most often a DNS server of their ISP.

Question: How can you browse the content of the DNS resolver cache on a DNS server?

Answer: You can browse the content of the DNS resolver cache on a DNS server by enabling the **Advanced** view in the **DNS Manager** console or by using Windows PowerShell cmdlets.

Lab B: Integrating DNS with AD DS

Question and Answers

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 AD DS domain controller in the domain, thereby creating automatic multi-master 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 aspect of AD DS functionality.

Lab C: Configuring advanced DNS settings

Question and Answers

Question: The Windows PowerShell cmdlet Add-DnsServerZoneScope requires what two parameters?

Answer: It requires the -ZoneName to identify the zone the scope is being added to, and the -Name parameter to give the scope a name.

Module 5

Implementing and managing IPAM

Contents:

Lesson 1

Overview of IPAM

Contents:

Question and Answers

Question: To manage IPv6 with IPAM, you must enable IPv6 on the IPAM server.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

To manage IPv6 with IPAM, you must enable IPv6 on the IPAM server.

Resources

What is IPAM?

Additional Reading: For more information, refer to: http://aka.ms/Sezy6m

Lesson 2

Deploying IPAM

Contents:

Question and Answers

Question: What GPOs are created when you deploy IPAM? What are they for?

Answer: The created GPOs are:

- <Prefix>_DHCP. This GPO applies settings that allow IPAM to monitor, manage, and collect information from managed DHCP servers on the network. It sets up IPAM provisioning scheduled tasks and adds Windows Firewall inbound rules for Remote Event Log Management (RPC-EMAP and RPC), Remote Service Management (RPC-EMAP and RPC), and DHCP Server (RPCSS-In and RPC-In).
- <Prefix>_DNS. This GPO applies settings that allow IPAM to monitor and collect information from managed DNS servers on the network. It sets up IPAM provisioning scheduled tasks and adds Windows Firewall inbound rules for RPC (TCP, Incoming), RPC Endpoint Mapper (TCP, Incoming), Remote Event Log Management (RPC-EMAP and RPC), and Remote Service Management (RPC-EMAP and RPC).
- <Prefix>_DC_NPS. This GPO applies settings that allow IPAM to collect information from managed domain controllers and NPSs on the network for IP address tracking purposes. It sets up IPAM provisioning scheduled tasks and adds Windows Firewall inbound rules for Remote Event Log Management (RPC-EMAP and RPC) and Remote Service Management (RPC-EMAP and RPC).

Resources

Process of implementing IPAM

Additional Reading: For more information, refer to: http://aka.ms/Skefwm

Demonstration: Installing and provisioning the IPAM role

Demonstration Steps

Install IPAM

1. Switch to **LON-SVR2**.
2. Click **Start**, and then click **Server Manager**.
3. In Server Manager, in the results pane, click **Add roles and features**.
4. In the **Add Roles and Features Wizard**, click **Next**.
5. On the **Select installation type** page, click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, select the **IP Address Management (IPAM) Server** check box.
9. In the **Add features that are required for IP Address Management (IPAM) Server** dialog box, click **Add Features**, and then click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. 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.
7. In the **GPO name prefix** box, type **IPAM**, and then click **Next**.
8. On the **Confirm the Settings** page, click **Apply**. Provisioning will take a few moments to complete.

Note: If provisioning fails with a Windows Internal Database error, open **Services.msc** and restart the Windows Internal Database service. Then repeat steps 3 through 8.

9. When provisioning completes, click **Close**.
10. In the **IPAM Overview** pane, click **Configure server discovery**.
11. In the **Configure Server Discovery** dialog box, click **Get forests**.
12. In the **Configure Server Discovery** dialog box, click **OK**, and then click **OK** again.
13. In the **IPAM Overview** pane, click **Configure server discovery**.
14. In the **Configure Server Discovery** dialog box, click **Add**, and then click **OK**.
15. In the **IPAM Overview** pane, click **Start server discovery**.

Note: Discovery might take 5-10 minutes to run. The yellow bar indicates when discovery is complete.

16. 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 then note the status report.

Note: The IPAM server has not yet been granted permission to manage **LON-DC1** through Group Policy.

17. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
18. At the command prompt in the Windows PowerShell command-line interface, type the following command, and then press Enter.

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

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

Note: The command will take a few minutes to complete.

20. Close Windows PowerShell.

21. Switch to Server Manager.
22. In the **IPv4 details** pane, right-click **lon-dc1**, and then click **Edit Server**.
23. In the **Add or Edit Server** dialog box, in the **Manageability status** drop-down list, select **Managed**, and then click **OK**.

Note: If a Group Policy Object (GPO) error appears, switch the server back to **Unspecified**, restart **LON-DC1**, and then restart **LON-SVR2**. Sign in to both servers as **Adatum\Administrator** with the password **Pa55w.rd**.

24. Switch to **LON-DC1**.
25. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
26. At the Windows PowerShell command prompt, type the following command, and then press Enter.

```
Gpupdate /force
```

27. Close the Windows PowerShell window.
28. Switch back to **LON-SVR2**.
29. In Server Manager, right-click **LON-DC1**, and then click **Refresh Server Access Status**.
30. When completed, refresh IPv4 by clicking **Refresh**.

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

31. Click back to the **IPAM Overview** pane. In the **IPAM Overview** pane, click **Retrieve data from managed servers**.

Note: This action will take a few moments to complete.

Demonstration: Administering IPAM

Demonstration Steps

Add a custom role group

1. On **LON-SVR2**, in Server Manager, in the **IPAM navigation** pane, click **ACCESS CONTROL**. View and describe the available built-in roles.
2. Right-click **Roles**, and then click **Add User Role**.
3. In the **Add or Edit Role** dialog box, in the **Name** box, type **A Datum DHCP and DNS Management role**.
4. In the **Operations** list, select the following check boxes, and then click **OK**:
   - **DHCP server operations**
   - **DNS zone operations**
   - **DNS server operations**

Add a custom scope

1. In the navigation pane, right-click **Access Scopes**, and then click **Add Access Scope**.
2. In the **Add Access Scope** dialog box, in the **Select the parent access scope** list, click **Global**, and then click **New**.
3. In the **Name** box, type **London**, click **Add**, and then click **OK**.

Add an IPAM access policy

1. In the navigation pane, right-click **Access Policies**, and then click **Add Access Policy**.
2. In the **Add Access Policy** dialog box, under **User Settings**, click **Add**.
3. In the **Select User or Group** dialog box, click **Locations**.
4. In the **Locations** dialog box, expand **Entire Directory**, expand **Adatum.com**, click **IT**, and then click **OK**.
5. In the **Select User, Computer or Group** dialog box, type **IT**, click **Check Names**, and then click **OK**.
6. In the **Add Access Policy** dialog box, under **Access Settings**, click **New**.
7. In the **Select role** list, click **A Datum DHCP and DNS Management role**.
8. In the **Select the access scope for the role** list, click **London**, and then click **OK**.
9. In the navigation pane, click **Access Policies**. The newly created policy displays in the list.

Set the access scope

1. In the navigation pane, click **DNS and DHCP Servers**.
2. In the details pane, right-click the DNS role for LON-DC1.Adatum.com, and then click **Set Access Scope**.
3. In the **Set Access Scope** dialog box, clear the **Inherit access scope from parent** check box.
4. In the **Select the access scope** list, click **London**, and then click **OK**.
5. In the details pane, right-click the DHCP role for LON-DC1.Adatum.com, and then click **Set Access Scope**.
6. In the **Set Access Scope** dialog box, clear the **Inherit access scope from parent** check box.
7. In the **Select the access scope** list, click **London**, and then click **OK**.

Demonstration: Managing DNS with IPAM

Demonstration Steps

Add a conditional forwarder

1. On **LON-SVR2**, in Server Manager, in IPAM, on the **DNS and DHCP Servers** tab, right-click the DNS server role for LON-DC1.Adatum.com, and then click **Create DNS conditional forwarder**.
2. In the **Create DNS conditional forwarder** dialog box, in the **DNS domain** box, type **TreyResearch.net**.
3. In the **FQDN or IP address** box, type **172.16.0.11**, click **Add**, and then click **OK**.

Create a DNS zone

1. On the **DNS and DHCP Server** tab, in the details pane, right-click the DNS server role for LON-DC1.Adatum.com, and then click **Create DNS zone**.
2. In the **Create DNS zone** dialog box, in the **Zone name** box, type **Contoso.com**, and then click **OK**.

Add a DNS record

1. In the navigation pane, on the **DNS Zones** tab, in the details pane, right-click **Contoso.com**, and then click **Add DNS resource record**.
2. In the **Add DNS resource records** dialog box, click **New**.
3. In the **Resource record type** list, click **A**.
4. In the **Name** box, type **Contoso1**.
5. In the **IP address** box, type **172.32.0.99**, and then click **Add resource record**.
6. In the **Add DNS resource records** dialog box, click **OK**.
7. In the navigation pane, on the **DNS and DHCP Server** tab, right-click the DNS server role for LON-DC1.Adatum.com, and then click **Launch MMC**.
8. In the **DNS Manager** dialog box, expand **LON-DC1.Adatum.com**, expand **Forward Lookup Zones**, and then click **Contoso.com**. Verify the presence of the zone and the record that you created.
9. In the navigation pane, click **Conditional Forwarders**. Verify the presence of the conditional forwarding record that you established.
10. Close the **DNS Manager** console.

Demonstration: Managing DHCP scopes with IPAM

Demonstration Steps

1. On **LON-SVR2**, in Server Manager, in the **IPAM navigation** pane, on the **DNS and DHCP Servers** tab, right-click the DHCP server role for LON-DC1.Adatum.com, and then click **Create DHCP Scope**.
2. In the **Create DHCP Scope** dialog box, on the **General Properties** tab, in the **Scope name** box, type **Contoso**.
3. In the **Start IP address** box, type **172.32.0.100**.
4. In the **End IP address** box, type **172.32.0.200**.
5. Next to the **Activate scope on creation** option, click **No**.
6. Under **DHCP Scope Options**, click **New**.
7. In the **New Configuration** section, in the **Option** list, click **006 DNS Servers**.
8. In the **Server name** box, type **LON-DC1.Adatum.com**, click **resolve**, click **Add Configuration**, and then click **OK**.
9. In the navigation pane, on the **DNS and DHCP Server** tab, right-click the DHCP server role for LON-DC1.Adatum.com, and then click **Launch MMC**.
10. In the **DHCP** dialog box, expand **LON-DC1.Adatum.com**, expand **IPv4**, and then click **Scope [172.32.0.0] Contoso.com**. Click **Address Pool**, and then click **Scope Options** to verify the configuration of the scope.
11. Close the **DHCP** console.

Lesson 3

Managing IP address spaces by using IPAM

Contents:

Question and Answers

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 that IPAM manages. IP address ranges correspond to a managed IP address space. You typically create an IP address block to maintain an inventory for a static IP address range.

Resources

Using IPAM to manage IP addressing

Additional Reading: For more information, refer to: http://aka.ms/Rg40h1

Demonstration: Managing IP addressing with IPAM

Demonstration Steps

Add an address block in IPAM

1. On **LON-SVR2**, in Server Manager, in the **IPAM navigation** pane, click **IP Address Blocks**.
2. In the **IPv4** pane, next to the **Current view**, click **IP Address Ranges**.
3. On the upper-right side of the window, click **Tasks**, and then click **Add IP Address Block**.
4. In the **Add or Edit IPv4 Address Block** dialog box, type the following in the text boxes, and then click **OK**:
   - Network ID: **172.16.18.0**
   - Prefix length: **24**
   - Start IP address: **172.16.18.0**
   - End IP address: **172.16.18.255**
   - Description: **Toronto subnet**
5. In the **IPv4** pane, next to the **Current view**, click **IP Address Blocks**. Note the newly created address block for Toronto.

Create an IP address reservation

1. In Server Manager, on the **IPAM configuration** page, in the navigation pane, click **IP Address Blocks**.
2. In the **IPv4** pane, next to the **Current view**, click **IP Address Ranges**.
3. Right-click **172.32.0.0/16**, and then click **Edit IP Address Range**.
4. In the **Edit IP Address Range** window, click **Reservations**.
5. In the **Reservation** box, type **172.32.0.170**, click **Add**, and then click **OK**.

Module Review and Takeaways

Review Questions

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 was allocated for use elsewhere in your environment, and it 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 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 permissions to manage servers in the domain. When you run the command, it creates three GPOs that link to the domain. These GPOs apply permissions for management of domain controller, 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 6

Remote access in Windows Server 2016

Contents:

Lesson 1

Overview of remote access

Contents:

Question and Answers

Question: What kinds of policies can you configure on a Network Policy Server, and for what are they used?

Answer: You can configure two types of policies on a Network Policy Server: network policies and connection request policies. You can use network policies to manage and control authentication and authorization of remote access connection attempts. You can use connection request policies to forward remote access connection attempts to another RADIUS (Network Policy Server) server for processing.

Question: When you first install the Network Policy and Access Services role, all connections to the Remote Access server are allowed.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

When you first deploy the Network Policy and Access Services role, the two default network policies deny remote access to all connection attempts. You must configure at least one policy to allow access.

Discussion: When to use remote access

Question: Do you allow users to connect to your network resources remotely? If so, how?

Answer: Answers may vary but could include:

- Access to the company´s VPN server.
- Access to company resources via DirectAccess.
- Access to company resource by using RDS.

Question: What are your business requirements for using remote access?

Answer: Answers may vary but could include:

- Allowing your administrators to work from home.
- Fix issues that arise during weekends.
- Allow users access to company resources while traveling.

Resources

Managing remote access in Windows Server 2016

Additional Reading: For more information, refer to Remote Access Cmdlets: http://aka.ms/Fp4ry6

Network Policy Server policies

Additional Reading: For more information, refer to RADIUS Proxy: http://aka.ms/Oy16cb

Demonstration: Installing and managing the Remote Access server role

Demonstration Steps

Install the Remote Access server role

1. On LON-SVR1, click the **Start** button, and then click the **Server Manager** tile.
2. In **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
3. On the **Before you begin** page, 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 **Remote Access**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Remote Access** page, click **Next**.
9. On the **Select role services** page, click **DirectAccess and VPN (RAS)**, and then in the **Add Roles and Features Wizard** dialog box, click **Add Features**.
10. Verify that **DirectAccess and VPN (RAS)** is selected, and then on the **Select role services** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. 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.

Demonstration: Configuring Network Policy Server policies

Demonstration Steps

1. On EU-RTR, open **Server Manager**, and then on the **Tools** menu, click **Network Policy Server**.
2. In the **Network Policy Server** console, in the navigation pane, expand **Policies**, right-click **Network Policies**, and then click **New**.
3. In the **New Network Policy Wizard**, in the **Policy name** box, type **Adatum IT VPN**
4. In the **Type of network access server** drop-down box, click **Remote Access Server (VPN-Dial up)**, and then click **Next**.
5. On the **Specify Conditions** page, click **Add**.
6. In the **Select condition** dialog box, click **Windows Groups**, and then click **Add**.
7. In the **Windows Groups** dialog box, click **Add Groups**.

8. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** box, type **IT**, click **Check Names**, and then click **OK**.
9. Click **OK** again, and then click **Next**.
10. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then click **Next**.
11. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
12. To add **EAP Types**, click **Add**.
13. On the **Add EAP** page, click **Microsoft Secured password (EAP-MSCHAP v2)**, and then click **OK**.
14. To add **EAP Types**, click **Add**.
15. On the **Add EAP** page, click **Microsoft: Smart Card or other certificate**, click **OK**, and then click **Next**.
16. On the **Configure Constraints** page, click **Next**.
17. On the **Configure Settings** page, click **Next**.
18. On the **Completing New Network Policy** page, click **Finish**.
19. Close all open windows.

Lesson 2

Implementing Web Application Proxy

Contents:

Question and Answers

Question: The Web Application Proxy role requires AD FS.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

You must install AD FS in your environment if you plan to use the Web Application Proxy role in Windows Server 2016. This is a requirement even if you plan to use only pass-through authentication.

Question: What types of preauthentication does Web Application Proxy support?

Answer: Web Application Proxy supports two types of preauthentication: AD FS preauthentication and pass-through preauthentication.

Resources

Publishing applications with Web Application Proxy

Additional Reading: For more information, refer to Publishing Applications with SharePoint, Exchange and RDG: http://aka.ms/Qopw7d

Demonstration: Publishing a secure website

Demonstration Steps

Move the client to the Internet

1. To move the client from the internal network to the Internet, on LON-CL1, right-click the **Start** button, and then click **Network Connections**.
2. In **Network Connections**, right-click **London_Network**, and then click **Disable**.
3. Right-click **Internet**, and then click **Enable**.
4. On the taskbar, click the **Microsoft Edge** icon.
5. In **Microsoft Edge**, in the **Search or enter web address** box, type **https://lon-svr1.adatum.com**, and then press Enter. Notice that a Network Error message displays.
6. Right-click the **Start** button, and then click **Run**. In the **Run** dialog box, type **mstsc**, and then press Enter.
7. In the **Remote Desktop Connection** app, in the **Computer** box, type **lon-dc1**, and then press Enter. Notice that you cannot connect to lon-dc1, because the computer cannot be found on the network.
8. Close all open windows.

Note: You are unable to open the internal website running on lon-svr1 and connect to lon-dc1 by using Remote Desktop because the client cannot access the internal network.

Install the Web Application Proxy role service

1. Switch to EU-RTR.
2. Click the **Start** button, and then click the **Server Manager** tile.
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** three times.
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 ADFSWAP farm

1. On EU-RTR, right-click the **Start** button, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type **mmc**, and then press Enter.
3. In the MMC, on the **File** menu, click **Add/Remove Snap-In**.
4. In the **Add or Remove Snap-ins** window, 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)**, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
7. On the **Before You Begin** page, click **Next**.
8. On the **Select Certificate Enrollment Policy** page, click **Next**.
9. On the **Request Certificates** page, click **Adatum Web Server**, and then click the **More information is required to enroll for this certificate. Click here to configure settings** link.
10. In the **Subject name** section, in the **Type** drop-down list, select **Common name**, in the **Value** box, type **adfswap.adatum.com**, and then click **Add**.
11. In the **Alternative name** list, under the **Type** box, click the drop-down list, and then select **DNS**. In the **Value** box, type **adfswap.adatum.com**, and then click **Add**.
12. In the **Alternative name** list, click **DNS**, in the **Value** box, type **rdgw.adatum.com**, and then click **Add**.
13. In the **Alternative name** list, click **DNS**, in the **Value** box, type **lon-svr1.adatum.com**, and then click **Add**.
14. Click **OK** to close the **Certificate Properties** dialog box.
15. Click **Enroll** to proceed with Certificate Enrollment.
16. Click **Finish** to close the **Certificate Enrollment** dialog box.

Configure Web Application Proxy

1. In **Server Manager**, from the **Tools** menu, open the **Remote Access Management** console.
2. 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 **adfswap.adatum.com**, which is the FQDN of the federation service.
    b. In the **User name** box, type **Administrator**, in the **Password** box, type **Pa55w.rd**, 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 **adfswap.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**.

 **Note:** If you receive an error message, check if LON-SVR2 is started and if the AD FS service is running on LON-SVR2. Then return to step 2 to run the **Web Application Proxy Configuration Wizard** again.

Publish the internal website

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 **Adatum LOB Web App (LON-SVR1)**.
    b. In the **External URL** box, type **https://lon-svr1.adatum.com**.
    c. In the **External certificate** list, click **adfswap.adatum.com**.
    d. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed, and then click **Next**.

 **Note:** The value for **Backend server URL** is automatically entered when you type the external URL.

5. On the **Confirmation** page, review the settings, and then click **Publish**. You can 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**.

Configure internal website authentication

1. Switch to LON-SVR1.
2. Click the **Start** button, and then click the **Server Manager** tile. Click the **Tools** menu, and then click **Internet Information Services (IIS) Manager**.
3. In the **Internet Information Services (IIS) Manager** console, expand **LON-SVR1 (ADATUM\administrator)**.
4. Expand **Sites**, and then click **Default Web site**.

5. In the **Internet Information Services (IIS) Manager** console, in the **Default Web Site Home** pane, double-click **Authentication**.
6. In the **Internet Information Services (IIS) Manager** console, in the **Authentication** pane, right-click **Windows Authentication**, and then click **Enable**.
7. In the **Internet Information Services (IIS) Manager** console, in the **Authentication** pane, right-click **Anonymous Authentication**, and then click **Disable**.
8. Close the **Internet Information Services (IIS) Manager** console.

Verify access to the internal website

1. Switch to LON-CL1.
2. On the taskbar, click the **Microsoft Edge** icon.
3. In the **Search or enter web address** box, type **https://lon-svr1.adatum.com**, and then press Enter.
4. When prompted, in the **Microsoft Edge** dialog box, type **adatum\logan** for the user name and **Pa55w.rd** for the password, and then click **OK**.
5. Verify that the default IIS 9.0 webpage for LON-SVR1 opens.

Module Review and Takeaways

Best Practice

Remember that AD FS is required when implementing the Web Application Proxy role. If you plan to use only pass-through authentication with Web Application Proxy, you need only install AD FS and run the AD FS configuration wizard; you do not have to configure anything else.

For ease of deployment, consider using public SSL certificates for your Web Application Proxy server, Remote Desktop Gateway server, and web application servers.

Review Questions

Question: What remote access solutions can you deploy by using Windows Server 2016?

Answer: In Windows Server 2016, you can deploy the following remote access solutions: DirectAccess, VPN, Routing, and Web Application Proxy.

Question: What type of remote access solutions can you provide by using VPN in Windows Server 2016?

Answer: You can configure the following remote access solutions by using VPN in Windows Server 2016:

- 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 2016, 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 2016 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 2016?

Answer: Web Application Proxy in Windows Server 2016 is a role service that you can use for publishing web applications or Remote Desktop Gateway Servers. 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

The following table lists the tools that this module references.

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

Tool	Use for	Where to find it
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 a customized MMC for managing operating system roles, features, and settings.	Run from command-line
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

Lab Review Questions and Answers

Lab: 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 7

Implementing DirectAccess

Contents:

Lesson 1

Overview of DirectAccess

Contents:

Resources

DirectAccess components

Additional Reading: For more information, refer to: "Internet Protocol Version 6 (IPv6) Overview" at: http://aka.ms/l43ird

Additional Reading: For more information, refer to: "Remote Access Overview" at: http://aka.ms/Rlc58t

DirectAccess tunneling protocol options

Additional Reading: For more information, refer to: "IPv6 transition technologies" at: http://aka.ms/Hn3u61

Additional Reading: For more information, refer to: "Teredo Overview" at: http://aka.ms/Jdw9r8

Additional Reading: For more information, refer to: "[MS-IPHTTPS]: IP over HTTPS (IP-HTTPS) Tunneling Protocol" at: http://aka.ms/Bcviz1

Managing remote access in Windows Server 2016

Additional Reading: For a complete list of remote access cmdlets in Windows PowerShell, refer to: "Remote Access Cmdlets" at: http://aka.ms/Ar09tz

Demonstration: Installing the Remote Access server role

Demonstration Steps

Install the Remote Access server role

1. On LON-SVR1, click **Start**, click **Server Manager**, 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)**.
9. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then verify that **DirectAccess and VPN (RAS)** is selected.
10. On the **Select role services** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. When the installation completes, click **Close**.

Lesson 2

Implementing DirectAccess by using the Getting Started Wizard

Contents:

Question and Answers

Question: How many GPOs does the Getting Started Wizard create?

( ) 1

( ) 2

( ) 3

( ) 4

( ) 5

Answer:

( ) 1

(√) 2

( ) 3

( ) 4

( ) 5

Feedback:

The Getting Started Wizard creates two GPOs: DirectAccess Server Settings, and DirectAccess Client Settings.

Question: You want to deploy a dedicated network location server. Would you be able to use the Getting Started Wizard for that?

Answer: No. If you use the Getting Started Wizard, the network location server and DirectAccess server will be the same machine. You would have to configure network location server manually from the **Remote Access Management** console.

Resources

Getting Started Wizard configuration changes

Additional Reading: For more information, refer to: "DirectAccess Unsupported Configurations" at: http://aka.ms/R3r2ec

Demonstration: Running the Getting Started Wizard

Demonstration Steps

Create a security group for DirectAccess client computers

1. On LON-DC1, in **Server Manager**, in the upper-right corner, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console tree, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
3. In the **New Object – Organizational Unit** dialog box, in the **Name** text box, type **Special Accounts**, and then click **OK**.
4. In the **Active Directory Users and Computers** console tree, expand **Adatum.com**, right-click **Special Accounts**, click **New**, and then click **Group**.

5. In the **New Object - Group** dialog box, in the **Group name** text box, type **DirectAccessClients**.
6. Under the **Group** scope, ensure that **Global** is selected. Under the **Group** type, ensure that **Security** is selected, and then click **OK**.
7. In the details pane, right-click **DirectAccessClients**, and then click **Properties**.
8. In the **DirectAccessClients Properties** dialog box, click the **Members** tab, and then click **Add**.
9. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.
10. In the **Enter the object names to select (examples)** text box, type **LON-CL1**, click **Check Names**, and then click **OK**.
11. Verify that **LON-CL1** displays under **Members**, and then click **OK**.
12. Close the **Active Directory Users and Computers** console.

Configure DirectAccess by running the Getting Started Wizard

1. Switch to **EU-RTR**.
2. Click **Start**, and then click the **Server Manager** tile.
3. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
4. In the **Remote Access Management** console, under **Configuration**, click **DirectAccess and VPN**, and then click **Run the Getting Started Wizard**.
5. In the **Getting Started Wizard**, on the **Configure Remote Access** page, click **Deploy DirectAccess only**.
6. On the **Network Topology** page, verify that **Edge** is selected, in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** text box, type **131.107.0.10**, and then click **Next**.
7. On the **Configure Remote Access** page, click the **here** link.

 **Note:** Ensure that you click the **here** link as it will display an additional window for configuring both Group Policy Object (GPO) settings, and Active Directory groups, which will contain the computers that will be affected by the DirectAccess settings.

8. On the **Remote Access Review** page, verify that two GPO objects are created: **DirectAccess Server Settings**, and **DirectAccess Client settings**.
9. Next to **Remote Clients**, click the **Change** link.
10. Click **Domain Computers (ADATUM\Domain Computers)**, and then click **Remove**.
11. Click **Add**. In **Enter the object names to select (examples)** text box, type **direct**, and then click **Check Names**. Verify that **DirectAccessClients** displays, and then click **OK**.
12. Clear the **Enable DirectAccess for mobile computers only** check box, and then click **Next**.
13. On the **DirectAccess Client Setup** page, fill out the following information, and then click **Finish**:
    - Helpdesk email address: **DAHelp@adatum.com**
    - DirectAccess connection name: **A. Datum DirectAccess**

Note: Mention to the students that even though including a Helpdesk email address is not required, we highly recommend it. If no email is available, the user will not be able to collect the DirectAccess client log files if there is an issue.

14. On the **Remote Access Review** page, click **OK**.
15. On the **Configure Remote Access** page, click **Finish** and wait for the configuration to finish.
16. In the **Applying Getting Started Wizard Settings** dialog box, verify that the configuration was successful, and then click **Close**.

Demonstration: Identifying the Getting Started Wizard settings

Demonstration Steps

Review the configuration changes in the Remote Access Management console

1. Switch to the **Remote Access Management** console on EU-RTR
2. In the **Remote Access Setup** window, under the image of the client computer named **Step 1 Remote Clients**, click **Edit**.
3. In the **DirectAccess Client Setup** window, click **Deployment Scenario**, and review the default settings.
4. Click **Select Groups**, and record the default settings.
5. Click **Network Connectivity Assistant**, and then record the default settings.
6. Click **Cancel**, and then click **OK**.
7. In the **Remote Access Setup** window, under the image of the client computer named **Step 2 Remote Access Server**, click **Edit**.
8. In the **Remote Access Server Setup** window, click **Network Topology**, and review the default settings.
9. Click **Network Adapters**, and review the default settings.
10. Click **Authentication**, and record 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 3 Infrastructure Servers**, click **Edit**.
13. In the **Infrastructure Server Setup** window, click **Network Location Server**, and record the default settings.
14. Click **DNS**, and review the default settings.
15. Click **DNS Suffix Search List**, and record the default settings.
16. Click **Management**, and review the default settings.
17. Click **Cancel**, and then click **OK**.
18. In the **Remote Access Setup** window, under the image of the client computer named **Step 4 Application Servers**, click **Edit**.
19. In the **DirectAccess Application Server Setup** window, review the default settings. Click **Cancel**, and then click **OK**.
20. Close all open windows.

Review the infrastructure changes in the Group Policy Management Console

1. On **EU-RTR**, click **Start** and then click the **Server Manager** icon.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management Console**, expand **Forest: Adatum.com,** expand **Domains**, and then expand **Adatum.com**. Point out the two new GPOs that were created:
   - **DirectAccess Client Settings**
   - **DirectAccess Server Settings**
4. In the navigation pane, click the **DirectAccess Server Settings** GPO.
5. In the **Group Policy Management Console** dialog box, click **OK**, and then in the details pane, click the **Settings** tab.
6. 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.
7. Point out that there are three groups of firewall settings configured for the DirectAccess servers: **Global Settings**, **Inbound Rules**, and **Connection Security Settings**.
8. In the **Global Settings** row, click the **show** link, and then review the **IPsec exempt** setting for **ICMP**.
9. In the **Inbound Rules** row, click the **show** link, and then review the following settings:
   - **Core Networking – IPHTTPS (TCP-In)**. Note that this rule allows the inbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
   - **Domain Name Server (UDP-In)**, and **Domain Name Server (TCP-In)**. Explain that these rules allow traffic to the DNS64 server that is deployed on the Remote Access server. Point out the IPv6 address in the rules, and explain that it is the address of the London_Network adapter on EU-RTR, which can be verified by running the **ipconfig /all** command in a Windows PowerShell window.
10. 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 that you recorded in step 9 of the previous section in this demonstration. Notice that they are the same prefixes that you configured in the Getting Started Wizard.
11. In the **Rules** row, click the **hide** link.
12. Under the **Connection Security Settings** row, in the **First Authentication** row, click the **show** link, and then review the Kerberos authentication setting.
13. Repeat step 12 for the **Second Authentication**, **Key Exchange (Main Mode)**, and **Data Protection (Quick Mode)** settings.
14. In the navigation pane, click the **DirectAccess Client Settings** GPO.
15. In the **Group Policy Management Console** dialog box, click **OK**.
16. In the details pane, click the **Settings** tab.
17. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, click the **show** link on the right side. In the **Public Key Policies/Trusted Root Certification Authorities** row, click the **show** link, and then in the **Certificates** row, click the **Show** link. Note 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.

18. In the details pane, under **Computer Configuration (Enabled)**, for both the **Security Setting** row and in the **Windows Firewall with Advanced Security** row, click the **show** link.
19. Notice that there are three groups of firewall settings configured for the DirectAccess clients: **Global Settings**, **Outbound Rules**, and **Connection Security Settings**.
20. In the **Global Settings** row, click the **show** link, and then review the IPsec ICMP exception setting.
21. 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.
22. In the **Connection Security Settings** row, click the **show** link, and then in the **Rules** row, click the **show** link.
23. Review the three rules, and then compare the IPv6 address prefixes with the IPv6 address prefixes that you recorded in step 9 in the previous section of this demonstration. Notice that they are the same prefixes that they configured with the Getting Started Wizard.
24. In the **Rules** row, click the **hide** link.
25. Under the **Connection Security Settings** row, in the **First Authentication** row, click the **show** link, and then review the Kerberos authentication setting.
26. Repeat step 25 for the following rows: **Second Authentication**, **Key Exchange (Main Mode)** and **Data Protection (Quick Mode)**.
27. Close the **Group Policy Management Console**.
28. On LON-DC1, in **Server Manager**, click **Tools**, and then click **DNS**.
29. In the **Domain Name System (DNS) Manager** console, in the navigation pane, expand **Forward Lookup Zones**, and then expand **Adatum.com**.
30. Review the A and AAAA records for the following hosts:
    - **directaccess-corpConnectivityHost**
    - **DirectAccess-NLS**
    - **directaccess-WebProbeHost**.

    The Getting Started Wizard creates these records.

Lesson 3

Implementing and managing an advanced DirectAccess infrastructure

Contents:

Question and Answers

Question: What must you configure in order to use computers running Windows 7 as DirectAccess clients?

> **Answer:** You must configure your DirectAccess deployment to use certificates in order to support Windows 7 as a DirectAccess client.

Question: What must you configure on the DirectAccess server so the users can see the Collect logs button?

> **Answer:** You must fill out the **Helpdesk email address** field when configuring the DirectAccess server.

Resources

Load balancing and high availability options

Additional Reading: For more information, refer to: "Plan a Load-Balanced Cluster Deployment" at: http://aka.ms/H2edc3

Supporting multiple locations

Additional Reading: For more information, refer to: "Deploy Multiple Remote Access Servers in a Multisite Deployment" at: http://aka.ms/Jz1esb

Additional Reading: For more information, refer to: "Planning for Multi-site DirectAccess" at: http://aka.ms/T6qfvh

Integrating a PKI with DirectAccess

Additional Reading: For more information, refer to: "Active Directory Certificate Services" at: http://aka.ms/T8xtn9

Implementing client certificates for DirectAccess

Additional Reading: For more information, refer to: "Configure DirectAccess with OTP Authentication" at: http://aka.ms/Ax93rb

Internal network configuration options

Additional Reading: For more information, refer to: "Step 2: Plan the DirectAccess Deployment" at: https://aka.ms/f2rnc6

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** console, click **Direct Access and VPN**.
3. Under Step 1, click **Edit** to select the clients that will be enabled for 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 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** dialog box, verify that **HTTP** is selected, and then in the text box next to **HTTP**, type **https://lon-svr1.adatum.com**.
9. Click **Validate**, and then click **Add**.
10. On the **Network Connectivity Assistant** page, click **Finish**.
11. Under Step 2, click **Edit**.
12. On the **Network Topology** page, verify that **Edge** is selected and **131.107.0.10** is listed and then click **Next**.
13. 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**.
14. On the **Authentication** page, click **Use computer certificates**, click **Browse**, verify that **AdatumCA** is listed, and then click **OK**.
15. Click **Enable Windows 7 client computers to connect via DirectAccess**, and then click **Finish**.
16. In the **Remote Access Setup** pane, under Step 3, click **Edit**.
17. 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**.
18. On the **DNS** page, click **Next**.
19. On the **DNS Suffix Search List** page, click **Next**.
20. On the **Management** page, click **Finish**.
21. Under Step 4, click **Edit**.
22. On the **DirectAccess Application Server Setup** page, click **Finish**.
23. Click **Finish** to apply the changes.
24. On 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 10 clients

1. Switch to LON-CL1.
2. Restart LON-CL1, and then sign in again as **Adatum\Administrator** with the password of **Pa55w.rd**.
3. Open a **Command Prompt** window, and then type the following commands, pressing Enter at the end of each line:

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

4. Verify that **DirectAccess Client Settings** GPO displays in the list of Applied Policy objects for the Computer Settings.
5. Close the **Command Prompt** window.

Move the client computer to the Internet virtual network

1. To move the client from the intranet to the public network, on LON-CL1, right-click **Start**, and then click **Network Connections**.
2. In the **Network Connections** window, right-click **London_Network**, and then click **Disable**.
3. Right-click **Internet**, and then click **Enable**.
4. Close the **Network Connections** window.

Verify connectivity to the DirectAccess server

1. On **LON-CL1**, open a **Command Prompt** window.
2. At the command prompt, type the following command, and then press Enter:

```
ipconfig
```

   Notice the IPv6 address that starts with 2002. This is an IP-HTTPS address.

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

```
Netsh name show effectivepolicy
```

4. Click **Start**, and then click **Settings**.
5. In **Settings**, select **Network & Internet**, and then click **DirectAccess**.
6. Verify that **Your PC is set up correctly for single-site DirectAccess** is displayed under **Location**.
7. Notice the **Collect** button under **Troubleshooting info**.

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 **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.

5. If no information displays under the **Connected Clients** list, restart **EU-RTR** and login as **Adatum\Administrator**. Once **EU-RTR** has re-started, restart **LON-CL1**, login as **Adatum\Administrator**, and repeat step 4.
6. In the left pane, click **Reporting**, and then in the central pane, click **Configure Accounting**.
7. In the **Configure Accounting** window, under **Select Accounting Method**, click **Use inbox accounting**, click **Apply**, and then click **Close**.
8. In the central pane, under **Remote Access Reporting**, click **Generate Report** and review the data returned.
9. Close the **Remote Access Management Console**.

Module Review and Takeaways

Best Practices

- Windows Server 2016, Windows 10, Windows 8.1 and Windows 8 include 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, and Network Connectivity Assistant on the client side.
- DirectAccess now can access IP4 servers on your network. In addition, your servers do not require that you implement IPv6 addresses through DirectAccess because your DirectAccess server acts as a proxy.
- Consider integrating DirectAccess with your existing Remote Access solution. Windows Server 2016 can implement a DirectAccess server behind the NAT device, which is the most common remote access solution for organizations.

Review Questions

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

Answer: The primary 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 can be managed by the administrators.
- 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 which DNS server to contact, and the DNS client behavior for that namespace.

Tools

Tool	Use for	Where to find it
Remote Access	Managing DirectAccess and VPN	Server Manager/Tools

Tool	Use for	Where to find it
Management Console		
Remote Access Getting Started Wizard	A graphical tool that simplifies DirectAccess configuration	Server Manager/Tools/Remote Access Management console
Dnscmd.exe	A command-line tool used for DNS management	Run from the command line
Services.msc	Helps in managing Windows services	Server Manager/Tools
Gpedit.msc	Helps in editing the Local Group Policy	Run from the command line
IPconfig.exe	A command-line tool that displays the current TCP/IP network configuration	Run from the 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 settings.	Run from the command line
Gpupdate.exe	Helps in managing Group Policy applications	Run from the 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 an efficient way to troubleshoot their issues.	Basic troubleshooting is integrated in the 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 DirectAccessClients group?

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

Question: How will you configure an IPv6 address for client computers running Windows 10 to use DirectAccess?

Answer: Global unicast IPv6 addresses are generated automatically based on the network infrastructure. As a result, Windows 10 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.

Module 8

Implementing VPNs

Contents:

Lesson 1

Planning VPNs

Contents:

Question and Answers

Question: What are the names of the various tunnel protocols that you can use in Windows Server 2016?

Answer: You can use the PPTP, L2TP, IKEv2, and SSTP tunnel protocols in Windows Server 2016.

Question: What are the requirements for VPN Reconnect?

Answer: The requirements for using VPN Reconnect are:

- A computer that is running Windows Server 2016, Windows Server 2012, or Windows Server 2008 R2 as a VPN server.
- A computer that is running Windows 10, Windows 8, Windows Server 2012, Windows 7, or Windows Server 2008 R2 client.
- PKI, because VPN Reconnect requires a computer certificate for a remote connection. You can use certificates that an internal CA or a public CA issues.

Question: You can use app-triggered VPN with domain-member computers.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

One of the requirements for using app-triggered VPN is that the client computer *cannot* be a domain member.

Lesson 2

Implementing VPNs

Contents:

Question and Answers

Question: How many network interface cards are required when configuring a VPN server in Windows Server 2016?

Answer: Two network interface cards are required. One must be connected to the internal network, and one must be connected to the Internet.

Question: What methods can you use to distribute a VPN profile to your end users?

Answer: You can distribute VPN profiles to your end users by using:

- System Center Configuration Manager
- Group Policy
- A startup script
- A logon script

Question: What is the maximum number of ports that you can configure for SSTP?

( ) 25

( ) 75

( ) 128

( ) 500

( ) 999

Answer:

( ) 25

( ) 75

( ) 128

( ) 500

(√) 999

Feedback:

You can configure a maximum of 999 SSTP ports on a Remote Access server that is running Windows Server 2016.

Resources

Distributing VPN profiles

Additional Reading: For more information, refer to "How to Create VPN profiles in System Center Configuration Manager" at: http://aka.ms/Gmn5hp

Additional Reading: For more information, refer to "VPN connections in Microsoft Intune" at: http://aka.ms/vp3kds

Additional Reading: For more information, refer to "Deploying VPN Connections by Using PowerShell and Group Policy" at: http://aka.ms/Khk938

Demonstration: Configuring VPN

Demonstration Steps

Prepare the environment

1. On **LON-DC1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. At the **Windows PowerShell** command prompt, type the following command, and then press Enter:

```
cd E:\Labfiles\Mod08
```

3. At the **Windows PowerShell** command prompt, type the following command, and then press Enter:

```
.\mod8.ps1
```

4. Wait for the script to complete, which should take approximately 20 seconds.

Request certificate for EU-RTR

1. On **EU-RTR**, click **Start**, and then type **Command Prompt**. In the results, click **Command Prompt**.
2. In the **Command Prompt** window, type the following command, and then press Enter:

```
mmc
```

3. In the **Console** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, click **Certificates**, and then click **Add**.
5. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.
6. In the **Select Computer** dialog box, click **Local computer**, click **Finish**, and then click **OK**.
7. In the **Certificates** snap-in, in the console tree of the **Certificates** snap-in, navigate to **Certificates (Local Computer)\Personal**.
8. Right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
9. On the Before you begin page, click Next, and then, on the Select Certificate Enrollment Policy page, click Next.
10. On the Request Certificates page, click Adatum Web Server, and then click More information is required to enroll for this certificate. Click here to configure settings.
11. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, under **Type**, select **Common name**.
12. In the **Value** text box, type **131.107.0.10**, and then click **Add**.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the **Certificates** snap-in, expand **Personal** and click **Certificates**, and then, in the **details** pane, verify that a new certificate with the name **131.107.0.10** is enrolled with **Intended Purposes** of **Server Authentication**.
15. Close the console window.
16. When you receive a prompt to save the settings, click **No**.

Change the HTTPS bindings

1. On EU-RTR, open Server Manager, click Tools, and then click Internet Information Services (IIS) Manager.
2. In the Internet Information Services (IIS) Manager, expand EU-RTR (ADATUM\Administrator).

3. In Internet Information Services (IIS) Manager, in the console tree, expand Sites, and then click Default Web site.
4. In the **Actions** pane, click **Bindings**, and then click **Add**.
5. In the **Add Site Binding** dialog box, under the **Type** select **https** and in the **SSL Certificate** list, click the **131.107.0.10** certificate, click **OK**, and then click **Close**.
6. Close the Internet Information Services (IIS) Manager console.

Review the default VPN configuration

1. On **EU-RTR**, in **Server Manager**, click **Tools**, and then click **Routing and Remote Access**.
2. Maximize the **Routing and Remote Access** window, right-click **EU-RTR (local)**, and then select **Disable Routing and Remote Access**.
3. When you receive a prompt, in the **Routing and Remote Access** dialog box, click **Yes**.
4. Right-click **EU-RTR (local)**, and then select **Configure and Enable Routing and Remote Access**.
5. On the **Welcome to Routing and Remote Access Server Setup Wizard**, click **Next**.
6. On the **Configuration** page, select **Custom configuration**, and then click **Next**.
7. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then click **Next**.
8. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**.
9. When you receive a prompt, in the **Routing and Remote Access** dialog box, click **Start service**.
10. Expand **EU-RTR (local)**, right-click **Ports**, and then click **Properties**.
11. In the **Ports Properties** dialog box, verify that five ports exist for **Wan Miniport (SSTP)**, **Wan Miniport (IKEv2)**, **Wan Miniport (PPTP)**, and **Wan Miniport (L2TP)**.
12. Double-click **WAN Miniport (SSTP)**. In the **Maximum ports** text box, type **4**, and then click **OK**.
13. In the **Routing and Remote Access** message box, click **Yes**.
14. Repeat steps 12 and 13 for IKEv2, PPTP, and L2TP.
15. To close the **Ports Properties** dialog box, click **OK**.
16. Right-click **EU-RTR (local)**, and then click **Properties**.
17. In the **EU-RTR (local) Properties** dialog box, on the **General** tab, verify that **IPv4 Remote access server** is selected.
18. Click the **Security** tab, and click the drop-down arrow next to **Certificate**, and then select **131.107.0.10**.
19. Click **Authentication Methods**, verify that **EAP** is selected as the authentication protocol, and then click **OK**.
20. Click the **IPv4** tab, and then verify that VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
21. To close the **EU-RTR (local) Properties** dialog box, click **OK**, and then, when you receive a prompt, click **Yes**.

Configure the Remote Access policies

1. On **EU-RTR**, in **Server Manager**, on the **Tools** menu, click **Network Policy Server**.
2. In the **Network Policy Server** console, in the navigation pane, expand **Policies**, and then click **Network Policies**.

3. In the **navigation** pane, right-click **Network Policies**, and then click **New**.
4. In the **New Network Policy Wizard**, in the **Policy name** text box, type **Adatum IT VPN**.
5. In the **Type of network access server** list, click **Remote Access Server(VPN-Dial up)**, and then click **Next**.
6. On the **Specify Conditions** page, click **Add**.
7. In the **Select condition** dialog box, click **Windows Groups**, and then click **Add**.
8. In the **Windows Groups** dialog box, click **Add Groups**.
9. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** text box, type **IT**, click **Check Names**, and then click **OK**.
10. Click **OK** again, and then click **Next**.
11. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then click **Next**.
12. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
13. To add **EAP Types**, click **Add**.
14. On the **Add EAP** page, click **Microsoft Secured password (EAP-MSCHAP v2)**, and then click **OK**.
15. To add **EAP Types**, click **Add**.
16. On the **Add EAP** page, click **Microsoft: Smart Card or other certificate**, click **OK**, and then click **Next**.
17. On the **Configure Constraints** page, click **Next**.
18. On the **Configure Settings** page, click **Next**.
19. On the **Completing New Network Policy** page, click **Finish**.
20. Close all open windows.

Demonstration: Creating a connection profile

Demonstration Steps

Install CMAK

1. If necessary, on **LON-CL1**, sign in as **Adatum\administrator** by using the password **Pa55w.rd**.
2. Right-click **Start**, and then click **Programs and Features**.
3. In the **Programs and Features** dialog box, click **Turn Windows features on or off**.
4. In the **Windows Features** dialog box, select **RAS Connection Manager Administration Kit (CMAK)**, and then click **OK**.
5. Click **Close**.

Create a connection profile

1. Right-click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **System and Security**, and then click **Administrative Tools**.
3. Double-click **Connection Manager Administration Kit**.
4. On the **Welcome to the Connection Manager Administration Kit Wizard** page, 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**, and 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 **Phone book from this profile**.
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 **This PC**, expand **Local Disk (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.

Module Review and Takeaways

Best Practices

- We recommend that you do not use PPTP for remote access and site-to-site VPN connections because it is considered unsecured. You should use L2TP, IKEv2, or SSTP instead. If you must use PPTP due to capability issues, you should use it with MS- CHAP v2 and PEAP, because of a security flaw in PPTP.
- You can monitor the VPN environment by using Windows PowerShell and Remote Access Management.
- You should use DHCP to allocate IP addresses to your VPN clients, unless you have fewer than 20 clients.
- You should not enable the CHAP, SPAP, or PAP authentication protocols, because they are not secure.
- You can restrict connections to your VPN server by user name or IP address.

Review Questions

Question: What remote-access solutions can you deploy by using Windows Server 2016?

> **Answer:** In Windows Server 2016, you can deploy the following remote access solutions: DirectAccess, VPN, Routing, and Web Application Proxy.

Question: What type of remote-access solutions can you provide by using VPN in Windows Server 2016?

> **Answer:** You can configure the following remote-access solutions by using VPN in Windows Server 2016:
>
> - Secure remote access to internal network resources for users located on the Internet. The users connect to a VPN server that is running Windows Server 2016.
> - Secure communication between network resources that are located on different geographical locations or sites. This solution is *site-to-site VPN*. In each site, a VPN server that is running Windows Server 2016 encrypts communication between the sites.

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
Dnscmd.exe	A command-line tool for DNS management	Run from command-line
Services.msc	Helps in managing Windows services	Server Manager/Tools
Gpedit.msc	Helps in editing 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

Tool	Use for	Where to find it
DNS Manager console	Helps in configuring name resolution	Server Manager/Tools
Mmc.exe	Creating customized MMC for managing operating-system roles, features, and settings.	Run from command-line
Gpupdate.exe	Helps in managing Group Policy application	Run from command-line
Active Directory Users and Computers	Helping to configure group membership for client computers that you will configure with DirectAccess	Server Manager/Tools

Lab Review Questions and Answers

Lab: Implementing VPN

Question and Answers

Question: In the lab, you configured the VPN server to assign IPv4 addresses by using Dynamic Host Configuration Protocol (DHCP). Are there any other options for assigning IPv4 addresses to clients?

> **Answer:** Yes, you could use a static address pool by specifying a range of IPv4 addresses. However, you must remember to exclude these in DHCP.

Question: In exercise 1, task 3, you configured a network policy that allowed members of the IT group to connect to A. Datum´s VPN server. Would you be able to connect if you had not created that policy?

> **Answer:** If you had not created the network policy for the IT group, no one would be able to connect. Two default policies exist, and they both deny access. If no policy exists on the Network Policy server, no one will be able to connect to the VPN server.

Question: In the troubleshooting exercise, you imported the AdatumCA Root certificate manually into the Trusted Root Certification Authority store on LON-CL1. Is it possible to automate this process?

> **Answer:** If the computer is a domain member, you could use Group Policy to distribute Root certificates. If the computer is a workgroup member, you could use a script or direct users to a web site from which they could download the root certificate.

Module 9

Implementing networking for branch offices

Contents:

Lesson 1

Networking features and considerations for branch offices

Contents:

Question and Answers

Question: Discuss several factors that can determine a suitable configuration for a branch office.

Answer:

- Security. Hosting services in a branch office can introduce potential security risks.
- Availability and reliability. The quality of a WAN link from the branch office to the head office or datacenter is usually the most significant factor that can affect availability and reliability.
- Performance and capacity. The key determiner for the location of a service or application might be performance and capacity requirements.
- Legal and regulatory requirements. Depending on the geographic and industry affiliations of your organization, legal restrictions or requirements for compliance with regulations can affect the location of services.
- IT organization. The IT resources to manage onsite infrastructure at head offices and branch offices are often different.
- Business considerations. The ownership structure of an organization can affect service placement.
- Cost. Centralizing server infrastructure typically results in greater cost savings.

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 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

Question: What types of DFS namespaces can be deployed in an organization? What type is more appropriate for your organization?

> **Answer:** You can create either a domain-based or standalone namespace. Each student might have a different choice depending on company infrastructure and requirements.

Question: What scenarios can be addressed with DFS functionality in Windows Server 2016?

> **Answer:** DFS can be implemented to provide the following efficiencies to different network file usage scenarios in branch offices:
>
> - Sharing files across branch offices.
> - Data collection from branch offices.
> - Data distribution to branch offices.

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 are not consistent with the data.

Planning for DFS

Question: You must use DFS to ensure that a file share hosted on a file server running Windows Server 2016 is replicated to another file server running Windows Server 2016 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:** Data Deduplication would work well with the data being replicated. However, if your organization still has Windows Server 2008 R2 servers, you cannot use Data Deduplication in this scenario, because it is not available in Windows Server 2008 R2.

Demonstration: Configuring DFS namespaces and replication

Demonstration Steps

Install the DFS Replication role service

1. On **LON-SVR1**, click **Start**, and then click **Server Manager**.
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 through 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. To close the **\\Adatum.com\Research Properties** dialog box, click **OK**.

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. To create the shared folder, in the **Warning** dialog box, click **Yes**.
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. To create the folder, in the **Warning** dialog box, click **Yes**.
8. To close the **New Folder** dialog box, click **OK**.
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 appears.

Create a new folder target for replication

1. In the **DFS Management** console, right-click the **Proposals** folder, and then click **Add Folder Target**.
2. In the **New Folder Target** dialog box, under **Path to folder target**, type **\\TOR-SVR1\Proposal_docs**, and then click **OK**.
3. To create the shared folder, in the **Warning** dialog box, click **Yes**.
4. In the **Create Share** dialog box, in the **Local path of shared folder** box, type **C:\Proposal_docs**.
5. 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**.
6. To create the folder, in the **Warning** dialog box, click **Yes**.
7. 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 replicates all data between all members of the replication group.

   If you have 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 later.
5. After reviewing all the selections, click **Next**.
6. On the **Replication Group Schedule and Bandwidth** page, allow the default selection of **Replicate continuously using the specified bandwidth**, and then configure the setting to use **Full bandwidth**. Note that you also can 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:

Question and Answers

Question: What modes can you configure for BranchCache?

Answer: You can configure BranchCache to use the hosted cache mode or distributed cache mode.

Question: What type of servers that use BranchCache are BranchCache-enabled content servers?

Answer: There are three types of servers that can act as BranchCache-enabled content servers:

- Web servers.
- File servers.
- Application servers.

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 **Start**, type **gpedit.msc**, and then press Enter.
2. In the **Local Group Policy Editor** window, expand **Computer Configuration**, expand **Administrative Templates**, expand **Network**, click **Lanman Server**, and then double-click **Hash Publication for BranchCache**.
3. In the **Hash Publication for BranchCache** dialog box, click **Enabled**.
4. 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**.
5. 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

Review Questions

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

Answer: DFSR 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. DFSR 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 or a newer operating system. However, it is likely that these computers or laptops might be shut down or removed from the office. This means that a cached file might not be available, which forces the system to download the file across the WAN link again. However, if the hosted cache mode is used, the computer running Windows Server 2016 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 B: Implementing BranchCache

Question and Answers

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 10

Configuring advanced networking features

Contents:

Lesson 1

Overview of high-performance networking features

Contents:

Question and Answers

Categorize Activity

Question: Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	This allows you to combine up to 32 network adapters and then use them as a single network interface.
2	This is a collection of technologies that allow you to meet the service requirements of a workload.
3	You can configure this through Device Manager or Windows PowerShell.
4	This configuration can be deployed with only one network adapter but does not offer fault tolerance.
5	This can help you to implement bandwidth management.
6	You can implement this by allocating a virtual machine's multiple cores through the advanced network.
7	To use this, the host must have at least two external virtual switches.
8	You can use this to prioritize traffic such as voice or video streaming.
9	To use this, you must configure a virtual machine to use multiple CPU cores.

Category 1		Category 2		Category 3
NIC Teaming		QoS		RSS

Answer:

Category 1		Category 2		Category 3
NIC Teaming		QoS		RSS
This allows you to combine up to 32 network adapters and then use them as a single network interface. This configuration can be deployed with only one network adapter but does not offer fault tolerance. To use this, the host must have at least two external virtual switches.		This is a collection of technologies that allow you to meet the service requirements of a workload. This can help you to implement bandwidth management. You can use this to prioritize traffic such as voice or video streaming.		You can configure this through Device Manager or Windows PowerShell. You can implement this by allocating a virtual machine's multiple cores through the advanced network. To use this, you must configure a virtual machine to use multiple CPU cores.

Resources

Implementing SMB 3.1.1 shared folders

Additional Reading: For more information, refer to Server Message Block Overview: http://aka.ms/obyww0

What is RSC?

Additional Reading: For more information on the preceding Windows PowerShell cmdlets, refer to "Network Adapter Cmdlets in Windows PowerShell" at: http://aka.ms/D40x84

Demonstration: Implementing NIC Teaming

Demonstration Steps

1. On **LON-HOST1**, if Server Manager is not started, click **Start**, and then click the **Server Manager** icon to start Server Manager.
2. In the **Server Manager** console tree, click the **Local Server** node.
3. In the **Properties details** pane, next to the **NIC Teaming** item, click the **Disabled** hyperlink.
4. In the **NIC Teaming** dialog box, in the **Adapters and Interfaces** pane, click **Ethernet 2**, and then in the **Tasks** list, select **Add to new team**.
5. In the **Add to new team** dialog box, in the **Team name** box, type **Host NIC Team**, and then click **OK**.
6. In the **NIC Teaming** dialog box, in the **Teams** pane, note the following details:
    a. Team: **Host NIC Team**
    b. Status: **OK**
    c. Teaming Mode: **Switch Independent**
    d. Load Balancing: **Dynamic**
    e. Adapters: **1**

Note: Explain that as previously mentioned, you have created a NIC team with only one adapter, which is not fault tolerant but allows for the separation of network traffic when you are also using VLANs.

Lesson 2

Configuring advanced Hyper-V networking features

Contents:

Question and Answers

Question: What is the ping-pong effect?

( ) The ping-pong effect occurs when multiple physical network adapters from the host are matched to several virtual network adapters. They continuously swap physical addresses.

( ) The ping-pong effect occurs when a virtual switch extension applies network forwarding. It bypasses the default forwarding, which causes network packets to loop back and forth to the router.

( ) The ping-pong effect results from a rare circumstance that can occur in dynamic VMQ when a CPU core is being used, and the processing happens to generates a large amount of inbound traffic. Because of this, another, less-busy CPU core is dynamically selected, and because the traffic load has not changed, it jumps back to the original or another CPU core. This process continues.

( ) When you use Remote Direct Memory Access (RDMA), a network adapter can switch repeatedly between Switch Embedded Teaming (SET) and RDMA functionality.

( ) The ping-pong effect occurs when a NIC team switches repeatedly among team member adapters.

Answer:

( ) The ping-pong effect occurs when multiple physical network adapters from the host are matched to several virtual network adapters. They continuously swap physical addresses.

( ) The ping-pong effect occurs when a virtual switch extension applies network forwarding. It bypasses the default forwarding, which causes network packets to loop back and forth to the router.

(√) The ping-pong effect results from a rare circumstance that can occur in dynamic VMQ when a CPU core is being used, and the processing happens to generates a large amount of inbound traffic. Because of this, another, less-busy CPU core is dynamically selected, and because the traffic load has not changed, it jumps back to the original or another CPU core. This process continues.

( ) When you use Remote Direct Memory Access (RDMA), a network adapter can switch repeatedly between Switch Embedded Teaming (SET) and RDMA functionality.

( ) The ping-pong effect occurs when a NIC team switches repeatedly among team member adapters.

Demonstration: Configuring network adapter advanced features

Demonstration Steps

Use Windows PowerShell to enable DHCP guarding

1. Ensure that you have performed the preparation steps.
2. On **LON-CL1**, In the notification area of the taskbar, right-click the **Network** icon, and then click **Open Network and Sharing Center**.
3. In the **Network and Sharing Center** window, click the **Ethernet** hyperlink.
4. In the **Ethernet Status** window, click **Details**. Note that it now has a **DHCP Server IP Address** of **172.16.0.10** (**LON-DC1**).
5. On **LON-HOST1**, click **Start**, and then click **Windows PowerShell**.
6. At the Windows PowerShell prompt, type the following commands to prevent **LON-DC1** from issuing a DHCP lease, and then press Enter after each line:

```
Set-VMNetworkAdapter -VMName 20741B-LON-DC1-B -DhcpGuard On
```

```
Set-VMNetworkAdapter -VMName 20741B-LON-SVR1-B -DhcpGuard Off
```

7. On **LON-CL1**, right-click **Start**, and then click **Command Prompt (Admin)**.
8. In the **Command Prompt** window, type the following commands, pressing Enter after each line:

```
IPConfig /release
IPConfig/renew
```

9. In the notification area of the taskbar, right-click the **Network** icon, and then click **Open Network and Sharing Center**.
10. In the **Network and Sharing Center** window, click the **Ethernet** hyperlink.
11. In the **Ethernet Status** window, click **Details**. Note that it now has a **DHCP Server IP Address** from **LON-SVR1**.

Turn off DHCP guarding (for the subsequent lab to work correctly)

- On the physical host computer, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Set-VMNetworkAdapter -VMName 20741B-LON-DC1-B -DhcpGuard Off
```

Revert the virtual machines

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

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20741B-LON-DC1-B**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741B-LON-SVR1-B** and **20741B-LON-CL1-B**.

Module Review and Takeaways

Best Practices

When implementing advanced networking features for Hyper-V, use the following best practices:

- Deploy multiple network adapters to a Hyper-V physical host, and then configure those adapters as part of a team. This helps to ensure that you will retain network connectivity if individual network adapters fail. Configure multiple teams with network adapters that are connected to different switches to help ensure that connectivity will remain if a hardware switch fails.
- Use bandwidth management to allocate a minimum and a maximum bandwidth allocation on a per–virtual network adapter basis. You should configure bandwidth allocation to help guarantee that each virtual machine will have a minimum bandwidth allocation. This helps to ensure that if another virtual machine that is physically hosted on the same Hyper-V server experiences a traffic spike, other virtual machines will be able to communicate normally with the network.
- Provision a Hyper-V physical host with an adapter that supports VMQ. VMQ uses hardware packet filtering to deliver network traffic directly to a virtual machine. This helps to improve performance because the packet does not need to be copied from the physical host operating system to the virtual machine. When you do not configure virtual machines to support VMQ, the physical host operating system can become a bottleneck when it processes large amounts of network traffic.
- If you are physical hosting large numbers of virtual machines and need to isolate them, use network virtualization rather than VLANs. Network virtualization is complicated to configure, but it has an advantage over VLAN—it is not necessary to configure VLANs on all the switches that are connected to the Hyper-V physical host. You can perform all the necessary configurations when you need to isolate servers on a Hyper-V physical host without needing to involve the network team.

Review Question

Question: You want to deploy a Windows Server 2016 Hyper-V virtual machine's virtual hard disk on a file share. What operating system must the file server be running to support this configuration?

> **Answer:** You can deploy virtual hard disks only to file shares that support at least SMB 3.0, and only the Windows Server 2012 and Windows Server 2016 operating systems support the physical hosting of SMB 3.0 and SMB 3.1.1 file shares.

Lab Review Questions and Answers

Lab: Configuring advanced Hyper-V networking features

Question and Answers

Question: In the "NIC Teaming" task, you created **LON-SVR1 NIC Team** on the Ethernet 2 network adapter. Is this fault tolerant?

Answer: No, it is not. Although you can create a NIC team with only one network adapter, this lets you provide network isolation but not fault tolerance.

Question: In the task named "Create virtual network adapters in the parent partition," you had to shut down the **LON-SVR1** virtual machine. Why?

Answer: You were adding hardware—specifically, a network adapter. You cannot do this while a virtual machine is running.

Module 11

Implementing Software Defined Networking

Contents:

Lesson 1

Overview of SDN

Contents:

Question and Answers

Question: In SDN, each physical compute host must be assigned at least one IP address from the Management logical network. You can use Dynamic Host Configuration Protocol (DHCP) for this assignment.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

In SDN, each physical compute host must be assigned at least one IP address from the Management logical network. You can use DHCP for this assignment.

Question: Does the complexity of your organization's network infrastructure suggest the need for SDN?

Answer: Answers will vary based on students' experiences and their organizations' network infrastructures.

Lesson 2

Implementing network virtualization

Contents:

Question and Answers

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

> **Answer:** When you move a virtual machine, its CA stays the same. The only thing that changes is its PA, 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.

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

> **Answer:** Network virtualization policies define the Hyper-V host on which 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.

Lesson 3

Implementing Network Controller

Contents:

Question and Answers

Question: What does Network Controller use the Northbound and Southbound APIs for?

Answer: Network Controller uses the Southbound API to communicate with network devices, services, and components. With the Southbound API, Network Controller can:

- Discover network devices.
- Detect service configurations.
- Gather all the information that you need about the network.
- Send information to the network infrastructure; for example, configuration changes that you have made.

The Network Controller Northbound API enables you to configure, monitor, troubleshoot, and deploy new devices on a network by using:

- Windows PowerShell.
- Representational state transfer (REST) API.
- A management application with a GUI; for example, Virtual Machine Manager.

Resources

The procedure for deploying Network Controller

 **Additional Reading:** For more information on the syntax of these cmdlets, refer to: http://aka.ms/Jforwt

 **Additional Reading:** For more information on the syntax of this cmdlet, refer to: http://aka.ms/Yv09r3

Software Load Balancing

 **Additional Reading:** You also can use Windows PowerShell cmdlets. For more information on the Windows PowerShell cmdlets that you can use to manage Network Controller, refer to: http://aka.ms/Q9ih9a

Demonstration: Preparing to deploy Network Controller

Demonstration Steps

Create Active Directory Domain Services (AD DS) security groups

1. Switch to **LON-DC1**.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In **Active Directory Users and Computers**, expand **Adatum.com**, and then click **IT**.
4. Right-click **IT**, click **New**, and then click **Group**.
5. In the **New Object – Group** dialog box, in the **Group name** text box, type **Network Controller Admins**, and then click **OK**.
6. In the details pane, double-click **Network Controller Admins**, and then in the **Network Controller Admins Properties** dialog box, on the **Members** tab, click **Add**.
7. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **administrator; Beth**, and then click **OK** twice.

8. Right-click **IT**, click **New**, and then click **Group**.
9. In the **New Object – Group** dialog box, in the **Group name** text box, type **Network Controller Ops**, and then click **OK**.
10. In the details pane, double-click **Network Controller Ops**, and then in the **Network Controller Ops Properties** dialog box, on the **Members** tab, click **Add**.
11. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **administrator; Beth**, and then click **OK** twice.
12. Close **Active Directory Users and Computers**.

Request a certificate

1. Switch to **LON-SVR2**, right-click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc.exe**, and then press Enter.
3. In the **Console1 – [Console Root]** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, in the **Snap-in** list, double-click **Certificates**.
5. Click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
6. In the navigation pane, expand **Certificates (Local Computer)**, and then click **Personal**.
7. Right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
8. In the **Certificate Enrollment** dialog box, on the **Before you Begin** page, click **Next**.
9. On the **Select Certificate Enrollment Policy** page, click **Next**.
10. Select the **Computer** check box, click **Enroll**, and then click **Finish**.
11. Close the management console, and do not save the changes.

Demonstration: Deploying Network Controller

Demonstration Steps

Add the Network Controller role

1. On **LON-SVR2**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, in the details pane, click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, on the **Before you begin** page, 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, in the **Roles** list, select the **Network Controller** check box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Network Controller** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. When the role installs, click **Close**.
11. Right-click **Start**, point to **Shut down or sign out**, and then click **Restart**.
12. In the **Choose a reason that best describes why you want to shut down this computer** dialog box, click **Continue**.

13. After **LON-SVR2** restarts, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

Configure the Network Controller cluster

1. On **LON-SVR2**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$node=New-NetworkControllerNodeObject -Name "Node1" -Server "LON-SVR2.Adatum.com" -
FaultDomain "fd:/rack1/host1" -RestInterface “London_Network”
```

3. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$Certificate = Get-Item Cert:\LocalMachine\My | Get-ChildItem | where {$_.Subject -
imatch "LON-SVR2" }
```

4. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
Install-NetworkControllerCluster -Node $node -ClusterAuthentication Kerberos -
ManagementSecurityGroup "Adatum\Network Controller Admins" -
CredentialEncryptionCertificate $Certificate
```

Configure the Network Controller application

- At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
Install-NetworkController -Node $node -ClientAuthentication Kerberos -
ClientSecurityGroup "Adatum\Network Controller Ops" -RestIpAddress "172.16.0.99/24" -
ServerCertificate $Certificate
```

Validate the deployment

1. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
```

2. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$cred.type="usernamepassword"
```

3. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$cred.username="admin"
```

4. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
$cred.value="abcd"
```

5. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
New-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
Properties $cred –ResourceId cred1
```

6. Press **Y**, and then press Enter when prompted.
7. At the Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
Get-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
ResourceId cred1
```

Module Review and Takeaways

Review Questions

Question: You decide to deploy Network Controller in your AD DS domain environment. What steps must you take to prepare for the deployment?

Answer: The deployment requirements in a domain environment are as follows:

- You can only deploy Network Controller on Windows Server 2016 Datacenter edition.
- The management client that you use must be installed on a computer or virtual machine that is running Windows 10, Windows 8.1, or Windows 8.
- You must configure dynamic Domain Name System (DNS) registration to enable registration of required DNS records for Network Controller.
- If the computers or virtual machines that are running Network Controller or the management client for Network Controller are joined to a domain, you must:
  - Create a security group that holds all the users who have permission to configure Network Controller.
  - Create a security group that holds all of the users who have permission to configure and manage the network by using Network Controller.

Question: What are the reasons to consider implementing SDN with Windows Server 2016?

Answer: SDN provides network resources that are:

- Flexible. You can move traffic from your on-premises infrastructure to your private or public cloud infrastructure.
- Efficient. You can abstract the hardware components of your network infrastructure with software components.
- Scalable. Your on-premises infrastructure has a finite capacity. Your cloud-based infrastructure has far broader limits, enabling you to scale up your infrastructure when necessary.

Question: How do you install the Network Controller feature in Windows Server 2016 by using Windows PowerShell?

Answer: To deploy Network Controller with Windows PowerShell, install the feature by running the following cmdlet:

Install-WindowsFeature -Name NetworkController –IncludeManagementTools

Lab Review Questions and Answers

Lab: Deploying Network Controller

Question and Answers

Question: In the lab, you used Windows PowerShell to manage Network Controller. What other tools could you use?

Answer: You could also use Virtual Machine Manager and third-party management tools to manage Network Controller.

Question: In the lab, you deployed Network Controller in a domain environment. In a non-domain environment, what steps must you take to provide authentication?

Answer: In a non-domain environment, certificates provide authentication. You must configure certificate-based authentication by:

- Creating a certificate for use on the management client. The Network Controller must trust this certificate.
- Creating a certificate on the Network Controller for computer authentication.