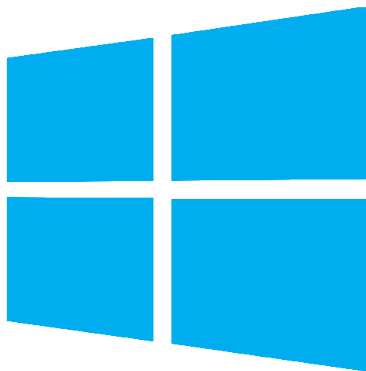




OFFICIAL MICROSOFT LEARNING PRODUCT

20741A

Networking with Windows Server 2016



Windows  
Server

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2016 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/trademarks> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Product Number: 20741A

Part Number: X21-15012

Released: 09/2016

## **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 that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code 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](http://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 des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, 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

# Welcome!

Thank you for taking our training! We've worked together with our Microsoft Certified Partners for Learning Solutions and our Microsoft IT Academies to bring you a world-class learning experience—whether you're a professional looking to advance your skills or a student preparing for a career in IT.

- **Microsoft Certified Trainers and Instructors**—Your instructor is a technical and instructional expert who meets ongoing certification requirements. And, if instructors are delivering training at one of our Certified Partners for Learning Solutions, they are also evaluated throughout the year by students and by Microsoft.
- **Certification Exam Benefits**—After training, consider taking a Microsoft Certification exam. Microsoft Certifications validate your skills on Microsoft technologies and can help differentiate you when finding a job or boosting your career. In fact, independent research by IDC concluded that 75% of managers believe certifications are important to team performance<sup>1</sup>. Ask your instructor about Microsoft Certification exam promotions and discounts that may be available to you.
- **Customer Satisfaction Guarantee**—Our Certified Partners for Learning Solutions offer a satisfaction guarantee and we hold them accountable for it. At the end of class, please complete an evaluation of today's experience. We value your feedback!

We wish you a great learning experience and ongoing success in your career!

Sincerely,

Microsoft Learning  
[www.microsoft.com/learning](http://www.microsoft.com/learning)

**Microsoft** | Learning

<sup>1</sup> IDC, Value of Certification: Team Certification and Organizational Performance, November 2006

## Acknowledgments

Microsoft Learning would like to acknowledge and thank the following for their contributions towards developing this title. Their effort at various stages of development has ensured that you have a good classroom experience.

### **Michael Buchardt: Content Developer**

Michael Buchardt is an independent consultant and trainer based in Copenhagen, Denmark. He has extensive experience consulting for some of the largest companies and institutions in Denmark about Microsoft System Center Configuration Manager, Active Directory, and infrastructure and virtualization. Michael is a highly experienced trainer and has been an active Microsoft Certified Trainer (MCT) since 2001. He has taught more than 300 Microsoft Official Courses (MOCs), and holds certifications on every Windows operating system since Windows 2000. He worked for various training centers and consulting firms before starting his own company, Mimercon, in 2012, through which he offers consulting and freelance training.

### **Gary Dunlop: Content Developer**

Gary Dunlop, who is based in Winnipeg, Canada, is a technical consultant and trainer for Broadview Networks. He has authored a number of Microsoft Learning titles and has been an MCT since 1997.

### **David Franklyn: Content Developer**

David M. Franklyn is a Microsoft Certified Solutions Expert (MCSE), Microsoft Certified IT Professional (MCITP), Microsoft Most Valuable Professional (MVP) for Windows and Devices for IT, and also is an Eastern Regional Lead MCT for the United States. Dave has been a Microsoft MVP since 2011, and a Senior Information Technology Trainer and Consultant at Auburn University in Montgomery Alabama, since 1998. He is the owner of DaveMCT, Inc. LLC, and is a training partner with Dunn Training. Dave has worked with computers since 1976, starting out in the mainframe world, and then moving early into the networking arena. Before joining Auburn University, Dave spent 22 years in the United States Air Force as an electronic communications and computer systems specialist, retiring in 1998. Dave is president of the Montgomery Windows IT Professional Group, and is a guest speaker at many events involving Microsoft products.

### **Conan Kezema: Technical Reviewer**

Conan Kezema, B. Ed, is an MCSE and MCT, as well as an educator, consultant, network systems architect, and author who specializes in Microsoft technologies. As an associate of S.R. Technical Services, Conan has been a subject matter expert (SME), instructional designer, and author on numerous Microsoft courseware-development projects.

### **Clifton Leonard: Content Developer**

Clifton Leonard is a content developer and SME with more than 25 years of experience in the IT industry as an engineer, architect, consultant, trainer, and author. Clifton has extensive experience consulting on Active Directory, Microsoft Exchange Server, Microsoft Lync Server, identity management, and Microsoft Office 365. His clients include large energy corporations, elementary through high school, universities, technology manufacturers, financial institutions, the United States Air Force, and the United States Department of Defense. Clifton has been a SME for multiple courses on Windows Desktop, Windows Server, Exchange Server, Microsoft SharePoint Server, Microsoft Hyper-V, identity management, and Office 365.

**Vladimir Meloski: Content Developer**

Vladimir Meloski, an MCT and Microsoft MVP on Microsoft Office Servers and Services, is a consultant who provides solutions for unified communications and infrastructures based on Microsoft Exchange Server, Skype for Business, Office 365, and Windows Server. Vladimir has 20 years of professional IT experience, and has been involved in Microsoft conferences in Europe and the United States as a speaker, moderator, proctor for hands-on labs, and as a technical expert. He also has been involved as a SME and technical reviewer for MOC courses about Exchange Server, Office 365, and Windows Server.

**David Susemihl: Content Developer**

David Susemihl has worked as consultant, trainer, and courseware developer since 1996. David has extensive experience consulting on Microsoft Systems Management Server, System Center Configuration Manager 2007, Active Directory, Exchange Server, and Terminal Server/Citrix deployments. David has developed courseware development for Microsoft and Hewlett-Packard, and has delivered those courses successfully in Europe, Central America, and across North America. For the last several years, David has been writing courseware for Microsoft Learning, and consulting on infrastructure transitions in Michigan.

**Andrew J. Warren: Content Developer**

Andrew Warren has more than 25 years of experience in the IT industry, many of which he has spent teaching and writing. He has been involved as a SME for many of the Windows Server 2012 courses, and as the technical lead for several Windows 8 and Windows 8.1 courses. He also has been involved in developing TechNet sessions on Microsoft Exchange Server. Andrew is based in the United Kingdom, where he runs his own IT training and education consultancy.

# Contents

<b>Module 1: Planning and implementing an IPv4 network</b>	
Module Overview	1-1
<b>Lesson 1:</b> Planning IPv4 addressing	1-2
<b>Lab A:</b> Planning an IPv4 network	1-12
<b>Lesson 2:</b> Configuring an IPv4 host	1-15
<b>Lesson 3:</b> Managing and troubleshooting IPv4 network connectivity	1-20
<b>Lab B:</b> Implementing and troubleshooting an IPv4 network	1-31
Module Review and Takeaways	1-34
<b>Module 2: Implementing DHCP</b>	
Module Overview	2-1
<b>Lesson 1:</b> Overview of the DHCP server role	2-2
<b>Lesson 2:</b> Deploying DHCP	2-6
<b>Lesson 3:</b> Managing and troubleshooting DHCP	2-15
<b>Lab:</b> Implementing DHCP	2-27
Module Review and Takeaways	2-35
<b>Module 3: Implementing IPv6</b>	
Module Overview	3-1
<b>Lesson 1:</b> Overview of IPv6 addressing	3-2
<b>Lesson 2:</b> Configuring an IPv6 host	3-13
<b>Lesson 3:</b> Implementing IPv6 and IPv4 coexistence	3-22
<b>Lesson 4:</b> Transitioning from IPv4 to IPv6	3-26
<b>Lab:</b> Configuring and evaluating IPv6 transition technologies	3-32
Module Review and Takeaways	3-43
<b>Module 4: Implementing DNS</b>	
Module Overview	4-1
<b>Lesson 1:</b> Implementing DNS servers	4-2
<b>Lesson 2:</b> Configuring zones in DNS	4-21
<b>Lesson 3:</b> Configuring name resolution between DNS zones	4-27
<b>Lab A:</b> Planning and implementing name resolution by using DNS	4-33
<b>Lesson 4:</b> Configuring DNS integration with AD DS	4-37
<b>Lab B:</b> Integrating DNS with AD DS	4-44
<b>Lesson 5:</b> Configuring advanced DNS settings	4-46
<b>Lab C:</b> Configuring advanced DNS settings	4-62
Module Review and Takeaways	4-67

<b>Module 5: Implementing and managing IPAM</b>	
Module Overview	5-1
<b>Lesson 1:</b> Overview of IPAM	5-2
<b>Lesson 2:</b> Deploying IPAM	5-7
<b>Lesson 3:</b> Managing IP address spaces by using IPAM	5-16
<b>Lab:</b> Implementing IPAM	5-23
Module Review and Takeaways	5-28
<b>Module 6: Remote access in Windows Server 2016</b>	
Module Overview	6-1
<b>Lesson 1:</b> Overview of remote access	6-2
<b>Lesson 2:</b> Implementing Web Application Proxy	6-13
<b>Lab:</b> Implementing Web Application Proxy	6-18
Module Review and Takeaways	6-25
<b>Module 7: Implementing DirectAccess</b>	
Module Overview	7-1
<b>Lesson 1:</b> Overview of DirectAccess	7-2
<b>Lesson 2:</b> Implementing DirectAccess by using the Getting Started Wizard	7-13
<b>Lab A:</b> Implementing DirectAccess by using the Getting Started Wizard	7-20
<b>Lesson 3:</b> Implementing and managing an advanced DirectAccess infrastructure	7-27
<b>Lab B:</b> Deploying an advanced DirectAccess solution	7-44
Module Review and Takeaways	7-55
<b>Module 8: Implementing VPNs</b>	
Module Overview	8-1
<b>Lesson 1:</b> Planning VPNs	8-2
<b>Lesson 2:</b> Implementing VPNs	8-12
<b>Lab:</b> Implementing VPN	8-20
Module Review and Takeaways	8-30
<b>Module 9: Implementing networking for branch offices</b>	
Module Overview	9-1
<b>Lesson 1:</b> Networking features and considerations for branch offices	9-2
<b>Lesson 2:</b> Implementing DFS for branch offices	9-12
<b>Lab A:</b> Implementing DFS for branch offices	9-25
<b>Lesson 3:</b> Implementing BranchCache for branch offices	9-28
<b>Lab B:</b> Implementing BranchCache	9-37
Module Review and Takeaways	9-42

<b>Module 10: Configuring advanced networking features</b>	
Module Overview	<b>10-1</b>
<b>Lesson 1:</b> Overview of high-performance networking features	<b>10-2</b>
<b>Lesson 2:</b> Configuring advanced Hyper-V networking features	<b>10-12</b>
<b>Lab:</b> Configuring advanced Hyper-V networking features	<b>10-23</b>
Module Review and Takeaways	<b>10-28</b>
<b>Module 11: Implementing Software Defined Networking</b>	
Module Overview	<b>11-1</b>
<b>Lesson 1:</b> Overview of Software Defined Networking	<b>11-2</b>
<b>Lesson 2:</b> Implementing network virtualization	<b>11-11</b>
<b>Lesson 3:</b> Implementing Network Controller	<b>11-16</b>
<b>Lab:</b> Deploying Network Controller	<b>11-28</b>
Module Review and Takeaways	<b>11-32</b>
<b>Lab Answer Keys</b>	
<b>Module 1 Lab A:</b> Planning an IPv4 network	<b>L1-1</b>
<b>Module 1 Lab B:</b> Implementing and troubleshooting an IPv4 network	<b>L1-3</b>
<b>Module 2 Lab:</b> Implementing DHCP	<b>L2-7</b>
<b>Module 3 Lab:</b> Configuring and evaluating IPv6 transition technologies	<b>L3-17</b>
<b>Module 4 Lab A:</b> Planning and implementing name resolution by using DNS	<b>L4-27</b>
<b>Module 4 Lab B:</b> Integrating DNS with AD DS	<b>L4-30</b>
<b>Module 4 Lab C:</b> Configuring advanced DNS settings	<b>L4-33</b>
<b>Module 5 Lab:</b> Implementing IPAM	<b>L5-39</b>
<b>Module 6 Lab:</b> Implementing Web Application Proxy	<b>L6-45</b>
<b>Module 7 Lab A:</b> Implementing DirectAccess by using the Getting Started Wizard	<b>L7-55</b>
<b>Module 7 Lab B:</b> Deploying an advanced DirectAccess solution	<b>L7-62</b>
<b>Module 8 Lab:</b> Implementing VPN	<b>L8-77</b>
<b>Module 9 Lab A:</b> Implementing DFS for branch offices	<b>L9-78</b>
<b>Module 9 Lab B:</b> Implementing BranchCache	<b>L9-90</b>
<b>Module 10 Lab:</b> Configuring advanced Hyper-V networking features	<b>L10-97</b>
<b>Module 11 Lab:</b> Deploying Network Controller	<b>L11-103</b>



## About This Course

This section provides a brief description of your course, including the audience, suggested prerequisites, and course objectives.

### Course Description

This course provides you with the fundamental networking skills that you require to deploy and support Windows Server 2016 in most organizations. It covers IP fundamentals, remote-access technologies, and more advanced content, including software-defined networking.

### Audience

This course is for existing information technology (IT) professionals who have some networking knowledge and experience, and are looking for a single course that provides insight into core and advanced networking technologies in Windows Server 2016. This audience typically includes:

- Network administrators who are looking to reinforce existing skills and learn about new networking technology changes and functionality in Windows Server 2016.
- System or Infrastructure Administrators who have a general networking knowledge and who are looking to gain core and advanced networking knowledge and skills on Windows Server 2016.

### Student Prerequisites

In addition to their professional experience, students who attend this training should have the following technical knowledge:

- Experience working with Windows Server 2008 or Windows Server 2012.
- Experience working in a Windows Server infrastructure enterprise environment.
- Knowledge of the Open Systems Interconnection (OSI) model.
- Understanding of core networking-infrastructure components and technologies, such as cabling, routers, hubs, and switches.
- Familiarity with networking topologies and architectures, such as local area networks (LANs), wide area networks (WANs), and wireless networking.
- Some basic knowledge of the TCP/IP protocol stack, addressing, and name resolution.
- Experience with, and knowledge of, Microsoft Hyper-V and virtualization.
- Hands-on experience working with the Windows client operating systems, such as Windows 8.1 or Windows 10.

### Course Objectives

After completing this course, students will be able to:

- Plan and implement an IPv4 network.
- Implement Dynamic Host Configuration Protocol (DHCP).
- Implement IPv6.
- Implement Domain Name System (DNS).
- Implement and manage IP address management (IPAM).
- Plan for remote access.
- Implement DirectAccess.

- Implement virtual private networks (VPNs).
- Implement networking for branch offices.
- Configure advanced networking features.
- Implement software-defined networking.

## Course Outline

The course outline is as follows:

- Module 1, "Planning and implementing an IPv4 network" explains how to plan and implement an IPv4 addressing scheme to support organizational needs. This module also explains how to use fundamental networking tools and techniques to configure and troubleshoot IPv4-based networks.
- Module 2, "Implementing DHCP" explains how to plan and implement DHCP to support the IPv4 infrastructure.
- Module 3, "Implementing IPv6" explains how to implement IPv6, and how to integrate IPv6 and IPv4 networks.
- Module 4, "Implementing DNS" explains how to install, configure, and troubleshoot DNS within the organization's network.
- Module 5, "Implementing and managing IPAM" explains how to implement and manage the IPAM feature in Windows Server 2016. This module also explains how to use IPAM to manage services such as DHCP and DNS.
- Module 6, "Remote access in Windows Server 2016" explains how to plan for remote access in Windows Server 2016 and how to implement Web Application Proxy.
- Module 7, "Implementing DirectAccess" explains how to implement and manage DirectAccess in Windows Server 2016.
- Module 8, "Implementing VPNs" explains how to implement and manage remote access in Windows Server 2016 by using VPNs.
- Module 9, "Implementing networking for branch offices" explains how to implement network services for branch offices.
- Module 10, "Configuring advanced networking features" explains how to explain how to implement an advanced networking infrastructure.
- Module 11, "Implementing Software Defined Networking" explains how to implement software-defined networking.

## Course Materials

Your kit includes the following materials:

- **Course Handbook:** This is a succinct classroom-learning guide that provides critical technical information in a crisp, tightly focused format, which is essential for an effective in-class learning experience. The course handbook sections include:
- **Lessons:** These guide you through learning objectives, and provide key points that are critical to the success of your in-class learning experience.
- **Labs:** These provide a real-world, hands-on platform on which you can apply the knowledge and skills that you learn in the module.
- **Module Reviews and Takeaways:** These provide on-the-job reference material to boost knowledge and skills retention.
- **Lab Answer Keys:** These provide step-by-step guidance for the labs.



**Additional Reading: Course Companion Content on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> Site:** This site provides searchable, easy-to-browse digital content with integrated premium online resources that supplement the Course Handbook.

- **Modules:** These include companion content for each lesson, including questions and answers, detailed demonstration steps, and additional reading links. Additionally, modules include Lab Review questions and answers, and Module Reviews and Takeaways sections, which contain the review questions and answers, best practices, common issues and troubleshooting tips with answers, and real-world issues and scenarios with answers.
- **Resources:** These include well-categorized additional resources that give you immediate access to the most current premium content on TechNet, Microsoft Developer Network (MSDN), and Microsoft Press.
- **Course evaluation:** At the end of the course, you will have the opportunity to complete an online evaluation in which you can provide feedback on the course, training facility, and instructor. Additionally:
  - To provide additional comments or feedback on the course, go to [mcspprt@microsoft.com](mailto:mcspprt@microsoft.com). To inquire about the Microsoft Certification Program, send an email to [mcphep@microsoft.com](mailto:mcphep@microsoft.com).

## Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the course's business scenario.

### Virtual Machine Configuration

In this course, you will use Microsoft Hyper-V to perform the labs.



**Note:** At the end of each lab, you must revert the virtual machines to a snapshot. You can find the instructions for this procedure at the end of each lab.

The following table details the role of each virtual machine that this course uses.

Virtual machine	Role
20741A-LON-DC1	Domain controller running Windows Server 2016 in the Adatum.com domain
20741A-LON-SVR1	Windows Server 2016 server in the Adatum.com domain
20741A-LON-SVR2	Windows Server 2016 server in the Adatum.com domain
20741A-TOR-SVR1	Windows Server 2016 server in the Adatum.com domain located in Toronto office
20741A-SYD-SVR1	Windows Server 2016 server in the Adatum.com domain located in Sydney office
20741A-INET1	Windows Server 2016 server providing simulated Internet access (running DHCP, DNS, and Web services)
20741A-EU-RTR	Standalone Windows Server used for router.
20741A-NA-RTR	Standalone Windows Server used for router.
20741A-LON-CL1	Client computer running Windows 10 and Office 2016 in the Adatum.com domain
20741A-LON-CL2	Client computer running Windows 10 and Office 2016 in the Adatum.com domain

### Software Configuration

The following software is installed on each host machine:

- Windows Server 2012 with the Hyper-V feature

The following software is installed on each virtual machine:

- Windows Server 2016 or Windows 10 Enterprise
- Microsoft Office 2016 on client virtual machines

## Classroom Setup

Each classroom computer has the same virtual machine and configuration.

## Course Hardware Level

To ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Learning Partner classrooms in which Official Microsoft Learning Product courseware is taught. This minimum configuration includes:

- Hardware Level 7
- Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V) processor
- Dual 500-gigabyte (GB) hard disks 7200 RPM Serial ATA (SATA) or better
- 16 GB of random access memory (RAM)
- DVD drive (dual layer recommended)
- Network adapter
- Dual Super VGA (SVGA) 17-inch monitors
- Microsoft mouse or compatible pointing device
- Sound card with amplified speakers

Additionally, the instructor's computer must be connected to a projection display device that supports SVGA 1024×768 pixels, 16-bit colors.

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 1

## Planning and implementing an IPv4 network

### Contents:

Module Overview	1-1
Lesson 1: Planning IPv4 addressing	1-2
Lab A: Planning an IPv4 network	1-12
Lesson 2: Configuring an IPv4 host	1-15
Lesson 3: Managing and troubleshooting IPv4 network connectivity	1-20
Lab B: Implementing and troubleshooting an IPv4 network	1-31
Module Review and Takeaways	1-34

## Module Overview

IPv4 is the network protocol used on the Internet and local area networks (LANs). To ensure that you can understand and troubleshoot network communication, it is essential that you understand how IPv4 is implemented. In this module, you will learn how to plan an IPv4 addressing scheme, in addition you will learn how to implement an IPv4 addressing scheme, and determine and troubleshoot network-related problems.

### Objectives

After completing this module, you will be able to:

- Plan IPv4 addressing.
- Configure an IPv4 host.
- Manage and troubleshoot IPv4 network connectivity.

## Lesson 1

# Planning IPv4 addressing

Understanding IPv4 network communication is critical to ensuring that you can implement, troubleshoot, and maintain IPv4 networks. One of the core components of IPv4 is addressing. By understanding addressing, subnet masks, and default gateways, you can identify proper communication between hosts. To identify IPv4 communication errors, you need to understand how the communication process is designed to work.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe IPv4 settings.
- Define IPv4 subnets.
- Identify public, private, and APIPA IPv4 addresses.
- Explain how to determine IPv4 notation and translation.
- Describe how to create a subnetting scheme for a new office.
- Describe how to create IPv4 supernets.

### Overview of IPv4 settings

To configure network connectivity, you must be familiar with IPv4 addresses and how they work. Network communication for a computer is directed to the IPv4 address of that computer. Therefore, each networked computer must be assigned a unique IPv4 address.

Each IPv4 address is 32 bits long, where a bit is the smallest unit of measurement in binary math, represented by either a 1 or a 0. To make IP addresses more readable, they are displayed in dotted decimal notation. Dotted decimal notation divides a 32-bit IPv4 address into four groups of 8 bits, which are converted to a decimal number between zero and 255. A decimal point separates the decimal numbers. Each decimal number is called an *octet*. For example, a 32-bit address of 10101100.00010000.00000000.00001010 could be difficult to read. This IP address is represented in dotted decimal as: 172.16.0.10.

**Dotted decimal notations are based on the decimal number system, but computers use IP addresses in binary**

Within an 8-bit octet, each bit position has a decimal value:

- A bit that is set to 0 always has a zero value
- A bit that is set to 1 can be converted to a decimal value
- The low-order bit represents a decimal value of 1
- The high-order bit represents a decimal value of 128

If all bits in an octet are set to 1, then the octet's decimal value is 255, the highest possible value of an octet:

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$$



### How a dotted decimal notation relates to binary numbers

When you assign IP addresses, you use a dotted decimal notation. Dotted decimal notations are based on the decimal number system. However, in the background, computers use IP addresses in binary. To properly design an IPv4 addressing scheme for complex networks, you must understand IP addresses in binary.

Within an 8-bit octet, each bit position has a decimal value. A bit that is set to 0 always has a zero value. A bit that is set to 1 can be converted to a decimal value. The low order bit is the rightmost bit in the octet, and it represents a decimal value of 1. The high order bit is the leftmost bit in the octet, and it represents



a decimal value of 128. If all bits in an octet are set to 1, then the octet's decimal value is 255, that is:  $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$ . 255 is the highest possible value of an octet.

Most of the time, you can use a calculator to convert decimal numbers to binary and vice versa. The Windows operating systems include the Calculator app that can perform decimal-to-binary conversions, as shown in the following example.

Binary	Bit Values	Decimal Value
10000011	$128+0+0+0+0+0+0+2+1$	131
01101011	$0+64+32+0+8+0+2+1$	107
00000011	$0+0+0+0+0+0+2+1$	3
00011000	$0+0+0+16+8+0+0+0$	24

Binary	Dotted decimal notation
10000011 01101011 00000011 00011000	131.107.3.24

### Subnet mask

Each IPv4 address is composed of a network identification (ID) and a host ID. The *network ID* identifies the network on which the computer is located. The *host ID* uniquely identifies the computer on that specific network. A *subnet mask* identifies which part of an IPv4 address is the network ID and which part is the host ID.

In the simplest scenarios, each octet in a subnet mask is either 255 or 0. A 255 represents an octet that is part of the network ID, while a 0 represents an octet that is part of the host ID. For example, a computer with an IP address of 172.16.0.10 and a subnet mask of 255.255.0.0 has a network ID of 172.16.0.0 and a host ID of 0.0.0.10.

You can present subnet masks in the *Classless Interdomain Routing* (CIDR) format, which represents how many continuous binary numbers with the value of 1 are contained in the subnet mask. For example, the network 172.16.0.0 that has the subnet mask 255.255.0.0 can be presented as 172.16.0.0/16. The /16 represents the 16 bits that have a value of 1 when the subnet mask is represented in a binary format: 11111111.11111111.00000000.00000000. The following table represents the default subnet masks and their network prefix notation.

### Default subnet masks (network prefix notation)

Address class		Bits for subnet mask	Network prefix
Class A	255.0.0.0	11111111 00000000 00000000 00000000	/8
Class B	255.255.0.0	11111111 11111111 00000000 00000000	/16
Class C	255.255.255.0	11111111 11111111 11111111 00000000	/24



**Note:** The terms *network*, *subnet*, and *virtual local area network* (VLAN) are often used interchangeably. A large network is often subdivided into subnets, and VLANs are configured on routers or on Layer 3 switches to represent subnets.



**Note:** The Internet Assigned Numbers Authority (IANA) is responsible for managing the public use of IPv4 addresses. The IANA is a department of the Internet Corporation for Assigned Names and Numbers (ICANN), which is an international nonprofit organization.

### Default gateway

A *default gateway* is a device, usually a router, on a Transmission Control Protocol/Internet Protocol (TCP/IP) network that forwards IP packets to other networks. The multiple internal networks in an organization can be referred to as an *intranet*.

On an intranet, any given network might have several routers that connect it to other networks, both local and remote. You must configure one of the routers as the default gateway for local hosts. This enables the local hosts to communicate with hosts on remote networks.

Before a host sends an IPv4 packet, it uses its own subnet mask to determine whether the destination host is on the same network or on a remote network. If the destination host is on the same network, the sending host transmits the packet directly to the destination host. If the destination host is on a different network, the host transmits the packet to a router for delivery.

When a host transmits a packet to a remote network, IPv4 consults the internal routing table to determine the appropriate router for the packet to reach the destination subnet. If the routing table does not contain any routing information about the destination subnet, IPv4 forwards the packet to the default gateway. The host assumes that the default gateway contains the required routing information. The default gateway is used in most cases.

Client computers usually obtain their IP addressing information from a Dynamic Host Configuration Protocol (DHCP) server. This is more straightforward than assigning a default gateway manually on each host. Most servers have a static IP configuration that is assigned manually.

**Question:** Convert the following values

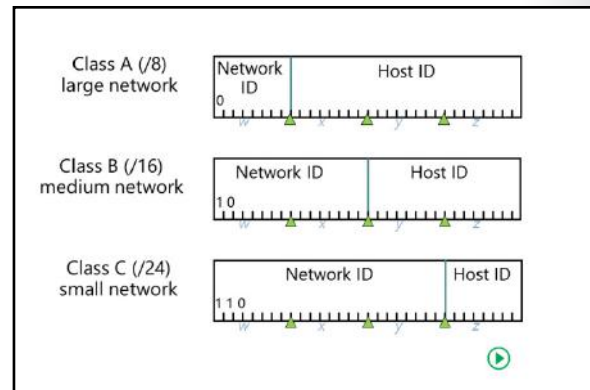
Binary	Dotted decimal notation
00001010 00001110 00011011 00100000	
	172.16.34.22
	192.168.87.19
10101100 00010000 01100010 00010111	
11000000 10101000 01010111 00111000	
	10.17.22.99

## Defining subnets

### IPv4 address classes

The IANA organizes IPv4 addresses into classes. Each class of address has a different default subnet mask that defines the number of valid hosts on the network. IANA has named the IPv4 address classes from *Class A* through *Class E*.

Classes A, B, and C are IP networks that you can assign to IP addresses on host computers. Computers and programs use Class D addresses for multicasting. The IANA reserves Class E for experimental use. An addressing process that uses an A, B, or C class is called *classful addressing*. A network that uses an A, B, or C class is called a *classful network*.



The following table lists the characteristics of each IP address class.

Class	First octet	Default subnet mask	Number of networks	Number of hosts per network
A	1-127	255.0.0.0	126	16,777,214
B	128-191	255.255.0.0	16,384	65,534
C	192-223	255.255.255.0	2,097,152	254

**Note:** Each octet can have a decimal value between 0 and 255, or 256 possible values. So why does a Class C network only have 254 usable addresses? The first address, where all bits are 0, in the host's portion of an IP is the subnet ID. The last address, where all bits are 1, is used for broadcasts such as a request to find the physical address associated with a particular IP address. As defined in RFC 923 (<http://aka.ms/Yhuupf>): "The address zero is to be interpreted as meaning "this", as in "this network". The address of all ones are to be interpreted as meaning "all", as in "all hosts"".

### Subnetting a classful network

You can use subnetting to divide a large network into multiple smaller networks. A network that uses host bits as part of the network ID is called a *classless network*. To transform a large network into smaller networks you take the leftmost bits from the host ID and assign them to the network ID portion of the subnet mask.

You can identify the network ID of a subnet mask by the 1s. You can identify the host ID by the 0s. Any bits taken from the host ID and allocated to the network ID must be contiguous with the original network ID:

- Each 1 bit is part of the network ID.
- Each 0 bit is part of the host ID.

The mathematical process that is used to compare an IP address and a subnet mask is called *ANDing*.

When you use more bits for the subnet mask, you can have more subnets, but you can then have fewer hosts on each subnet. Using more bits than you need allows for subnet growth, but limits growth for

hosts. Using fewer bits than you need allows for growth in the number of hosts you can have, but limits growth in subnets.

### Simple IPv4 networks

In simple IPv4 networks, the subnet mask defines full octets as part of the network ID and host ID. A 255 represents an octet that is part of the network ID, and a 0 represents an octet that is part of the host ID. For example, you can use the 10.0.0.0 network with a subnet mask of 255.255.0.0 to create 256 smaller networks.



**Note:** The IPv4 address 127.0.0.1 is used as a loopback address; you can use this address to test the local configuration of the IPv4 protocol stack. Consequently, the network address 127 is not permitted for configuring IPv4 hosts.

### Complex IPv4 networks

In complex networks, subnet masks might not be simple combinations of 255 and 0. Rather, you might subdivide one octet with some bits that are for the network ID, and some that are for the host ID. This allows you to have the specific number of subnets and hosts that you require. 172.16.0.0 with the subnet mask 255.255.240.0 is an example of a subnet mask that can be used to divide a Class B network into 16 subnets.

### Variable-length subnet masks

Modern routers support the use of variable length subnet masks, which allow you to create subnets of different sizes when you subdivide a larger network. For example, you could subdivide a small network with 256 addresses into three smaller networks of 128 addresses, 64 addresses, and 64 addresses. This allows you to use IP addresses in a network more efficiently.

### Determining subnet addresses

To select an appropriate addressing scheme for your organization, perform the following steps:

1. Decide whether to use public or private IPv4 addresses.
2. Determine the number of subnets you need and then determine the subnet bits. For example, if you need six subnets, then you would need three subnet bits (this will provide eight subnets). Subnets are calculated by using the formula  $2^n$ , where  $n$  is the number of bits. The following table lists more examples.


Subnet bits	Formula	Subnets
1	$2^1$	2
2	$2^2$	4
3	$2^3$	8
4	$2^4$	16
5	$2^5$	32
6	$2^6$	64

3. To determine the subnet mask, evaluate the binary number of subnet bits. For example, if you are using three subnet bits (11100000), then the subnet mask is 224. To determine the number of increments, evaluate the lowest-value bit in the subnet mask. For example, the lowest-value bit in the 224 subnet mask is 32, and that would be the increment between addresses. The following table lists more examples.

Subnets	Subnet bits	Binary	Subnet mask	Increment between addresses
2	1	10000000	128	128
4	2	11000000	192	64
8	3	11100000	224	32
16	4	11110000	240	16
32	5	11111000	248	8
64	6	11111100	252	4

4. To assign host IP addresses, remember the following:
- The first host is one binary digit higher than the current subnet ID.
  - The last host is two binary digits lower than the next subnet ID.
  - The first and last address in any network or subnet cannot be assigned to any individual host.
  - The number of usable hosts depends on the number of bits. The formula is  $(2^n)-2$ , where n is the number of bits.
  - 0 is the network address, and the value of 255 (or whatever the last address is) is reserved for broadcast communication. More examples are provided in the following table.

Subnets	Subnet bits	Binary	Subnet mask	Increment between addresses	Host bits	Number of usable hosts
2	1	10000000	128	128	7	126
4	2	11000000	192	64	6	62
8	3	11100000	224	32	5	30
16	4	11110000	240	16	4	14
32	5	11111000	248	8	3	6
64	6	11111100	252	4	2	2

 **Note:** Notice that you are trading off the number of subnets and the number of hosts. When you use more bits for the subnet mask, you can have more subnets, but fewer hosts on each subnet. Using more bits than you need allows for subnet growth but limits growth for hosts. Using fewer bits than you need allows for growth in the number of hosts you can have but limits growth in subnets.

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



**Question:** Does your organization use simple or complex networking?

## Public, private, and APIPA addresses

Devices and hosts that connect directly to the Internet require a public IPv4 address. Hosts and devices that do not connect directly to the Internet do not require a public IPv4 address.

### Public IPv4 addresses

Public IPv4 addresses must be unique. Internet Assigned Numbers Authority (IANA) assigns public IPv4 addresses to regional Internet registries, which then assign IPv4 addresses to Internet service providers (ISPs). Usually your ISP allocates you one or more public addresses from its address pool. The number of addresses that your ISP allocates to you depends upon how many devices and hosts that you connect to the Internet.

Public	Private
<ul style="list-style-type: none"> <li>• Required by devices and hosts that connect directly to the Internet</li> <li>• Must be globally unique</li> <li>• Routable on the Internet</li> <li>• Must be assigned by IANA/RIR</li> </ul> 	<ul style="list-style-type: none"> <li>• Not routable on the Internet               <ul style="list-style-type: none"> <li>• 10.0.0.0/8</li> <li>• 172.16.0.0/12</li> <li>• 192.168.0.0/16</li> </ul> </li> <li>• Can be assigned locally by an organization</li> <li>• Must be translated to access the Internet</li> </ul> 

### Private IPv4 addresses

Computers and devices that need to connect to the Internet must be configured with public IP addresses. However, the number of public IPv4 addresses is becoming limited. Because organizations cannot obtain public IPv4 address for every corporate computer, they use private IP addressing instead.

Because private IP addresses are not routable on the Internet, computers configured with a private IP address cannot access the Internet directly. Technologies such as network address translation (NAT) enable administrators to use a relatively small number of public IPv4 addresses and, at the same time, enable local hosts with private IP addresses to connect to remote hosts and services on the Internet.

IANA defines the address ranges in the following table as private. Internet-based routers do not forward packets originating from, or destined to, addresses in these ranges.

Network	Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

### Automatic Private IP Addressing (APIPA)

Typically, when a computer running Windows starts, it sends a broadcast to find a DHCP server from which to get an IP Address. However, if a Windows client is unable to find a DHCP server it can assign itself an APIPA address from a range reserved by Microsoft. The IP address range used for APIPA is 169.254.0.1 through 169.254.255.254. When a Windows client assigns itself an APIPA address, it also configures itself with a default Class B subnet mask of 255.255.0.0. A Windows client using an APIPA address does not assign itself a default gateway. A client will continue to use the APIPA address, broadcasting for a DHCP server every 5 minutes, until a DHCP server becomes available.

## Discussion: Determining IPv4 notation and translation

For this discussion, the following questions and examples will help with reviewing the previous material.

**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

**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

**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

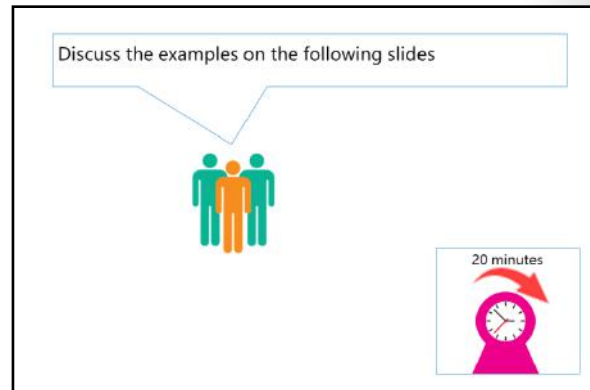
10.25.12.100/16

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



## Discussion: Creating a subnetting scheme for a new office



For this discussion, read the scenario and answer the questions on the slide.

### Scenario

You are designing an appropriate network configuration for a new campus. You have been allocated the 10.34.0.0/16 network that you can subnet as required, given these requirements:

- There are four buildings on the new campus, and each should have its own subnet to allow for routing between the buildings.
- Each building will have up to 700 users.
- Each building will have network printers that will require IP addresses.
- The typical ratio of users to printers is 50 to 1.
- You need to allocate a subnet for the server data center that will hold up to 100 servers.

- How many subnets are required?
- How many bits are required to create that number of subnets?
- How many hosts are required on each subnet?
- How many bits are required to support that number of hosts?
- What is an appropriate subnet mask that would satisfy these requirements?

### Discussion questions

Based on this scenario, answer the following questions:

**Question:** How many subnets are required?

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

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

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

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

## Creating supernets

*Supernetting* combines multiple small networks into a single large network. This could be appropriate when you have a small network that has grown and you need to expand the address space. For example, if a branch office that is using the network 192.168.16.0/24 exhausts all of its IP addresses, you could allocate the additional network 192.168.17.0/24 to it. If you use the default subnet mask of 255.255.255.0 for these networks, then you must perform routing between them. You can use supernetting to combine them into a single network.

- Supernetting combines multiple small networks into a larger network
- The networks that you combine must be contiguous
- The following table shows an example of supernetting two class C networks (host bits underlined)

Network	Range
192.168. <u>00010000</u> . <u>00000000</u> /24	192.168.16.0 - 192.168.16.255
192.168. <u>00010001</u> . <u>00000000</u> /24	192.168.17.0 - 192.168.17.255
192.168. <u>00010000</u> <u>00000000</u> /23	192.168.16.0 - 192.168.17.255

To perform supernetting, the networks that you are combining must be contiguous. For example, 192.168.16.0/24 and 192.168.17.0/24 can be supernetted, but you cannot supernet 192.168.16.0/24 and 192.168.54.0/24.



Supernetting is the opposite of subnetting. When you perform supernetting, you allocate bits from the network ID to the host ID. The following table shows how many networks you can combine by using a specific number of bits.

Number of bits	Number of networks combined
1	2
2	4
3	8
4	16

The following table shows an example of supernetting two Class C networks. The portion of the subnet mask that you are using as part of the network ID is in bold type.

Network	Range
192.168. <b>00010000</b> .00000000/24	192.168.16.0-192.168.16.255
192.168. <b>00010001</b> .00000000/24	192.168.17.0-192.168.17.255
192.168. <b>00010000</b> .00000000/23	192.168.16.0-192.168.17.255

### Check Your Knowledge

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.	
Select the correct answer.	
<input type="checkbox"/>	/20
<input type="checkbox"/>	/21
<input type="checkbox"/>	/22
<input type="checkbox"/>	/23
<input type="checkbox"/>	/24

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

## Lab A: Planning an IPv4 network

### Scenario

A. Datum Corporation is an international organization with the North American regional office located in Toronto. They are planning to open three branch offices in different cities in North America. The branch offices will be located in Houston, Mexico City, and Portland.

The following table describes the planned computer distribution in the branch offices.

Location	Computer and device requirements
Houston	<ul style="list-style-type: none"> <li>• 300 desktop computers</li> <li>• 100 laptop computers connecting to the wireless and wired networks</li> <li>• 50 tablet computers connecting only to the wireless network</li> </ul>
Mexico City	<ul style="list-style-type: none"> <li>• 100 desktop computers</li> <li>• 50 laptop computers connecting to the wireless and wired networks</li> <li>• 20 tablet computers connecting only to the wireless network</li> </ul>
Portland	<ul style="list-style-type: none"> <li>• 100 desktop computers</li> <li>• 75 laptop computers connecting to the wireless and wired networks</li> <li>• 150 tablet computers connecting only to the wireless network</li> </ul>

A. Datum is using Office 365 for all email and file access for the North American branch offices, with some shared folders located in the Toronto regional office on Windows servers. Because all offices have fast and highly available network connections to the Toronto office, A. Datum is not planning to deploy any servers in the branch offices at this point.

The A. Datum network team has assigned the subnets 172.16.18.0/18 to the Toronto regional office. The Toronto office is currently using the network assignments shown in the following table.

IP Subnet	Purpose
172.16.18.0/24	Network devices and network printers
172.16.19.0/24	Servers
172.16.20.0/24 to 172.16.52.0/24	Desktop computers
172.16.53.0/24 to 172.16.60.0/24	Wireless devices

You need to plan an IPv4 address assignment for each of the branch offices, use IP addresses from the list of addresses assigned to the Toronto office. Ensure that the IP addresses assigned to computers connected to wired connections are different from the IP addresses assigned to devices connected to the wireless networks.

## Objectives

After completing this lab, you will be able to:

- Plan an IPv4 implementation.

## Lab Setup

Estimated Time: 30 minutes

You do not need any virtual machines to complete this lab.

For this lab, you will not use a virtual machine environment.

## Exercise 1: Planning the IPv4 address assignments

### Scenario

You need to plan the IP address assignment for each North American branch office. Your IP addressing scheme must meet the following requirements:

- Wired and wireless clients must be assigned IP addresses from different IP ranges.
- Each branch office location should have dedicated IP ranges.
- Keep subnets in branch office locations as simple as possible.
- Ensure that branch office subnets have IP addresses for all potential wired and wireless clients that might request an IP address.

The main task for this exercise is as follows:

1. Plan the IPv4 implementation.

### ► Task 1: Plan the IPv4 implementation

1. How will you determine the number of IP addresses required for each location?
2. How do the laptops that have both wired and wireless network adapters affect the number of IP addresses required?
3. What is the simplest subnet class to use when planning an IP addressing scheme for each of the North America branch locations?
4. In the Houston office, what is the number of potential wired and wireless clients?
5. In the Houston office, how many /24 subnets are required for wired connections? How many are required for wireless?
6. In the Mexico City office, what is the number of potential wired and wireless clients?
7. In the Mexico City office, how many /24 subnets are required for wired connections? How many for wireless?
8. In the Portland office, what is the number of potential wired and wireless clients?
9. In the Portland office, how many /24 subnets are required for wired connections? How many for wireless?
10. Given the assigned IP range of 172.16.20.0/24 – 172.16.52.0/24 for wired clients, which subnets will you use for the Houston, Mexico City, and Portland offices?
11. Given the assigned IP range of 172.16.53.0/24 – 172.16.60.0/24 for wireless clients, which subnets will you use for the Houston, Mexico City, and Portland offices?

**Results:** You will have planned an IPv4 network.

**Question:** How many default gateways will be required?

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

## Lesson 2

# Configuring an IPv4 host

An incorrect IPv4 configuration affects the availability of services that are running on a server. To ensure connectivity to network services, you need to understand how to configure and troubleshoot IPv4.

### Lesson Objectives

After completing this lesson, you should be able to:

- Describe the configurable IP\*v4 settings.
- Describe the tools used to configure IPv4.
- Configure IPv4 manually to provide a static configuration for a server.
- Describe the automatic configuration of IPv4.

### Configurable IPv4 settings

You can configure IPv4 addresses manually or IP addresses can be assigned automatically. Manual configuration requires that you visit each computer or device and set the necessary entries. Static IP addresses are usually configured on servers, routers, switches, or other network devices that need to maintain persistent IP configuration that does not change over time. Manually entering a static configuration also increases the risk of configuration mistakes.

Automatic configuration lessens the chance of a manual error and does not require you to visit each system. Typically, automatic configuration is provided by a server on the networks, which is used to configure client workstations and mobile devices. When using automatic configuration, you can specify an alternate configuration for the client to use in case a configuration server cannot be contacted. By default, Windows systems use APIPA addressing if a configuration server cannot be contacted.

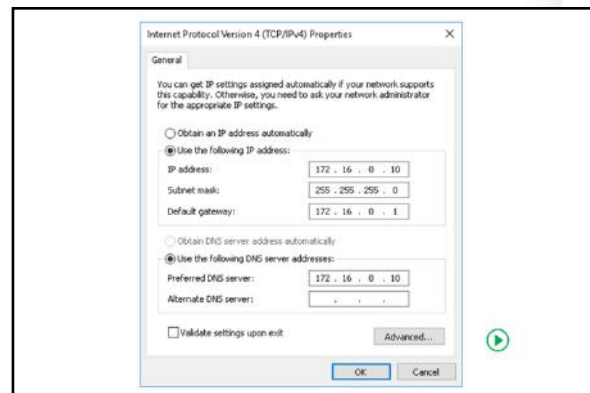
Regardless of how you configure a computer's IPv4 address, the following settings are required for communication:

- IPv4 address
- Subnet mask

If your network consists of multiple subnets that require communication, you are also required to configure the following:

- Default gateway
- Domain Name System (DNS) servers

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



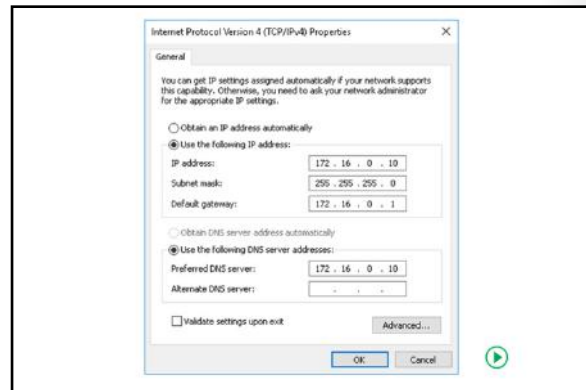
## Tools for configuring IPv4

To configure an IPv4 address manually, enter the IPv4 address by using the Windows Server graphical interface netsh or Windows PowerShell.

### Settings or the Network and Sharing Center

By using either the Settings app or the Network and Sharing Center, you can open the graphical interface as shown in the previous topic. In addition to the basic IPv4 settings, you can configure a network adapter with:

- Additional IPv4 addresses, such as when the server is a web server hosting multiple sites.
- Additional default gateways, for example if you wanted to specify a second gateway for failover support.
- Additional DNS servers to provide additional DNS servers to query if the other DNS servers are unavailable.
- DNS settings, such as DNS search suffixes, and whether or not the adapter should be automatically registered with DNS.
- Windows Internet Name Service (WINS) settings for legacy support.



### Configuring a static IP address by using netsh

You can configure a static IP address by using the netsh command-line tool. For example, the following command configures the interface Local Area Connection with the following parameters:

- Static IP address 10.10.0.10
- Subnet mask 255.255.255.0
- Default gateway 10.10.0.1
- DNS servers 10.12.0.1 and 10.12.0.2

```
Netsh interface ipv4 set address name="Local Area Connection" source=static
addr=10.10.0.10 mask=255.255.255.0 gateway=10.10.0.1
Netsh interface ipv4 set dns name="Local Area Connection" source=static addr=10.12.0.1
Netsh interface ipv4 add dns name="Local Area Connection" 10.12.0.2 index=2
```



**Note:** For more information about netsh commands, go to <http://aka.ms/Pyd130>

## Configuring a static IP address by using Windows PowerShell


Windows Server 2016 includes Windows PowerShell cmdlets that you can use to manage network configuration. The following table describes some of the Windows PowerShell cmdlets that are available for configuring IPv4.

Cmdlet	Description of IPv4 configuration uses
<b>Get-NetIPConfiguration</b>	Gets the IP network configuration.
<b>New-NetIPAddress</b>	Use this command to create a new IP address and bind it to a network adapter. You cannot use this command to change an IP address.
<b>Remove-NetIPAddress</b>	This command removes an IP address and its configuration.
<b>Set-NetIPAddress</b>	This command modifies the configuration of an IP address.
<b>Set-NetIPInterface</b>	You can use this command to enable or disable DHCP for an interface.
<b>New-NetRoute</b>	This command creates routing table entries, including the default gateway (0.0.0.0). You cannot use this cmdlet to modify the next hop of an existing route; instead, you must remove an existing route and create a new route with the correct next hop.
<b>Set-DNSClientServerAddress</b>	Configures the DNS server that is used for an interface.

The following code is an example of the Windows PowerShell cmdlets that you can use to configure the interface Local Area Connection with the following parameters:

- Static IP address      10.10.0.10
- Subnet mask            255.255.255.0
- Default gateway        10.10.0.1
- DNS servers 10.12.0.1 and 10.12.0.2.

```
New-NetIPAddress -InterfaceAlias "Local Area Connection" -IPAddress 10.10.0.10 -
PrefixLength 24 -DefaultGateway 10.10.0.1
Set-DNSClientServerAddress -InterfaceAlias "Local Area Connection" -ServerAddresses
10.12.0.1,10.12.0.2
```

 **Additional Reading:** For more information about net TCP/IP cmdlets in Windows PowerShell, go to <http://aka.ms/L50hb6>

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

## Demonstration: Configuring IPv4

There are multiple ways to configure an IPv4 address. Two common methods are by using the Internet Protocol Version 4 (TCP/IPv4) Properties interface and Windows PowerShell.

### Demonstration Steps

#### Configuring IPv4 by using the user interface

1. On **LON-SVR1**, open the **Network and Sharing Center**.
2. Open the **Network Connections** window.
3. Open the **Ethernet** adapter's properties.
4. Open the **Internet Protocol Version 4 (TCP/IPv4)** properties.
5. Change the **IP Address** to **172.16.0.111**.
6. Click **OK** and then close all open windows.

#### Configuring IPv4 by using Windows PowerShell

1. Open **Windows PowerShell**.
2. Check the IP address by running the following command:

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

3. Run the following command to remove the IP address:

```
Remove-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.0.111
```

4. Verify the IP address was removed by running the following command:

```
Get-NetIPAddress -InterfaceAlias "Ethernet"
```

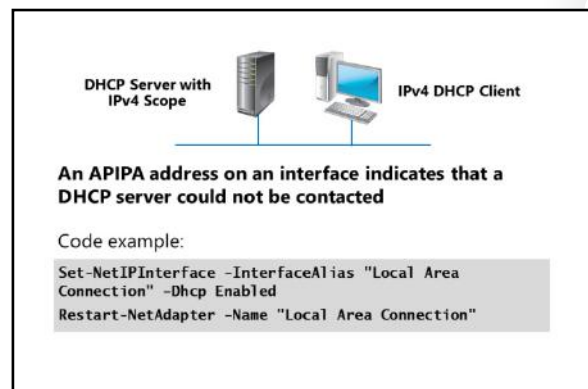
5. Add the new IP address to the interface by running the following command:

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.0.11 -PrefixLength 24
```

6. Close all open windows, and then minimize all the virtual machines.

## Configuring IPv4 automatically

DHCP for IPv4 enables you to automate the process of assigning IPv4 addresses to large numbers of computers without having to assign each one individually. The DHCP service receives requests for IPv4 configuration from computers that you configure to obtain an IPv4 address automatically. It also assigns additional IPv4 settings from scopes that you define for each of your network's subnets. The DHCP service identifies the subnet from which the request originated and assigns IP configuration from the





relevant scope.

DHCP helps simplify the IP configuration process. However, you must be aware that if you use DHCP to assign IPv4 information and the service is business-critical, you must do the following:

- Include resilience in your DHCP service design so that the failure of a single server does not prevent the service from functioning.
- Configure the scopes on the DHCP server carefully. If you make a mistake, it can affect the entire network and prevent communication.

When you use a laptop to connect to multiple networks, such as one at work and one at home, you should configure the IP addressing differently on each network. However, if a DHCP server exists on both networks, the DHCP server will configure the laptop IP settings automatically.

Windows operating systems also support the use of the following technologies for assigning IP addresses:

- Automatic Private IP Addressing (APIPA). In a scenario when there is no DHCP server on the network or the DHCP server is not available, Windows uses APIPA to automatically assign itself an IP address in the address range between 169.254.0.0 and 169.254.255.255. Because APIPA does not configure the computer with DNS and default gateway settings, computers with assigned APIPA addresses have limited networking functionality. APIPA can also be used for troubleshooting DHCP. If the network administrator notices that the computer has an address from the APIPA range, it is an indication that the computer cannot communicate with the DHCP server.
- Alternate static IP address. If you have configured an alternate static IP address on a computer network adapter and the DHCP server is not available, the computer network adapter will use the alternate static IP address.

Windows Server 2016 also has Windows PowerShell cmdlets that you can use to enable DHCP for an interface. The following table describes some of the available Windows PowerShell cmdlets that are available for configuring DHCP on an interface.

Cmdlet	Description
<b>Get-NetIPAddress</b>	Obtains a list of interfaces and their configuration. This does not include IPv4 configuration of the interface.
<b>Set-NetIPAddress</b>	Enables or disables DHCP for an interface.
<b>Get-NetAdapter</b>	Obtains a list of network adapters in a computer.
<b>Restart-NetAdapter</b>	Disables and reenables a network adapter. This forces a DHCP client to obtain a new DHCP lease.

The following code is an example of how you can enable DHCP for the adapter Local Area Connection, and ensure that it receives an address:

```
Set-NetIPAddress -InterfaceAlias "Local Area Connection" -Dhcp Enabled
Restart-NetAdapter -Name "Local Area Connection"
```

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

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

## Lesson 3

# Managing and troubleshooting IPv4 network connectivity

The troubleshooting tools in Windows Server 2016 are similar to the troubleshooting tools in previous versions of Windows client operating systems and Windows Server operating systems. You could use tools, such as Microsoft Message Analyzer, to perform detailed analysis of your network communication.

### Lesson Objectives

After completing this lesson, you should be able to:

- Describe IPv4 routing.
- Describe the methods for modifying routing.
- Describe the IPv4 troubleshooting process.
- Explain how to use IPv4 troubleshooting tools.
- Use IPv4 troubleshooting tools.
- Describe the function of Microsoft Message Analyzer.
- Use Microsoft Message Analyzer to capture and analyze network traffic.

### Routing between IPv4 networks

IPv4 subnets are typically separated by a router, typically the router address is configured as the default gateway in the IPv4 settings. The router is responsible for handling incoming and outgoing IPv4 traffic, and delivering the IPv4 traffic to its intended destination. When a router receives traffic destined for an endpoint outside of the local network, it checks to determine whether it has a route to the destination network. If the route exists, the router forwards the packet to the destination network router address. If a route does not exist, the router sends the traffic to the router's default gateway or default route.

- IPv4 subnets are typically separated by a router
- The router is responsible for handling incoming and outgoing IPv4 traffic, and delivering the IPv4 traffic to its intended destination
- Routers send traffic to destinations based on a set of data called routing tables
- Routing tables contain the following information about a route for a specific interface:
  - Network destination
  - Netmask
  - Gateway
  - Interface
  - Metric

Traffic travel between routers and IPv4 endpoints is typically described in hops. One hop represents the traffic between two individual routers or a router and an IPv4 endpoint. When a router forwards IPv4 traffic, it does so in a way that will minimize the number of hops between IPv4 endpoints.

### Understanding routing tables

Routers send traffic to destinations based on a set of data called *routing tables*. Routing tables contain:

- All routes of which the router is aware.
- Information on which connections lead to different IP address ranges.
- Priorities for connections to be used.
- Rules for handling both typical and special cases of traffic.

The data stored in routing tables is typically dynamic. They are updated by using routing protocols, such as the Routing Information Protocol or the Open Shortest Path First (OSPF).

Routing tables contain the following information about a route for a specific interface:

- Network destination. The destination host where the traffic is to be transmitted.
- Netmask. The subnet mask for the route.
- Gateway. The gateway address to be used for IPv4 traffic using the route.
- Interface. The IPv4 interface address number for the route.
- Metric. The relative cost for the route. Lower values represent less cost.

Routing tables also exist on client computers to enable client computers to determine the default route for network traffic.

For example, the following entry in the routing table would point any traffic destined for the 10.0.0.0/8 network to the gateway at the IPv4 address of 192.168.0.1, with a metric of 1.

Network Destination	Netmask	Gateway	Metric
10.0.0.0	255.0.0.0	192.168.0.1	1



**Note:** The default gateway for a computer running Windows Server 2016 is configured as the default route. In a default route, both Network Destination and Netmask are set to 0.0.0.0, and the Gateway is set to the default gateway specified in the IPv4 settings for the network adapter. The default route will be used to direct all outgoing traffic, unless a route exists corresponding to the appropriate Network Destination in the routing table.

## Routing IPv4 with Windows Server 2016

In many cases, organizations separate their local network from the public Internet by using a perimeter network (also known as DMZ, demilitarized zone, or screened subnet). The perimeter network contains IPv4 endpoints that must be reachable from the public Internet, but that should not be located on the local network for functional or security reasons.

Windows Server 2016 can be used as a router between a local network and the perimeter network, or—less commonly—between the perimeter network and the public Internet. Windows Server 2016 can be configured to act as a router by installing the Remote Access role with the Routing role service. It is also common for a Windows Server 2016 router to have a more complex Windows Firewall with Advanced Security configuration to ensure adequate protection from external threats and to ensure that acceptable traffic is allowed to pass through the firewall.

## Modifying IPv4 routing

After Windows Server 2016 is configured to route IPv4 traffic, there can be several cases when you might want to modify routing tables to ensure that traffic passes to the correct network through the correct network interface. This occurs most commonly in routers positioned in the perimeter network that need to route IPv4 traffic within the perimeter network into the local, private network, or out to the Internet.

You can use several methods to view and modify the routing table:

- The Route command  
**route add 10.0.0.0 netmask 255.0.0.0 192.168.0.1**
- Get-NetRoute, New-NetRoute, and Set-NetRoute Windows PowerShell cmdlets  
**Get-NetRoute -AddressFamily IPv4**
- The Routing and Remote Access console

## Viewing and modifying the routing table

There are several ways you can view the routing table for a computer running Windows Server 2016:

- By using Windows PowerShell:
  - To view the IPv4 routing table, type the following at the command line, and then press Enter.

```
Get-NetRoute -AddressFamily IPv4
```

- To create a new route in the routing table, use the **New-NetRoute** cmdlet. For example, the following command will add a new route on the network adapter with the interface index of 10 for the 10.0.0.0/8 network, and direct it to the gateway at 192.168.0.1.

```
New-NetRoute -InterfaceIndex 10 -DestinationPrefix 10.0.0.0/8 -NextHop  
192.168.0.1
```

- You can also change route settings with the **Set-NetRoute** cmdlet. Typically, **Set-NetRoute** is used to adjust metric values for existing routes. You cannot modify the **DestinationPrefix** or **NextHop** properties of an existing route by using **Set-NetRoute**.
- By using the **route** command:
  - To view the routing table, type the following at the command line, and then press Enter.

```
route print
```

This command will output a text-based table displaying the following information:

- Network destination. The destination host where the traffic is to be transmitted.
- Netmask. The subnet mask for the route.
- Gateway. The gateway address to be used for IPv4 traffic using the route.
- Interface. The IPv4 interface address number for the route.
- Metric. The relative cost for the route. Lower values represent less cost, which typically means a shorter round trip for the packets.
- To modify the routing table, you can use the **route** command with either the **Add**, **Delete**, or **Change** commands, specifying the preceding parameters. For example, the following command will add a new route for the 10.0.0.0/8 network, and direct it to the gateway at 192.168.0.1 with a relatively low metric of 2.

```
Route add 10.0.0.0 netmask 255.0.0.0 192.168.0.1 metric 2
```

- By using the **Routing and Remote Access** console:

You can view and modify IPv4 routing tables on a Windows Server 2016 router by expanding the **IPv4** node within the **Routing and Remote Access** console. After installing the Remote Access role, you can access the **Routing and Remote Access** console from the **Tools** menu in **Server Manager**.

- To view the routing table, follow these steps:
  - i. Open the **Routing and Remote Access** console.
  - ii. In the **Routing and Remote Access** console, expand the local server, and then expand **IPv4**.
  - iii. Right-click **Static Routes**, and then click **Show IP Routing Table**.

- o To add a new route, perform the following steps from within the **Routing and Remote Access** console:
  - i. Under the **IPv4** node, right-click **Static Routes**, and then click **New Static Route**.
  - ii. Configure the static route with the appropriate Interface, Destination, Network Mask, and Gateway, and then click **OK**.

Manually created static routes will appear in the details pane when the **Static Routes** node is selected.

## IPv4 troubleshooting methodology

The first step in troubleshooting a network problem is identifying the scope of the problem. The causes of a problem that affects a single user probably differs from a problem that affects all users. If a problem affects only a single user, then the problem is likely related to the configuration of that one computer. If a problem affects all users, then the problem is likely either a server configuration issue or a network configuration issue. If a problem affects only a group of users, then you need to determine the common denominator among that group of users.

One methodology is to ask a series of questions about the nature of the issue.

1. Can you duplicate the issue?
2. What is working?
3. What does not work?
4. How are the things that work and do not work related?
5. Does it work for other systems on the network?
6. Has it worked in the past?
7. What has changed since it last worked?

To troubleshoot network communication problems, you need to understand the overall communication process. This requires that you understand the routing and firewall configuration on your network. There are many approaches to troubleshooting TCP/IP issues. One methodology that is quite useful is a logical approach starting with common questions, such as:

1. Can you duplicate the issue? This will help you determine if there is really an issue or if a simple mistake had been made.
2. What is working? This will help you to determine the nature of the issue. For example, the system might be able to reach resources on the local network but not on a remote network.
3. What does not work? This question can help further expand the answer to the previous question. For example, a system might not be able to connect to a remote resource but it might be able to resolve the address of the remote resources.
4. How are the things that work and that do not work related? For example, being able to connect to local resources shows that IP is working and being able to resolve remote addresses shows that DNS is working. If the DNS server is on a different network, it also tells you the default gateway is working.
5. Does it work for other systems on the network? This will help you determine where the issue lies. For example, if a different system cannot access the same remote resource, it is an indication that the issue lies with the infrastructure in-between or the remote resource itself.
6. Has it worked in the past? This will help determine what should be examined. For example, if it is a remote resource that has never been accessed before, the issue could be as simple as the new resource not being ready yet.
7. What has changed since it last worked? For example, with the unreachable remote resource, questions you might ask include: Were new networking components installed? Did the IP address schema change?

Answering these questions can help you to determine which tools you will need to resolve an issue in a timely fashion.

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

## Tools for troubleshooting IPv4

Windows Server 2016 includes a number of command-line tools that can help you diagnose network problems. These tools were commonly used in earlier Windows Server editions.

### Ipconfig

Ipconfig is a command-line tool that displays the current TCP/IP network configuration. Additionally, you can use the **ipconfig** command to refresh DHCP and DNS settings. The following table describes the command-line options for **ipconfig**.

Use the following tools to troubleshoot IPv4:

- Ipconfig
- Ping
- Tracert
- Pathping
- Telnet
- Netstat
- Resource Monitor
- Windows Network Diagnostics
- Event Viewer

Command	Description
<b>ipconfig /all</b>	View detailed configuration information.
<b>ipconfig /release</b>	Release the leased configuration back to the DHCP server.
<b>ipconfig /renew</b>	Renew the leased configuration.
<b>ipconfig /displaydns</b>	View the DNS resolver cache entries.
<b>ipconfig /flushdns</b>	Purge the DNS resolve cache.

### Ping

Ping is a command-line tool that verifies IP-level connectivity to another TCP/IP computer. It sends Internet Control Message Protocol (ICMP) echo request messages and displays the receipt of corresponding echo reply messages. Ping is the primary TCP/IP command that you use to troubleshoot connectivity, but firewalls might block the ICMP messages.

### Tracert

Tracert is a command-line tool that identifies the path taken to a destination computer by sending a series of ICMP echo requests. Tracert then displays a list of router interfaces between a source and a destination. This tool also determines which router has failed and what the latency, or speed, is. These results might not be accurate if the router is busy because the ICMP packets are assigned a low priority by the router.

### Pathping

Pathping is a command-line tool that traces a route through the network in a manner similar to Tracert. However, Pathping provides more detailed statistics on the individual steps, or *hops*, through the network. Pathping can provide greater detail because it sends 100 packets for each router, which enables it to establish trends.

## Route

Route is a command-line tool that allows you to view and modify the local routing table. You can use this to verify the default gateway, which is listed as the route 0.0.0.0. In Windows Server 2016, you can also use Windows PowerShell cmdlets to view and modify the routing table. The cmdlets for viewing and modifying the local routing table include **Get-NetRoute**, **New-NetRoute**, and **Remove-NetRoute**.

## Telnet

You can use the Telnet Client feature to verify whether a server port is listening. For example, the command **telnet 10.10.0.10 25** attempts to open a connection with the destination server, 10.10.0.10, on port 25, Simple Mail Transfer Protocol (SMTP). If the port is active and listening, it returns a message to the Telnet client.

## Netstat

Netstat is a command-line tool that enables you to view network connections and statistics. For example, the **netstat -ab** command returns all listening ports and the executable that is listening.

## Resource Monitor

Resource Monitor is a graphical tool that allows you to monitor system resource utilization. You can use Resource Monitor to view TCP and User Datagram Protocol (UDP) ports that are in use. You can also verify which programs are using specific ports and the amount of data that they are transferring on those ports.

## Network Diagnostics

Use Windows Network Diagnostics to diagnose and correct networking problems. In the event of a Windows Server networking problem, the **Diagnose Connection Problems** option helps you diagnose and repair the problem. Windows Network Diagnostics returns a possible description of the problem and a potential remedy. However, the solution might require manual intervention from the user.

## Event Viewer

*Event logs* are files that record significant events on a computer, such as when a process encounters an error. When these events occur, the Windows Server 2016 operating system records the event in an appropriate event log. You can use Event Viewer to read the event log. IP conflicts, which might prevent services from starting, are listed in the System event log.

## Windows PowerShell

Although you could use Windows PowerShell in earlier versions of Windows Server to perform network troubleshooting and configuration, it requires you to use Windows Management Instrumentation (WMI) objects, which are more difficult to use than native Windows PowerShell cmdlets.

The following table lists some of the Windows PowerShell cmdlets that you can use.

Cmdlet	Purpose
<b>Get-NetAdapter</b>	Obtains a list of network adapters in a computer.
<b>Get-NetIPv4Protocol</b>	Gets information about the IPv4 protocol configuration. Note that the <b>Get-NetIPv6Protocol</b> gets information about the IPv6 protocol configuration.
<b>Restart-NetAdapter</b>	Disables and reenables a network adapter.
<b>Get-NetIPInterface</b>	Obtains a list of interfaces and their configuration.
<b>Get-NetIPAddress</b>	Obtains a list of IP addresses that are configured for interfaces.

Cmdlet	Purpose
<b>Get-NetRoute</b>	Obtains the list of routes in the local routing table.
<b>Get-NetConnectionProfile</b>	Obtains the type of network (public, private, domain) to which a network adapter is connected.
<b>Get-DnsClient</b>	Retrieves configuration details specific to the different network interfaces on a specified computer.
<b>Get-DNSClientCache</b>	Obtains the list of resolved DNS names that are stored in the DNS client cache.
<b>Get-DnsClientGlobalSetting</b>	Retrieves global DNS client settings such as the suffix search list.
<b>Get-DNSClientServerAddress</b>	Obtains the list of DNS servers that are used for each interface.
<b>Register-DnsClient</b>	Registers all of the IP addresses on the computer on the configured DNS server.
<b>Set-DnsClient</b>	Sets the interface-specific DNS client configurations on the computer.
<b>Set-DnsClientGlobalSetting</b>	Configures the global DNS client settings such as the suffix search list.
<b>Set-DnsClientServerAddress</b>	Configures the computer's network adapter with the IP addresses of the DNS server.
<b>Set-NetIPAddress</b>	Sets information about the IP address configuration.
<b>Set-NetIPv4Protocol</b>	Sets information about the IPv4 protocol configuration. Note that the Set-NetIPv6Protocol returns information about the IPv6 protocol configuration.
<b>Set-NetIPInterface</b>	Modifies the IP interface properties.
<b>Test-Connection</b>	Runs connectivity tests that are similar to those used by ping.
<b>Test-NetConnection</b>	Displays the following: <ul style="list-style-type: none"> <li>• Results of a DNS lookup</li> <li>• Listing of IP interfaces</li> <li>• Option to test a TCP connection</li> <li>• IPsec rules</li> <li>• Confirmation of connection establishment</li> </ul>
<b>Resolve-Dnsname</b>	Performs a DNS name query resolution for the specified name.



The following are some of the actions that you can use to identify the cause of network communication problems:

- If you know what the correct network configuration for the host should be, use one of the following to verify that it is configured correctly:

- Windows PowerShell: **Get-NetIPAddress**
- Command-line: **ipconfig**

If the command returns an address on the 169.254.0.0/16 network, it indicates that the host failed to obtain an IP address from DHCP.

- To help identify the routing path through your network, you can use the Windows PowerShell cmdlet **Test-NetConnection -TraceRoute**, or you can use the command-line tool **tracert**.
- To see if the remote host responds, use one of the following:

- Windows PowerShell: **Test-NetConnection**
- Command-line: **ping**

When you use either method to return the DNS name of the remote host, you verify both name resolution and whether the host responds. Be aware that Windows Firewall on member servers and client computers often blocks ping attempts. When this happens, the lack of a ping response might not be an indicator that the remote host is not functional, but only that the ping is being blocked. If you can ping other remote hosts on the same network, this might mean that the problem is on the remote host.

- You can use the **Test-NetConnection** cmdlet in Windows PowerShell to test the service you are connecting to on the remote host. For example, use **Test-NetConnection -Port 80** to test connectivity to a web server. You can also use **Telnet** to connect to the port of the remote program.
- To see if the default gateway responds, use one of the following:
  - Windows PowerShell: **Test-NetConnection**
  - Command-line: **ping**

Most routers respond to **Test-NetConnection** and **ping** requests. If you do not get a response when you ping the default gateway, then there is likely a configuration error on the client computer, such as an incorrect configuration of the default gateway. It is also possible that the router is experiencing errors.

## Demonstration: Troubleshooting IPv4

There are several Windows PowerShell and command-line tools that can help you analyze a network connection.

### Demonstration Steps

#### Using Get-NetIPAddress and ipconfig

1. On **LON-SVR1**, open a **Windows PowerShell** window and a **cmd** window, and then show the windows side-by-side.
2. Run the following commands in their respective windows:

```
Get-NetIPAddress -InterfaceAlias "Ethernet"  
ipconfig
```

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

## Using Test-NetConnection and ping

1. Run the following commands in their respective windows:

```
Test-NetConnection 172.16.0.1
Ping 172.16.0.1
```

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

## Using Test-NetConnection –TraceRoute and tracert

1. Run the following commands in their respective windows.

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

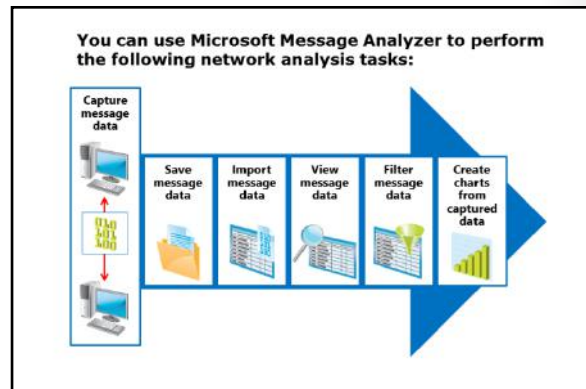
2. Discuss the similarities and differences between the output of each command.

## What is Microsoft Message Analyzer?

*Microsoft Message Analyzer* is a tool used to capture network traffic and then display and analyze information about that traffic. You can use Microsoft Message Analyzer to monitor live network traffic, or to import, aggregate, and analyze data from log and trace files.

You can use Microsoft Message Analyzer to perform the following network analysis tasks:

- Capture message data
- Save message data
- Import message data
- View message data
- Filter message data




Microsoft Message Analyzer uses several built-in Trace Scenarios that you can access through the **Microsoft Message Analyzer** console. Trace Scenarios contain specific capture settings that enable you to quickly start a trace session and then capture the information you need for your troubleshooting task. These Trace Scenarios include predefined capture configuration for Windows Firewall troubleshooting, LAN and wide-area network (WAN) monitoring, and Web Proxy troubleshooting. You can customize Trace Scenarios to remove items that do not require monitoring.

The **Microsoft Message Analyzer** console contains a **Charts** tab that creates charts from captured data. You can customize the parameters and data that will be included in the charts, including network transactions, operations, and the network protocol. Furthermore, you can define different types of chart views, such as Timeline Chart, Pie Chart, Grid View, or Bar Chart. Charts can help you understand incoming trace data by presenting complicated traffic information visually. Often, this feature is helpful when you need to perform mathematical calculations on the trace data, such as the number of retries required for a packet being sent between hosts.

Microsoft Message Analyzer introduces remote live monitoring, which is a feature that allows administrators to monitor the network from a remote host. Administrators can connect to both remote host network adapters and virtual machine network adapters in order to capture and analyze the network traffic data.

Microsoft Message Analyzer is capable of loading data from native Microsoft Message Analyzer files, event tracing log (.etl) files, Network Monitor capture files (.cap), comma-separated values (.csv) files, and several other formats. You can download Microsoft Message Analyzer at no cost from the Microsoft website.

 **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 <http://aka.ms/S20hr4>.

## Demonstration: Using Microsoft Message Analyzer

You can use Microsoft Message Analyzer to capture and view packets transmitted on a network. This allows you to view detailed information that you would not normally be able to see. This type of information can be useful for troubleshooting.

In this demonstration, you will see how to:

- Start a new Capture/Trace in Microsoft Message Analyzer.
- Capture packets from a **Test-NetConnection** request.
- Analyze the captured network traffic.
- Filter the network traffic.

### Demonstration Steps

#### Start a new Capture/Trace in Microsoft Message Analyzer

1. Connect to **LON-SVR2**, if you have not already done so sign in to as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
2. Open a Windows PowerShell prompt and run the following command:

```
Clear-DnsClientCache
```

3. From the **Start** menu, open **Microsoft Message Analyzer**.
4. Start a local trace.

#### Capture packets from a ping request

1. Switch to the Windows PowerShell prompt.
2. At the Windows PowerShell prompt, run following cmdlet:

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

3. Wait for the command to complete, and then in Microsoft Message Analyzer, stop the packet capture.

#### 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. Expand the **ICMP** portion of the packet to view that it includes both **Echo Request** and **Echo Reply** packets. This is a **ping** request that was executed when running the **Test-NetConnection** cmdlet.
3. View the source and destination IP addresses for each packet.

**Filter the network traffic**

1. In Microsoft Message Analyzer, enter the following filter criteria, and then apply the filter:

**\*DestinationAddress == 172.16.0.10**

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

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

**Check Your Knowledge**

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?	
Select the correct answer.	
<input type="checkbox"/>	Restart the server.
<input type="checkbox"/>	Verify the client has a valid IP address.
<input type="checkbox"/>	Verify the client received the proper APIPA address.
<input type="checkbox"/>	Check the IP configuration of the servers to which the client is trying to connect.
<input type="checkbox"/>	All of the above.

## Lab B: Implementing and troubleshooting an IPv4 network

### Scenario

You have recently deployed a server in the North American region that clients from the European region will need to access. Before you tell the users the network is ready, you will use some IPv4 tools to verify that the London domain controller and the Toronto server can communicate.

After you tell the users to start using the Toronto server, you will need to be ready to troubleshoot and fix any communications issue that could arise.

### Objectives

After completing this lab, you will have:

- Verified IPv4 communication.
- Completed troubleshooting IPv4 connectivity issues.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20741A-LON-DC1**, **20741A-LON-CL1**, **20741A-LON-CL2**, **20741A-EU-RTR**, **20741A-NA-RTR**, **20741A-TOR-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you need to use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Microsoft Hyper-V Manager**, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-CL1**, **20741A-LON-CL2**, **20741A-EU-RTR**, and **20741A-TOR-SVR1**.

### Exercise 1: Verify IPv4 communication

#### Scenario

You have recently completed configuring networking between the London headquarters and the new Toronto office. The office workers need to copy files from their client systems in London to the Toronto server. Because this is a new circuit, you need to be ready to troubleshoot any issues that could arise.

The main tasks for this exercise are as follows:

1. Verify IPv4 traffic.
2. Prepare **LON-CL1** for troubleshooting.
3. Prepare **LON-CL2** for troubleshooting.

### ► Task 1: Verify IPv4 traffic

#### Verify that the LON-DC1 server can communicate with the default gateway

1. On **LON-DC1**, open a **Windows PowerShell** window, type the following command, and then press Enter.

```
Test-NetConnection 172.16.0.1
```

2. Review the results.

#### Verify that LON-DC1 can communicate with TOR-SVR1

1. On **LON-DC1**, in the **Windows PowerShell** window, type the following command, and then press Enter.

```
Test-NetConnection -TraceRoute TOR-SVR1.adatum.com
```

2. Review the results.

### ► Task 2: Prepare LON-CL1 for troubleshooting

1. On **LON-CL1**, open **File Explorer** and copy **LON-CL1.ps1** from `\\LON-DC1\Labfiles\Mod01` to the **LON-CL1** desktop.



**Note:** Do not open the file. This script creates the problem that you will troubleshoot and repair in the next exercise. Opening the file can cause issues with the lab tasks.

2. Close **File Explorer**.
3. Right-click the **LON-CL1.ps1** file, and then click **Run with PowerShell**.
4. If prompted to confirm, type **y**, and then press Enter.

### ► Task 3: Prepare LON-CL2 for troubleshooting

1. On **LON-CL2**, copy **LON-CL2.ps1** from `\\LON-DC1\Labfiles\Mod01` to the **LON-CL2** desktop.



**Note:** Do not open the file. This script creates the problem that you will troubleshoot and repair in the next exercise. Opening the file can cause issues with the lab tasks.

2. Close **File Explorer**.
3. Right-click the **LON-CL2.ps1** file and then click **Run with PowerShell**.
4. If prompted to confirm, type **y**, and then press Enter.

**Results:** After completing this exercise, you will have verified that the London computers can communicate with the Toronto server.

## Exercise 2: Troubleshooting IPv4

### Scenario

The two users in London that will be copying files to Toronto are complaining that no one can connect to the Toronto server. Use the IPv4 tools to troubleshoot and resolve the issues.

After some initial investigation, Arnold on LON-CL1 states that he is unable to connect to anything. Amy on LON-CL2 states that she can connect to the London servers but is unable to connect to the Toronto servers.

The main tasks for this exercise are as follows:

1. Troubleshoot IPv4 connectivity between the London clients and the Toronto server.
2. Prepare for the next module.

#### ► Task 1: Troubleshoot IPv4 connectivity between the London clients and the Toronto server

- Use your knowledge of IPv4 to troubleshoot and repair the connectivity problem between the London network and the Toronto network. Consider using any of the Windows PowerShell tools discussed in this module.

**Results:** After completing this lab, you should have resolved all IPv4 connectivity issues.

#### ► Task 2: Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-CL1**, **20741A-LON-CL2**, **20741A-EU-RTR**, and **20741A-TOR-SVR1**.

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

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

## Module Review and Takeaways

### 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?

**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?

**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?

### Best Practice

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 both 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.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
IP conflicts	
Multiple default gateways defined	
Incorrect IPv4 configuration	



## 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
<b>Get-NetIPAddress</b>	Obtains a list of IP addresses that are configured for interfaces	Windows PowerShell
<b>Test-NetConnection</b>	Displays the following: <ul style="list-style-type: none"> <li>• Results of a DNS lookup</li> <li>• Listing of IP interfaces</li> <li>• Option to test a TCP connection</li> <li>• Internet Protocol security (IPsec) rules</li> <li>• Confirmation of connection establishment</li> </ul>	Windows PowerShell
<b>Ipconfig</b>	View network configuration	Command prompt
<b>Ping</b>	Verify network connectivity	Command prompt
<b>Tracert</b>	Verify network path between hosts	Command prompt
<b>Pathping</b>	Verify network path and reliability between hosts	Command prompt
<b>Route</b>	View and configure the local routing table	Command prompt
<b>Telnet</b>	Test connectivity to a specific port	Command prompt
<b>Netstat</b>	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

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 2

## Implementing DHCP

### Contents:

Module Overview	2-1
<b>Lesson 1:</b> Overview of the DHCP server role	2-2
<b>Lesson 2:</b> Deploying DHCP	2-6
<b>Lesson 3:</b> Managing and troubleshooting DHCP	2-15
<b>Lab:</b> Implementing DHCP	2-27
Module Review and Takeaways	2-35

## Module Overview

All network clients need to have unique IP addresses assigned to their network interfaces. Manually assigning addresses and tracking the information can be arduous, even in small networks. Dynamic Host Configuration Protocol (DHCP) plays an important role in a typical network infrastructure. It provides an automated means of distributing important network configuration information to network clients, and it provides configuration information to other network-enabled services. To support and troubleshoot an IP-based network infrastructure, it is important that you understand how to deploy, configure, and troubleshoot the DHCP server role.

### Objectives

After completing this module, you will be able to:

- Explain the DHCP server role.
- Deploy DHCP.
- Manage and troubleshoot DHCP.

## Lesson 1

# Overview of the DHCP server role

You can use the DHCP server role to help simplify client computer configuration by distributing network configuration information to network clients and network-enabled services, such as Windows Deployment Services.

This lesson provides information about the basic function of DHCP, which leases IP addresses and associated information from a defined scope to network clients who request that information. This lesson also describes how leases are generated and maintained.

### Lesson Objectives

After completing this lesson, you will be able to:


- Identify the benefits of DHCP.
- Describe how DHCP allocates addresses.
- Describe how lease generation works.
- Describe how DHCP lease renewal works.

### Benefits of using DHCP

The DHCP protocol simplifies configuration of IP clients in a network environment. If you do not use DHCP, each time you add a client to a network you need to configure its network interface with information about the network on which you installed it, including the IP address, the network's subnet mask, and the default gateway for access to other networks.

When you need to manage many computers in a network, managing them manually is not practical. Many organizations manage thousands of computer devices, including printers, scanners, handhelds, desktop computers, and laptops. Therefore, performing manual management of the network IP configurations for organizations of this size is not feasible.

The DHCP Client service runs on all computers that have their TCP/IP properties set to automatically get an IP Address. The service helps to ensure that all clients have appropriate configuration information, which helps to eliminate human error during configuration. When key configuration information changes in the network, you can update the DHCP clients using the DHCP Server Service, so you do not have to change the information directly on each computer. The DHCP Server service only runs on computers that have the DHCP server role configured.

 **Note:** All Windows-based operating systems are configured to automatically get an IP address after the initial installation of the operating system.

DHCP is also a key service for mobile users who change networks often. DHCP enables network administrators to offer complex network-configuration information to nontechnical users, without users having to manage their network-configuration details.


DHCP reduces the complexity and amount of administrative work by using automatic IP configuration

Automatic IP configuration	Manual IP configuration
Supplies IP addresses automatically	Type IP addresses manually
Ensures correct configuration information	Typing incorrect IP address is a possibility
Updates client configuration automatically	Can result in possible communication and network issues
Eliminates a common source of network problems	Frequent computer moves increase administrative effort

IPv6 is also supported by Microsoft DHCP service

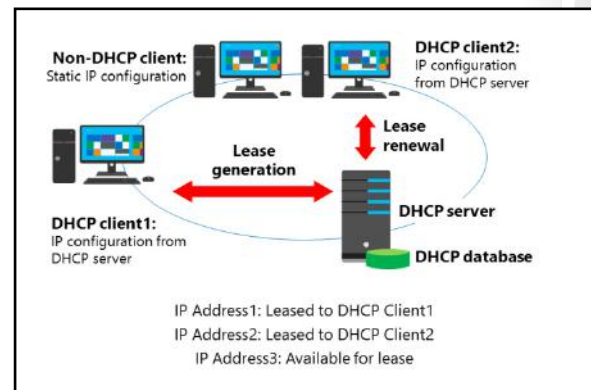
Clients can use the assigned DHCP address for a certain period, known as a *lease*. You can set the lease time to optimize your overall IP address scheme. Clients are programmed to attempt to renew their lease automatically after a specified time, usually after 50 percent of the lease period has passed. As long as there are IP addresses available, the DHCP continues to provide the renewals.

DHCP version 6 (v6) stateful and stateless configurations are supported for configuring clients in an IPv6 environment. Stateful configuration occurs when the DHCPv6 server assigns the IPv6 address to the client, along with additional DHCP data. Stateless configuration occurs when the subnet router assigns the IPv6 address automatically, and the DHCPv6 server only assigns other IPv6 configuration settings.

 **Note:** Although IPv6 is supported by the Microsoft DHCP service, most organizations use IPv4 as their network protocol. IPv6 has not yet been widely implemented. IPv6 uses a 128-bit addressing scheme whereas IPv4 uses a 32 bit address.

## How DHCP allocates addresses

DHCP allocates IP addresses on a dynamic basis, otherwise known as a *lease*. Although you can set the lease duration anywhere from a few minutes to unlimited, you will typically set the duration for not more than a few hours or days. The default lease time is eight days for wired clients and three days for wireless clients. IP addresses are handed out to requesting network clients from a pool of addresses that you define. When a client requests an IP address, the DHCP server offers the next available IP address from the pool. It is possible to reserve particular IP addresses for specific clients based on the media access control (MAC) address of the client's network interface.



DHCP uses IP broadcasts to initiate communications. Therefore, DHCP servers are limited to communication within their IP subnet. This means that in many networks, there is a DHCP server for each IP subnet.

By default, all Microsoft operating systems are configured to obtain an IP address automatically. For a computer to be a DHCP client, you must configure it to obtain an IP address automatically. In a network where a DHCP server is installed, DHCP clients respond to DHCP broadcasts.

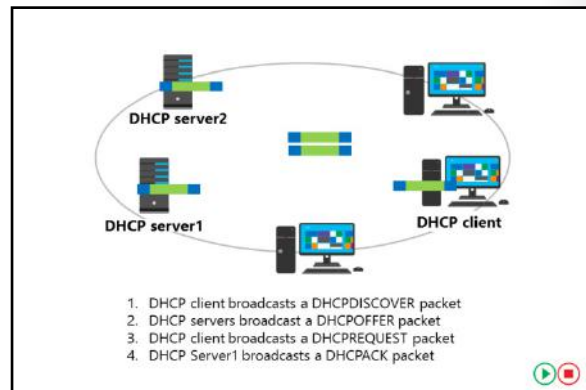
If you configure a computer with an IP address, that computer has a static IP address. Therefore, it is a non-DHCP client, and it does not communicate with a DHCP server. Servers and printers are examples of network clients that will usually have static IP addresses.

## How DHCP lease generation works

DHCP uses a four-step, lease-generation process to assign an IP address to clients. Understanding how each step of this process works helps you troubleshoot problems when clients cannot obtain an IP address.

The following are the four steps of the DHCP lease-generation process:

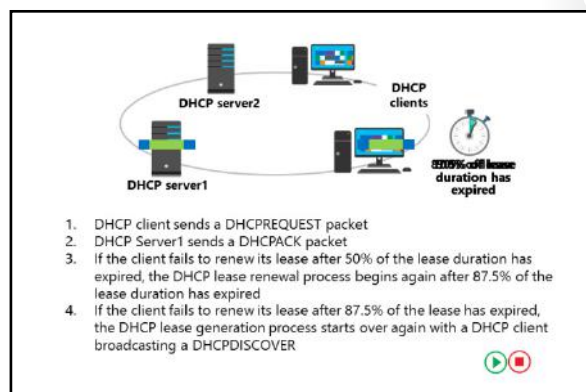
1. The DHCP client broadcasts a DHCPDISCOVER packet to every computer in the subnet. The only computers that respond are computers that have the DHCP server role, or computers or routers that are running a DHCP relay agent. In the latter case, the DHCP relay agent forwards the message to the DHCP server it is configured to relay requests to.
2. A DHCP Server responds with a DHCPOFFER packet, which contains a potential address for the client.
3. The client receives the DHCPOFFER packet. It might receive packets from multiple servers. If it does, it usually selects the server that made the fastest response to its DHCPDISCOVER, which typically is the DHCP server closest to the client. The client then broadcasts a DHCPREQUEST that contains a server identifier. This informs the DHCP servers that receive the broadcast which server's DHCPOFFER the client has chosen to accept.
4. The DHCP servers receive the DHCPREQUEST. Servers that the client has not accepted use this message as the notification that the client declines that server's offer. The chosen server stores the IP address client information in the DHCP database and responds with a DHCPACK message. If the DHCP server cannot provide the address that was offered in the initial DHCPOFFER, the DHCP server sends a DHCPNAK message.



## How DHCP lease renewal works

When the DHCP lease reaches 50 percent of the lease time, the client automatically attempts to renew the lease. This process occurs in the background. It is possible for a computer to have the same DHCP-assigned IP address for a long time, if the computer is not restarted. This is because the computer renegotiates the lease periodically.

To attempt to renew the IP address lease, the client sends a unicast DHCPREQUEST message. The server that leased the IP address originally sends a DHCPACK message back to the client. This message contains any new parameters that have changed since the original lease was created. Note that these packets do not broadcast, because the client at this point has an IP address that it can use for unicast communications.



If the DHCP client cannot contact the DHCP server, then the client waits until 87.5 percent of the lease time expires. At this point, the client sends a DHCPREQUEST broadcast (rather than a unicast) to obtain a renewal, and the request goes to all DHCP servers, not just the server that provided the original lease. However, this broadcast request is for a renewal, not a new lease.

The previous topic, "How DHCP Lease Generation Works," detailed that when a renewal is unsuccessful—if 100 percent of the lease time has expired—the client computer attempts to obtain an IP configuration from any DHCP server. Every time a client restarts within the lease period, it contacts the configured default gateway. If the gateway does not respond, the client considers itself to be on a new subnet and enters the discovery phase.

Because client computers might be moved while they are turned off, for example a laptop computer that is plugged into a new subnet, client computers also attempt renewal during the startup process, or when the computer detects a network change. If renewal is successful, the lease period is reset.

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

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

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

## Lesson 2

# Deploying DHCP

As a first step to implementing a DHCP solution, you will need to know how to perform a proper installation and authorization of a DHCP server. You also will need to understand the purpose of relay agents in a multi-subnet environment.

This lesson covers the process of installing and configuring DHCP. It describes how to install the DHCP server role and create scopes with various network configuration options. It also discusses DHCP relay agents and the concept of authorization of DHCP servers.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to install and configure DHCP.
- Explain the process of DHCP server authorization.
- Describe how to install a DHCP server and perform post installation tasks.
- Describe how to allocate and manage IPv4 addresses.
- Describe how to configure DHCP options.
- Describe how to configure a DHCP server.
- Describe how a DHCP relay agent works.

### Installing and configuring the DHCP server role

The DHCP server role can only be installed on Windows Server operating systems. You can install the DHCP server on a domain controller, but any server running Windows Server can host the DHCP server. For example, a branch office file and print server might also act as the local DHCP server. Local administrative rights are required to perform the installation, and the server must have a static IP address.



**Note:** You should not install the DHCP server on servers that are performing specialized functions such as hosting Web applications, hosting Microsoft Exchange or hosting Microsoft SQL Server.

- You can install the DHCP server role by using:
  - The Add Roles and Features Wizard in server manager
  - Windows PowerShell:
    - **Add-WindowsFeature DHCP**
- The server hosting DHCP requires a static IP address
- Post installation tasks include
  - Creating DHCP security groups
  - Restarting the DHCP Server service
  - Authorizing the DHCP server in AD DS

You can install the DHCP server role by using the Add Roles and Features Wizard in the Server Manager console, or by using the following Windows PowerShell command:

```
Add-WindowsFeature DHCP
```

If you want to install the DHCP management console while installing the DHCP server role, you would add the *IncludeManagementTools* parameter.

```
Add-WindowsFeature -IncludeManagementTools DHCP
```



Immediately after installing the DHCP server role you must complete the post-deployment configuration of the DHCP server. You can accomplish this by using the **DHCP Post-Install Configuration Wizard**. The wizard helps you perform the following steps to complete the configuration:

- Create the following Active Directory Domain Services (AD DS) security groups for delegation of DHCP server administration:
  - DHCP Administrators
  - DHCP Users
- Authorize DHCP server on the target computer if the computer is domain joined. Then you must restart the DHCP server service for the security groups to become effective.

You also can perform these post-installation tasks by running the following commands:

- Create the security groups

```
Netsh DHCP Add SecurityGroups
```

- Restart the service. You must perform this step.

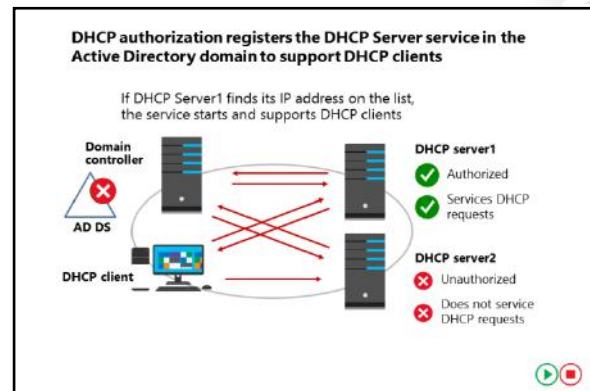
```
Restart-Service DHCPserver
```

- Authorize the DHCP server in AD DS

```
Add-DHCPserverinDC <hostname or IP address of DHCP server>
```

## DHCP server authorization

DHCP communication typically occurs before any user or computer authentication. Therefore, because the DHCP protocol is based on IP broadcasts, an unknown DHCP server can provide invalid information to clients. You can avoid this by authorizing the server. The domain administrator uses a process called DHCP authorization to register the DHCP Server in the Active Directory domain before it can support DHCP clients. Authorizing the DHCP server is one of the post-installation tasks that you must perform after installing the DHCP server.



### Active Directory requirements

You must authorize the Windows Server 2016 DHCP server role in AD DS before it can begin leasing IP addresses. It is possible to have a single DHCP server providing IP addresses for subnets that contain multiple Active Directory domains. Because of this, you must use an Enterprise Administrator account to authorize the DHCP server.

### Standalone DHCP server considerations

A *standalone DHCP server* is a computer that is running Windows Server 2016, that is not part of an Active Directory domain, and that has the DHCP server role installed and configured. If the standalone DHCP server detects an authorized DHCP server in the domain, it does not lease IP addresses and automatically shuts down.

## Unauthorized DHCP servers

Many network devices have built-in DHCP server software. As such, many routers and firewalls can act as a DHCP server, but often these servers do not recognize DHCP-authorized servers, and might lease IP addresses to clients. In this situation, you must perform an investigation to detect unauthorized DHCP servers, whether they are installed on devices or on third-party servers. Once you detect unauthorized DHCP servers, you should disable the DHCP service or functionality on them. You can find the IP address of the DHCP server by issuing the **ipconfig /all** command on the DHCP client computer.

## Demonstration: Install a DHCP server and performing post-installation tasks

In this demonstration you will learn how to:

- Install the DHCP server role.
- Perform post-installation tasks.

### Demonstration Steps

#### Install the DHCP server role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open **Server Manager**, and then use the **Add Roles and Features Wizard** to install the DHCP Server role. Accept all the default settings.

#### Perform the post-installation tasks

1. Click the **Notifications** icon in the top menu bar, and then click the **Complete DHCP configuration** link.
2. Complete the **DHCP Post-Install configuration wizard** by accepting all the default settings, and then close the wizard.
3. Restart the DHCP Server service.

## Allocating and managing IPv4 addresses with DHCP

You need to configure DHCP servers with the range of IP addresses and other network information that they will distribute to network clients. These ranges of IP addresses are called *scopes*. After the initial configuration of the DHCP server, the next thing you must do is create a scope.

### DHCP scopes

A *DHCP scope* is a range of IP addresses that are available for lease and that a DHCP server manages. A DHCP scope typically is confined to the IP addresses in a given subnet, though a DHCP server could host scopes for multiple different subnets. Those addresses would be distributed to clients on other subnets via DHCP relay agents.

- You must create scopes to define the network information that will be distributed to clients
- A scope must contain:
  - A range of IP addresses
  - A subnet mask
  - A lease duration
- A scope might contain:
  - Default gateway address
  - DNS server and suffix
  - Other network options
- IP addresses can be reserved based on the MAC address of the client network interface

For example, a DHCP scope for the network 192.168.1.0/24 (subnet mask of 255.255.255.0) can support a range from 192.168.1.1 through 192.168.1.254. When a computer or device on the 192.168.1.0/24 subnet requests an IP address, the scope that defined the range in this example allocates an address between 192.168.1.1 and 192.168.1.254.

In many scenarios the scope will not be assigned all the IP addresses in a given subnet. Usually a number of IP addresses are excluded from the scope so that they are available for assignment as static addresses. For example, the first twenty addresses of the scope might be excluded and then statically assigned to routers, printers, and servers on the subnet.

### Creating and configuring DHCP scopes

To create and configure a scope, you must define the following properties:

- **Name and description.** This property identifies the scope. The name is a mandatory.
- **IP address range.** This property lists the range of addresses that can be offered for lease. This property is mandatory.
- **Subnet mask.** This property is used by client computers to determine their location in the organization's network infrastructure. This property is mandatory.
- **Exclusions.** This property lists single addresses or blocks of addresses that fall within the IP address range, but that will not be offered for lease. This property is optional.
- **Delay.** This property is the amount of time to delay before sending DHCP OFFER. The default setting is 0 milliseconds.
- **Lease duration.** This property lists the lease duration. Use shorter durations for scopes that have limited IP addresses, and use longer durations for more static networks. The default setting is 8 days.
- **Options.** You can configure many optional properties on a scope, but typically you configure the following properties:
  - Option 003 – Router (the default gateway for the subnet)
  - Option 006 – DNS servers
  - Option 015 – DNS suffix
- **Activation.** The scope needs to be activated before it can hand out IP addresses.

### Creating DHCP scopes using Windows PowerShell

In Windows Server 2012, Microsoft introduced several new Windows PowerShell cmdlets to configure and manage DHCP servers. Each cmdlet has parameters that need to be met, depending on actions to be taken. Many of the new cmdlets address scope creation and management, which the following table shows.

Cmdlet name	Description
<b>Add-DhcpServerv4Scope</b>	Adds an IPv4 scope on the DHCP server service.
<b>Get-DhcpServerv4Scope</b>	Returns the IPv4 scope configuration of the specified scopes.
<b>Get-DhcpServerv4ScopeStatistics</b>	Gets the IPv4 scope statistics corresponding to the IPv4 scope identifiers specified for a DHCP server service.
<b>Remove-DhcpServerv4Scope</b>	Deletes the specified IPv4 scopes from the DHCP server service.

Cmdlet name	Description
<b>Set-DhcpServerv4Scope</b>	Sets the properties of an existing IPv4 scope on the DHCP server service.



**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>

### DHCP reservations

If you want a computer or device to obtain a specific address from the scope range, you can permanently reserve that address to be assigned to that device in DHCP. Reservations are useful for tracking IP addresses assigned to devices such as printers. To create a reservation, select the scope in the DHCP console, and from the **Action** menu, click **New Reservation**. You need to provide the following information to create the reservation:

- Reservation name. A friendly name to reference the reservation.
- IP address. The IP address from the scope that you want to assign to the device.
- MAC address. The MAC address of the interface you want to assign the address to.
- Description. An optional field to provide a comment about the reservation.

### Configuring DHCP options

DHCP servers can configure more than just an IP address. They also provide information about network resources, such as Domain Name System (DNS) servers and the default gateway. DHCP options are values for common configuration data that apply to the server, scopes, reservations, and class options. You can apply DHCP options at the server, scope, class, and reservation levels. An option code identifies the DHCP options, and most option codes come from the RFC documentation found on the Internet Engineering Task Force (IETF) website.

- DHCP options:
  - Are values for common configuration data
  - Can be applied to the server, scope, class, and reservation level
- Common scope options include:
  - Router (Default gateway)
  - DNS domain name
  - DNS servers

### Common DHCP options

The following table lists the common option codes that Windows-based DHCP clients request.

Option code	Name
1	Subnet mask
3	Router
6	DNS servers

Option code	Name
15	DNS domain name
31	Perform router discovery
33	Static route
43	Vendor-specific information
47	NetBIOS scope ID
51	Lease time
58	Renewal (T1) time value
59	Rebinding (T2) time value
60	Pre-Boot Execution (PXE) client
66	Boot server host name
67	Bootfile name
249	Classless static routes

### PXE Boot options

PXE-enabled network cards add the DHCP option 60 to their discover packets. Normally, DHCP clients send a DHCP option 67 packet, and then DHCP servers return a DHCP 68 option offer. The ports that DHCP uses also are used by the Windows Deployment Services PXE server function. Therefore, if you deploy DHCP and a PXE server on the same machine, you must set DHCP to make offers that also include the 60 option. A DHCP server then makes the DHCP 60 offer back to the client. You need to set DHCP options 60 (PXE Client), 66 (Boot Server Host Name), and 67 (Bootfile Name). You can set options 66 and 67 in the Scope Options window in the DHCP console, but you must set the 60 option via the command line.

The following code sample lists the procedure:

```
C:\WINDOWS\system32>netsh
netsh>dhcp
netsh dhcp>server \\<server_machine_name>
netsh dhcp>add optiondef 60 PXEClient String 0 comment=PXE support
netsh dhcp>set optionvalue 60 STRING PXEClient
netsh dhcp>exit
```

After this code has run, a PXE server then sends back boot server and boot information to the PXE-enabled network client. This enables it to accept an operating system installation.

### How DHCP options are applied

Options are applied in an order of precedence at four different levels. Going from least specific to most specific, they are:

1. Server level. Assigns a server-level option to all DHCP clients of the DHCP server
2. Scope level. Assigns a scope-level option to all clients of a scope. Scope options override server options

3. Class level. Assigns a class-level option to all clients that identify themselves as members of a class. Class options override both scope and server options
4. Reserved client level. Assigns a reservation-level option to one DHCP client. Reserved client options apply to devices that have a DHCP reservation

If you apply DHCP option settings at each level and they conflict, then the option that you applied last overrides the previously-applied setting. For example, if the default gateway is configured at the scope level and a different default gateway is applied for a reserved client, then the reserved client setting becomes the effective setting.

## Demonstration: Configure a DHCP server

In this demonstration you will learn how to:

- Create a DHCP scope.
- Configure DHCP options.
- Create a DHCP reservation.

### Demonstration Steps

#### Create a DHCP scope

1. In **Server Manager**, start the **DHCP management** console.
2. Click the **lon-svr1.adatum.com** server icon to open the **IPv4** node.
3. Right-click the **IPv4** node, and create a new scope with the following parameters:
  - o Name: **Adatum**
  - o Start IP address: **10.0.0.100**
  - o End IP address: **10.0.0.150**
  - o Subnet mask: **255.255.255.0**
  - o Lease Duration: **1 Day**
4. Do not configure DHCP options at this time.

#### Configure DHCP options

1. Expand the **IPv4** node, expand the **Scope [10.0.0.0] Adatum** folder, and then select the **Scope Options** folder.
2. Right-click the **Scope Options** folder, and then configure the following options:
  - o 003 Router: **10.0.0.1**
  - o 006 DNS Servers: **172.16.0.10**
3. Activate the scope.

#### Create a DHCP reservation

- Create a new reservation with the following properties:
  - o Reservation name: **Sales printer**
  - o IP address: **10.0.0.120**
  - o MAC address: **00-14-6D-01-73-6B**

## What is a DHCP relay agent?


When initially attempting to obtain an IP address, DHCP clients use IP broadcasts to initiate communications. Therefore, DHCP servers and clients can communicate only within their IP subnet. This means that in many networks there is a DHCP server for each IP subnet. If there are a large number of subnets, it might be expensive to deploy servers for every subnet. However, you can use a single DHCP server to service collections of smaller subnets.

For the DHCP server to respond to a DHCP client request, it must be able to receive DHCP requests.

You can enable this by configuring a DHCP relay agent on each subnet. A *DHCP relay agent* is a computer or router that listens for DHCP broadcasts from DHCP clients, and then relays them to DHCP servers in different subnets.

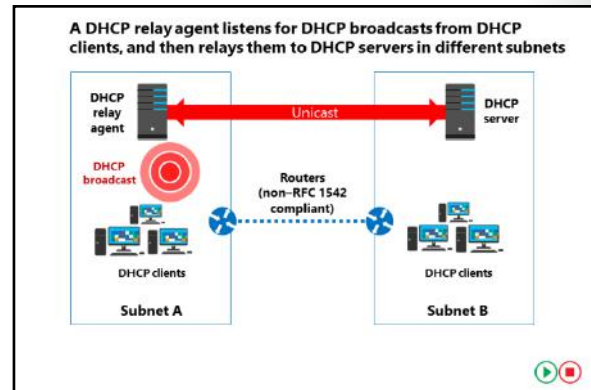
You configure the DHCP relay agent to point to the IP address of the DHCP server in the remote subnet. Once configured, the DHCP relay agent will relay any DHCP broadcast packets into unicast packets. These packets are sent to the relay agent's listed DHCP server, which typically is on another IP subnet across a router. The DHCP server sends DHCP offer and acknowledge packets back to the relay agent by using unicast broadcast. The relay agent then broadcasts these packets on the local subnet, so the client needing an address can receive it without having to change its core processing.

You also can relay DHCP packets into other subnets by using a router that is compatible with RFC 1542. This means that the router, upon receiving a DHCP broadcast packet, can replay the DHCP broadcasts on the other subnets to which it connects. Because this DHCP relay happens within the router, you do not have to create a specific DHCP relay agent on a server running Windows Server. Most modern routers have RFC 1542 capabilities. However, you should consult your router's documentation to learn the specific settings to implement this.

 **Note:** It is common to have a wireless access point act as either a DHCP server or as a relay agent for wireless network IP address requests.

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
Any domain administrator can authorize a DHCP server.	



**Check Your Knowledge**

Question	
In case of a conflict between DHCP options, which level will take precedence?	
Select the correct answer.	
<input type="checkbox"/>	Server level
<input type="checkbox"/>	Class level
<input type="checkbox"/>	Scope level
<input type="checkbox"/>	Client reservation level



## Lesson 3

# Managing and troubleshooting DHCP

You need to be able to provide some protection from unknown computers on your network, and be able to make the DHCP service highly available because if this service fails, client computers will eventually lose access to the network.

This lesson discusses the security options for DHCP and some of the advanced features such as policy-based assignments. It also discusses ways to make the DHCP service highly available to clients. DHCP uses a database to track client information. This lesson also describes database maintenance techniques and how to troubleshoot DHCP issues.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the DHCP security options.
- Describe the advanced DHCP configuration options.
- Describe how to configure superscopes and multicast scopes.
- Describe the high availability options for DHCP.
- Explain how DHCP failover works.
- Describe how to configure DHCP failover.
- Describe how to maintain a DHCP database.
- Describe how to troubleshoot DHCP.

### What are DHCP security options?

Because DHCP is an unauthenticated protocol, you must take precautions to ensure that only valid clients are receiving network information. You also should take precautions to ensure that the names that your client computers have registered in your organization's DNS are protected.

#### Limit access to the network

DHCP by itself can be difficult to secure. It is designed to work before the necessary information is in place for a client computer to authenticate with a domain controller. Therefore, you need to take precautions to prevent unauthorized computers from obtaining a lease with DHCP.

- Limit physical access to the network by:
  - Disconnecting unused LAN drops
  - Require authenticated layer 2 connections
- Enable DHCP auditing to track DHCP usage
- DHCP name protection:
  - Prevents Windows operating systems from having their DNS name registration overwritten by non-Windows operating systems using the same name
  - Uses a DHCPID resource record to track the devices that originally requested the DNS name registration

Basic precautions that you should take to limit unauthorized access include:

- Ensuring that you reduce physical access. If users can access an active network connection to your network, their computers will be able to obtain an IP address. If a network port is not being used, you should disconnect it physically from the switching infrastructure.
- Requiring authenticated Layer 2 connections to the network: Most enterprise hardware switches now support Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.1X authentication. This allows for port-level user authentication. Secure wireless standards, such as Wi-Fi Protected Access (WPA) Enterprise and WPA2 Enterprise, also use 802.1X authentication.

### Enable DHCP auditing

Enabling audit logging on all DHCP servers. This can provide an historical view of activity, in addition to allowing you to trace when an unauthorized user obtained an IP address in the network. Make sure to review the audit logs at regular intervals.

### DHCP name protection

During dynamic IP address allocation, the DHCP server creates resource records automatically for DHCP clients in the DNS database. You should protect the names that DHCP registers in DNS on behalf of other computers or systems, from being overwritten by non-Windows operating systems that use the same names. In addition, you also should protect the names from being overwritten by systems that use static addresses that conflict with DHCP-assigned addresses when they use unsecure DNS, and DHCP is not configured for conflict detections. For example, a UNIX-based system named Client1 could potentially overwrite the DNS address that was assigned and registered by DHCP on behalf of a Windows-based system also named Client1. DHCP Name Protection addresses this issue.

*Name squatting* is the term used to describe the conflict that occurs when one client registers a name with DNS but that name is already in use by another client. This problem causes the original machine to become inaccessible, and it typically occurs with systems that have the same names as Windows operating systems. DHCP Name Protection addresses this by using a resource record known as a Dynamic Host Configuration Protocol Information (DHCID) to track which machines originally requested which names. The DHCP server provides the DHCID record, which is stored in DNS. When the DHCP server receives a request from a machine with an existing name for an IP address, the DHCP server can refer to the DHCID in DNS to verify that the machine that is requesting the name is the original machine that used the name. If it is not the same machine, then the DNS resource record is not updated.

You can implement name protection for both IPv4 and IPv6. In addition, you can configure DHCP Name Protection at both the server level and the scope level. Implementation at the server level will only apply for newly created scopes.

To enable DHCP Name Protection for an IPv4 or IPv6 node:

1. Open the **DHCP** console.
2. Right-click the **IPv4** or **IPv6** node, and then open the **Property** page.
3. Click **DNS**, click **Advanced**, and then select the **Enable Name Protection** check box.

To enable DHCP Name Protection for an individual scope:

1. Expand the **IPv4** or **IPv6** node, right-click the scope, and then open the **Property** page.
2. Click **DNS**, click **Advanced**, and then select the **Enable Name Protection** check box.

## Advanced options for configuring DHCP

DHCP supports a number of ways to distribute IP addresses based on attributes of the device requesting the address. These include user class and vendor class attributes, and policy-based IP assignments.

### DHCP user classes

DHCP user classes allow you to define and assign a user class ID to a client. You can define new user classes on the DHCP server, and then set on the client computer's network interface. A network interface can only belong to one user class. The DHCP server then can allocate an IP address based on the user class ID field presented in the DHCP request from that client. For example, you might want to specify a different range of IP addresses for clients that have been assigned a user class that you defined named **Sales**.

All Windows clients initially belong to the default user class. To implement user classes, you must:

1. Define a new user class on the **IPv4** node of the DHCP server.
2. Assign the user class to the client device.
3. Assign DHCP options to the user class via DHCP policy-based assignments

You can define user classes only for the entire IPv4 node and not for individual scopes.

You cannot define user classes for the IPv6 node.

Use the following command from an elevated command prompt on the client computer to set the user class:

```
Ipconfig /setclassid <"name of adapter"> <name of user class>
```

For example, to set the user class to Sales on the network interface named LAN, the command would be:

```
Ipconfig /setclassid "LAN" Sales
```

### DHCP vendor classes

Vendor classes are used to assign options to clients based on a common vendor type. In order to receive specific vendor options, the client must identify itself as belonging to that vendor class by putting a value in the vendor class identifier field when requesting a lease from the DHCP server. Vendor classes are determined by the device vendor and are implemented via DHCP policy-based assignments.

### DHCP policy-based assignments

DHCP policies allow you to create policies that deliver specific IP address and option information to clients based on a set of conditions. This enables you to have different types of IP devices receive addresses and other options from a subset of IP addresses in the scope range. This strategy can assist you in identifying the device type based on the IP address. For example, if your DHCP subnet is the 192.168.1.0 network, you could use policies to dictate that IP-based phones receive addresses from 192.168.1.50 – 192.168.1.100 and have long leases, and laptops receive addresses from 192.168.1.101-192.168.1.200 with much shorter leases.


Policy-based assignments allow you to base IP assignment on the following criteria:

- Vendor class (defined by hardware vendors)
- User class (defined by Administrators)
- MAC address
- FQDN
- Relay agent information

DHCP policies are defined by rules and you can have multiple policies. Policies have the following characteristics:

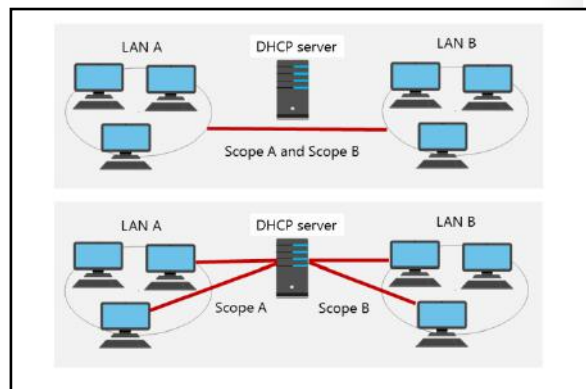
Characteristic	Description
Policy level	You can apply policies at the server or scope level
Processing order	A policy has a unique processing order. Lower numbered policies are applied before higher numbered policies
Conditions	<p>If the DHCP request from the client matches the conditions specified, then the settings of the policy will be applied. Conditions can be combined with Boolean <b>AND</b> or <b>OR</b> statements. Conditions criteria include:</p> <ul style="list-style-type: none"> <li>• Vendor class</li> <li>• User class</li> <li>• MAC address</li> <li>• Client identifier</li> <li>• Fully qualified domain name (FQDN)</li> <li>• Relay agent information</li> </ul>
Settings	Settings are the network configurations that are delivered to the client
Enabled/Disabled	The policy state is either enabled or disabled. Disabled policies are not processed

You create IP based policies in the **Policies** folder in the **IPv4** node, or in the **Policies** folder at the scope level. The **DHCP Policy Configuration Wizard** guides you through the process of creating a policy.

 **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>

## Configuring superscopes and multicast scopes

You can configure advanced DHCP scope designs, called *superscopes*. A superscope is a collection of individual scopes that are grouped together for administrative purposes. This allows client computers to receive an IP address from multiple logical subnets even when the clients are located on the same physical subnet. You can create a superscope only if you have two or more IP scopes created already in DHCP. You can use the **New Superscope Wizard** to select the scopes that you wish to combine to create a superscope.



## Benefits of superscopes

A superscope is useful in several situations. For example, if a scope runs out of addresses and you cannot add more addresses from the subnet, you can instead add a new subnet to the DHCP server. This scope will lease addresses to clients in the same physical network, but the clients will be in a separate network logically. This is known as *multinetting*. Once you add a new subnet, you must configure routers to recognize the new subnet so that you ensure local communications in the physical network.

A superscope is also useful when you need to move clients gradually into a new IP numbering scheme. Having both numbering schemes coexist for the original lease's duration means that you can move clients into the new subnet transparently. When you have renewed all client leases in the new subnet, you can retire the old subnet.


## Multicast scopes

A *multicast scope* is a collection of multicast addresses from the class **D** IP address range of 224.0.0.0 to 239.255.255.255 (224.0.0.0/3). These addresses are used when applications need to communicate with numerous clients efficiently and simultaneously. This is accomplished with multiple hosts that listen to traffic for the same IP address.

A multicast scope is commonly known as a *Multicast Address Dynamic Client Allocation Protocol (MADCAP)* scope. Applications that request addresses from these scopes need to support the MADCAP application programming interface (API). Windows Deployment Services is an example of an application that supports multicast transmissions. Multicast scopes allow applications to reserve a multicast IP address for data and content delivery.

## High availability options for DHCP

DHCP is a critical component in most modern networks and needs to be available when clients request IP addresses. Options for making DHCP highly available include using server clusters and split scopes and DHCP Failover.

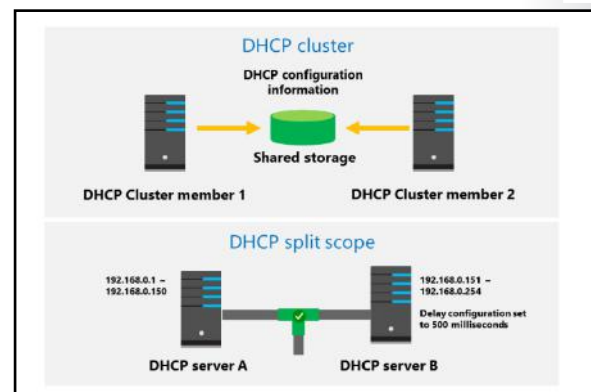
 **Note:** DHCP failover is discussed in the next topic.

### DHCP clustering

The DHCP server can run on Windows servers in a two-member failover cluster. Both members of the cluster would have the DHCP server installed with identical scopes. In this scenario the DHCP configuration information is stored on shared storage. If one member of the cluster should fail the other member in the cluster would detect the failure and start the DHCP service on the surviving member of the cluster.

### Split scopes

A split scope scenario also involves two DHCP servers. In this case each DHCP server controls a part of the entire range of IP addresses and both servers are active on the same network. For example, if your subnet is 192.168.0.0, you might assign an IP address range of 192.168.0.1–192.168.0.150 to DHCP server A—the primary server—and assign 192.168.0.151–192.168.0.254 to DHCP server B, which acts as a DHCP



secondary server. You can control which server is the primary server assigning addresses by setting the **Delay configuration** attribute on the **Advanced** tab of the scope properties on the secondary server. This ensures that the primary server will be the first server to respond to client requests. If the primary server fails and stops responding to requests, then the secondary server's response will be the one the client accepts.

## What is DHCP failover?


DHCP manages the distribution of IP addresses in TCP/IP networks of all sizes. When this service fails, clients lose connectivity to the network and all of its resources. DHCP failover is a feature in Windows Server 2016 that addresses this issue.

### DHCP failover

DHCP clients renew the leases of their IP addresses at regular, configurable intervals. If the DHCP service fails, the leases time out and clients no longer have IP addresses. In the past, DHCP failover was not possible because DHCP servers were independent and unaware of each other.


Therefore, configuring two separate DHCP servers to distribute the same pool of addresses could lead to duplicate addresses. Additionally, providing redundant DHCP services required that you configure clustering and perform a significant amount of manual configuration and monitoring.

The new DHCP failover feature in Windows server 2016 enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes. Therefore, you now can configure two DHCP servers to replicate lease information. If one of the servers fails, the other server services the clients for the entire subnet.

 **Note:** You can only configure two DHCP servers for failover, and you can configure these only for IPv4 scopes and subnets.

### Configuring DHCP failover

To configure DHCP failover, you need to establish a failover relationship between the two DHCP servers. You also must give this relationship a unique name. The failover partners exchange this name during configuration. This enables a single DHCP server to have multiple failover relationships with other DHCP servers so long as they all have unique names. To configure failover, use the **Configuration Failover Wizard**, which you launch by right-clicking the IP node or the scope node.

 **Note:** DHCP failover is time sensitive. You must synchronize time between the partners in the relationship. If the time difference is greater than one minute, the failover process will halt with a critical error.

#### • DHCP failover:

- Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes
- Requires failover relationships to have unique names
- Supports the hot standby mode and the load sharing mode

#### • When you use DHCP failover:

- The MCLT determines when a failover partner assumes control of the subnet or scope
- The auto state switchover interval determines when a failover partner is considered to be down
- Message authentication can validate the failover messages
- Firewall rules are auto-configured during DHCP installation

You can configure failover in one of the two modes listed in the following table.

Mode	Characteristics
Load sharing	This is the default mode. In this mode both servers supply IP configuration to clients simultaneously. The server that responds to IP configuration requests depends on how the administrator configures the load distribution ratio. The default ratio is 50:50.
Hot standby	<p>In this mode, one server is the primary server and the other is the secondary server. The primary server actively assigns IP configurations for the scope or subnet. The secondary DHCP server assumes this role only if the primary server becomes unavailable. A DHCP server can simultaneously act as the primary for one scope or subnet, and be the secondary for another.</p> <p>Administrators must configure a percentage of the scope addresses to be assigned to the standby server. These addresses are supplied during the Maximum Client Lead Time (MCLT) interval if the primary server is down. The default MCLT value is 5 percent of the scope. The secondary server takes control of the entire IP range after the MCLT interval has passed.</p> <p>Hot Standby mode is best suited to deployments in which a disaster recovery site is located at a different location. This way the DHCP server will not service clients unless there is a main server outage.</p>

### MCLT

The administrator configures the MCLT parameter to determine the amount of time a DHCP server should wait when a partner is unavailable, before assuming control of the address range. This value cannot be zero, and the default is one hour.

### Auto state switchover interval

A communication-interrupted state occurs when a server loses contact with its partner. Because the server has no way of knowing what is causing the communication loss, it remains in this state until the administrator manually changes it to a partner down state. The administrator also can enable automatic transition to partner down state by configuring the auto state switchover interval. The default value for this interval is 10 minutes.

### Message authentication

Windows Server 2012 enables you to authenticate the failover message traffic between the replication partners. The administrator can establish a shared secret—much like a password—in the **Configuration Failover Wizard** for DHCP failover. This validates that the failover message comes from the failover partner.

### Firewall considerations

DHCP uses Transmission Control Protocol (TCP) port 647 to listen for failover traffic. The DHCP installation creates the following inbound and outbound firewall rules:

- Microsoft-Windows-DHCP-Failover-TCP-In
- Microsoft-Windows-DHCP-Failover-TCP-Out

## Demonstration: Configure DHCP failover

In this demonstration, you will learn how to configure a DHCP failover relationship.

### Demonstration Steps

1. On **LON-DC1**, start the **DHCP management** console.
2. Select and then right-click **IPv4**, and then click **Configure Failover**.
3. Create a failover relationship with the following parameters:
  - o Partner server: **172.16.0.11**
  - o Relationship name: **Adatum**
  - o Maximum Client Lead Time: **15 minutes**
  - o Mode: **Load balance**
  - o Load Balance Percentage: **50%**
  - o State Switchover Interval: **60 minutes**
  - o Shared Secret: **Pa\$\$w0rd**

## Maintaining the DHCP database

The DHCP database is a dynamic database containing data that relates to scopes, address leases, and reservations. The database also contains the data file that stores both the DHCP configuration information and the lease data for clients that have leased an IP address from the DHCP server. By default, the DHCP database files are stored in the

**%systemroot%\System32\Dhcp** folder.

The following table describes the DHCP database files.

- The DHCP database (Dhcp.mdb) contains information relating to scopes, leases, reservations, and all other configuration information
- The default location of DHCP database files is **%systemroot%\system32\DHCP**
- The DHCP database is automatically backed up every 60 minutes, or can be backed up manually
- You can reconcile the DHCP database to repair inconsistencies
- You can move the DHCP database to a new DHCP server when the DHCP Server service is moved

File	Description
Dhcp.mdb	Dhcp.mdb is the DHCP server database file.
tmp.edb	Tmp.edb is a temporary file that the DHCP database uses as a swap file during database index maintenance operations. Following a system failure, tmp.edb sometimes remains in the <i>Systemroot\System32\Dhcp</i> directory.
J50.log and J50res#####.jrs	J50.log and J50res#####.jrs are logs of all database transactions. The DHCP database uses this log to recover data when necessary.
J50.chk	J50.chk is a checkpoint file.



## Backing up and restoring a DHCP database

The DHCP database is automatically backed up every 60 minutes. You can manually backup the database anytime in the DHCP management console by right-clicking the DHCP server and selecting **Backup**.

The following items are backed up:

- All scopes
- Reservations
- Leases
- All options, including server options, scope options, reservation options, and class options
- All registry keys and other configuration settings that are set in DHCP server properties.

You can initiate the database restore process from the DHCP console by right-clicking the DHCP server, and then clicking **Restore**. During the restore process the DHCP server service will be restarted.

## Reconciling the DHCP database

Over time the DHCP database can develop inconsistencies. Reconciliation allows you to initiate a database consistency check. Reconciling scopes can fix inconsistencies that can affect client computers.

The DHCP Server service stores scope IP address lease information in two forms:

- Detailed IP address lease information, which the DHCP database stores
- Summary IP address lease information, which the server's Registry stores

When you are reconciling scopes, the detail and summary entries are compared to find inconsistencies.

To correct and repair these inconsistencies, you must reconcile any scope inconsistencies. After you select and reconcile scope inconsistencies, the DHCP service either restores those IP addresses to the original owner, or creates a temporary reservation for those addresses. These reservations are valid for the lease time that you assign to the scope. When the lease time expires, the addresses are recovered for future use.

## Moving the DHCP database

In the event that you must move the DHCP server role to another server, as a best practice you also should move the DHCP database to the same server. This ensures that client leases are retained, and reduces the likelihood of client-configuration issues.

The following are high-level steps for moving a DHCP database:

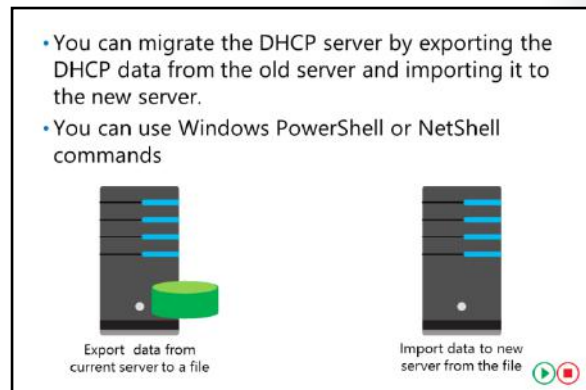
1. Back up the DHCP database on the old server.
2. Stop the old DHCP server service.
3. Copy the DHCP database to the new server, and if necessary, install the DHCP server role.
4. Restore the database.
5. Start the DHCP Server service.

## Migrating the DHCP server

When you decommission an outdated or old server, you must migrate the services from the old server to a new server. Migrating the DHCP server is not difficult, but you must use command-line utilities to export the DHCP data from the old server to a file, and then import the data from that file to the new DHCP server. You can use Microsoft Windows Netsh commands, or Windows PowerShell to accomplish this.

The following high-level steps detail how to migrate a DHCP server:

1. Install the DHCP server role on the computer that will be the new DHCP server.
2. Stop the DHCP service on the current DHCP server.
3. Export the DHCP data from the current server.
4. Copy the DHCP data to the new server (or make it available on the network).
5. Import the DHCP data to the new server.



### Exporting the DHCP data

You can use Windows PowerShell to export the DHCP data by using the **Export-DhcpServer** cmdlet. For example, the following command would export the DHCP data from a DHCP server named DHCP1 to a file named dhcp.xml:

```
Export-DhcpServer -ComputerName DHCP1 -Leases -File C:\dhcp.xml -verbose
```

You also can use the following Netsh series of commands by opening an elevated command prompt, and pressing Enter at the end of each line:

```
Netsh
DHCP
Server <name or IP address of current DHCP server>
Export C:\dhcp.txt all
```

### Importing the DHCP data

You can use Windows PowerShell to import the DHCP data by using the **Import-DhcpServer** cmdlet. For example, the following command would import the DHCP data from a file named dhcp.xml to the new DHCP server named DHCP2:

```
Import-DhcpServer -ComputerName DHCP2 -Leases -File C:\export\dhcp.xml -BackupPath
C:\dhcp\ -Verbose
```

You also can use the following Netsh series of commands by opening an elevated command prompt, and pressing Enter at the end of each line:



```
netsh
DHCP
Server <name or IP address of new DHCP server>
Import C:\dhcp all
```

## Discussion: Troubleshooting DHCP

The following table describes some common DHCP issues. Enter the possible solutions in the Solution column, and then discuss your answers with the class.

How do you address the following issues that can occur when you do not configure DHCP properly?

- Address conflicts
- Failure to obtain a DHCP address
- Address obtained from an incorrect scope
- DHCP database suffered data corruption or loss
- DHCP server has exhausted its IP address pool

Issue	Description	Example	Solution
Address conflicts	The same IP address is offered to two different clients.	An administrator deletes a lease. However, the client that had the lease is still operating as if the lease is valid. If the DHCP server does not verify the IP address, it might lease the IP address to another machine, causing an address conflict. This also can occur if two DHCP servers have overlapping scopes.	
Failure to obtain a DHCP address	The client does not receive a DHCP address and instead receives an Automatic Private IP Addressing (APIPA) self-assigned address.	If you configure a client's network card driver incorrectly, it might cause a failure to obtain a DHCP address. Additionally, the DHCP server or relay agent on the client's subnet might be not online. Another reason might be that the DHCP server has exhausted its scope. Therefore, you should extend or modify the scope.	
Address obtained from an incorrect scope	The client is obtaining an IP address from the wrong scope, causing it to experience communication problems.	If the client connects to the wrong network, or if you configure the DHCP relay agent incorrectly, this error could occur.	
DHCP database suffers data corruption or loss	The DHCP database becomes unreadable or is lost due to a hardware failure.	A hardware failure can cause the database to become corrupted.	
DHCP server exhausts its IP address pool	The DHCP server's IP scopes have been depleted. Any new clients requesting an IP address are refused.	This error occurs if all of the IP addresses that are assigned to a scope are leased.	

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

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

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

## Lab: Implementing DHCP

### Scenario

A. Datum Corporation is planning to open three branch offices in different cities in North America. The branch offices will be located in Houston Texas: Mexico City, Mexico; and Portland, Oregon.

The following table describes the planned computer distribution in the branch offices.

Location	Computer and device requirements
Houston	<ul style="list-style-type: none"> <li>• 300 desktop computers</li> <li>• 100 laptop computers connecting to both the wireless and wired networks</li> <li>• 50 tablet computers connecting only to the wireless network</li> </ul>
Mexico City	<ul style="list-style-type: none"> <li>• 100 desktop computers</li> <li>• 50 laptop computers connecting to both the wireless and wired networks</li> <li>• 20 tablet computers connecting only to the wireless network</li> </ul>
Portland	<ul style="list-style-type: none"> <li>• 100 desktop computers</li> <li>• 75 laptop computers connecting to both the wireless and wired networks</li> <li>• 150 tablet computers connecting only to the wireless network</li> </ul>

A. Datum is using Microsoft Office 365 for all email and file access for the North American branch offices, with some shared folders located in the Toronto regional office on servers that are running the Windows Server 2016. Because all offices have fast and highly available network connections to the Toronto office, A. Datum is not planning to deploy any servers in the branch offices at this point.

The A. Datum network team has assigned the subnets 172.16.18.0/18 to the Toronto main office. The Toronto office is currently using the network assignments shown in the following table.

IP subnet	Purpose
172.16.18.0/24	Network devices and network printers
172.16.19.0/24	Servers
172.16.20.0/24 to 172.16.52.0/24	Desktop computers
172.16.53.0/24 to 172.16.60.0/24	Wireless devices

Using this information, you must now plan and implement DHCP to support your design.

## Objectives

After completing this lab, you will be able to:

- Plan a DHCP server implementation.
- Implement the DHCP configuration.
- Validate the DHCP deployment.

## Lab Setup

Estimated Time: **70 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-EU-RTR**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, and **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Virtual machine: **20741A-NA-RTR**

User name: **Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Microsoft Hyper-V Manager**, click **20741A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20741A-EU-RTR**, **20741A-NA-RTR**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, and **20741A-LON-CL1**.

## Exercise 1: Planning the DHCP server implementation

### Scenario

You have been asked to implement a network server infrastructure that enables the assignment of IP addresses to the Houston, Mexico City, and Portland offices. You will use the TOR-SVR1 as the primary DHCP server.

Your solution must meet the following requirements:

- Wired and wireless clients must be assigned IP addresses from separate IP ranges.
- Each location should maintain a separate IP address range from other locations.
- Your solution should include a DHCP failover configuration to provide DHCP address leases if TOR-SVR1 is unavailable.

The main task for this exercise is as follows:

1. Plan the Dynamic Host Configuration Protocol (DHCP) server implementation.

► **Task 1: Plan the Dynamic Host Configuration Protocol (DHCP) server implementation**

Based on your answers to the following questions, you will develop a plan for implementing the DHCP server infrastructure.

1. What scopes do you need to create to enable the IP addressing scheme from module 1?
2. Where will DNS service come from?
3. How will you get DHCP messages from **TOR-SVR1** to the clients in the Houston, Mexico City, and Portland locations?
4. What configuration changes do you need to make to **NA-RTR** to enable the IP addressing scheme through the DHCP relay?
5. How will you assign different IP ranges to the clients in each location? How will you assign different IP addresses for wired and wireless clients?
6. What IP addresses will you assign to the network interfaces on **NA-RTR** that are connected to the Houston, Mexico City, and Portland networks?
7. How will you provide for DHCP Failover for **TOR-SVR1**?

**Results:** At the completion of this exercise you should have planned the DHCP implementation.

## Exercise 2: Implementing the DHCP configuration

### Scenario

Now that the IP addressing plan and DHCP server implementation plan are complete, you need to configure the server infrastructure to implement your plan.

The main tasks for this exercise are as follows:

1. Install and configure the DHCP server role on TOR-SVR1.
2. Configure DHCP scopes for Houston, Mexico City, and Portland.
3. Configure network adapters on NA-RTR.
4. Install the DHCP server role on LON-SVR1.
5. Configure DHCP failover between TOR-SVR1 and LON-SVR1.
6. Configure DHCP relay on NA-RTR for Houston, Mexico City, and Portland.

► **Task 1: Install and configure the DHCP server role on TOR-SVR1**

### Install the DHCP server role

1. On **TOR-SVR1**, open **Server Manager**, and then use the **Add Roles and Features Wizard** to install the DHCP Server role. Accept all the default settings.

### Perform the post-installation tasks

1. Click the **notifications** icon in the top menu bar, and then click the **Complete DHCP configuration** link.
2. Complete the **DHCP Post-Install configuration wizard** by accepting all the default settings, and then close the wizard.
3. Restart the DHCP Server service.

### ► Task 2: Configure DHCP scopes for Houston, Mexico City, and Portland

#### Create the Houston scopes

1. On **TOR-SVR1**, in **Server Manager**, start the **DHCP management** console.
2. Click the **TOR-SVR1.adatum.com** server icon to open the **IPv4** node.
3. Right-click the **IPv4** node, and then create a new scope with the following parameters:
  - o Name: **Houston-wired1**
  - o Start IP address: **172.16.30.2**
  - o End IP address: **172.16.30.254**
  - o subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.30.1**
  - o Lease duration: **8 days**
4. Create a second scope with the following parameters:
  - o Name: **Houston-wired2**
  - o Start IP address: **172.16.31.1**
  - o End IP address: **172.16.31.254**
  - o subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.30.1**
  - o Lease duration: **8 days**
5. Create a third scope with the following parameters:
  - o Name: **Houston-wireless**
  - o Start IP address: **172.16.55.2**
  - o End IP address: **172.16.55.254**
  - o subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.55.1**
  - o Lease duration: **1 days**

#### Create a superscope for Houston wired scopes

1. Right-click the **IPv4** node, and then click **New Superscope**.
2. Use the **New Superscope Wizard** to create a superscope with the following settings:
  - o Name: **Houston-wired**
  - o Include scopes: **[172.16.30.0] Houston-wired1** and **[172.16.31.0] Houston-wired2**



### Create the Mexico City scopes

1. Create a new scope with the following parameters:
  - o Name: **MexicoCity-wired**
  - o Start IP address: **172.16.35.2**
  - o End IP address: **172.16.35.254**
  - o subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.35.1**
  - o Lease duration: **8 days**
2. Create a second scope with the following parameters:
  - o Name: **MexicoCity-wireless**
  - o Start IP address: **172.16.56.2**
  - o End IP address: **172.16.56.254**
  - o Subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.56.1**
  - o Lease duration: **1 days**

### Create the Portland scopes

1. Create a new scope with the following parameters:
  - o Name: **Portland-wired**
  - o Start IP address: **172.16.40.2**
  - o End IP address: **172.16.40.254**
  - o subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.40.1**
  - o Lease duration: **8 days**
2. Create a second scope with the following parameters:
  - o Name: **Portland-wireless**
  - o Start IP address: **172.16.57.2**
  - o End IP address: **172.16.57.254**
  - o Subnet mask: **255.255.255.0**
  - o Default Gateway: **172.16.57.1**
3. Lease duration: **1 days**

### ► Task 3: Configure network adapters on NA-RTR

1. Switch to **NA-RTR**.
2. Right-click **Start**, and then click **Network Connections**.
3. Configure the **HOU\_WAN** adapter with the following TCP/IPv4 properties:
  - o IP address: **172.16.30.1**
  - o Subnet mask: **255.255.255.0**

4. Configure the **MEX\_WAN** adapter with the following TCP/IPv4 properties:
  - IP address: **172.16.35.1**
  - Subnet mask: **255.255.255.0**
5. Configure the **POR\_WAN** adapter with the following TCP/IPv4 properties:
  - IP address: **172.16.40.1**
  - Subnet mask: **255.255.255.0**

► **Task 4: Install the DHCP server role on LON-SVR1**

**Install the DHCP server role**

- On **LON-SVR1**, open **Server Manager**, and then use the **Add Roles and Features Wizard** to install the **DHCP Server** role, accepting all default values.

**Perform the post-installation tasks**

1. On the top menu bar, click the **Notifications** icon, and then click the **Complete DHCP configuration** link.
2. Complete the **DHCP Post-Install configuration wizard** by accepting all the default settings, and then close the wizard.
3. Restart the DHCP Server service.

► **Task 5: Configure DHCP failover between TOR-SVR1 and LON-SVR1**

1. Switch to **TOR-SVR1**.
2. In the **DHCP management** console, right-click the **IPv4** node, and then click **Configure Failover**.
3. Configure a failover relationship with the following parameters:
  - Partner Server: **172.16.0.11**
  - Maximum Client Lead Time: **1** minute
  - Mode: **Hot standby**
  - Shared Secret: **Pa\$\$wOrd**
4. Switch to **LON-SVR1**.
5. In the **DHCP management** console, expand the **IPv4** node, and note that all scopes now display.

► **Task 6: Configure DHCP relay on NA-RTR for Houston, Mexico City, and Portland**

1. On **NA-RTR**, open **Server Manager**, and then open **Routing and Remote Access**.
2. In the left pane, expand **NA-RTR**, expand **IPv4**, expand **General**, and then add a new routing protocol for **DHCP Relay Agent**.
3. Set the properties of the DHCP Relay Agent to send messages to the server address **172.16.18.20** and to server address **172.16.0.11**.
4. Add the following new interfaces to the DHCP Relay Agent and use the default settings:
  - **HOU\_WAN**
  - **MEX\_WAN**
  - **POR\_WAN**

**Results:** After completing this exercise, you should have you should have implemented your plan for the DHCP configuration.

## Exercise 3: Validating the DHCP implementation

### Scenario

Now that you have implemented DHCP, you need to test the configuration to ensure that the clients are receiving IP addresses, and that DHCP Failover is functioning correctly. You decide to use LON-CL1 to test DHCP by moving the client between the virtual networks.

The main tasks for this exercise are as follows:

1. Test DHCP allocation to the correct subnets.
2. Test DHCP failover.

#### ► Task 1: Test DHCP allocation to the correct subnets

1. Switch to **LON-CL1**.
2. Change the properties of the **London\_Network** adapter to **Obtain an IP address automatically**.
3. In the virtual machine settings, for **20741A-LON-CL1**, change the virtual switch from **London\_Network** to **HOU\_WAN**.
4. Open a **Command Prompt**, and use the **IPConfig /All** command to view the current IP address.



**Note:** Note that the IP address will be 172.16.30.2. The IP address of the DHCP server will be 172.16.18.20.

5. In the virtual machine settings, change the virtual switch from **HOU-WAN** to **MEX\_WAN**. Wait a few seconds for the change to take effect.
6. Open a command prompt, and use the **IPConfig /All** command to view the current IP address.



**Note:** Note that the IP address will be 172.16.35.2. The IP address of the DHCP server will be 172.16.18.20.

7. In the virtual machine settings, change the virtual switch from **MEX\_WAN** to **POR\_WAN**. Wait a few seconds for the change to take effect.
8. Open a Command Prompt and use the **IPConfig /All** command to view the current IP address.



**Note:** Note that the IP address will be 172.16.40.2. The IP address of the DHCP server will be 172.16.18.20.

#### ► Task 2: Test DHCP failover

1. Switch to **TOR-SVR1**.
2. Stop the DHCP Server service.
3. Switch to **LON-CL1**.
4. In the Command Prompt window, run the **Ipconfig /release** command.

5. In the Command Prompt window, run the **ipconfig /renew** command.
6. Run the **ipconfig /All** command.



**Note:** Note that the IP DHCP server will now be 172.16.0.11.

**Results:** After completing this exercise, you should have tested DHCP IP address allocation to the correct subnets, and tested DHCP failover.

### ► Task 3: Prepare for the next module

When you finish the lab, revert all the virtual machines to their initial state by performing the following steps:

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

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

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

## Module Review and Takeaways

### Best Practices

The following are best practices for working with DHCP:

- Configure DHCP failover relationships to provide high availability.
- Ensure lease durations are appropriate. Shorter lease durations are usually recommended for wireless networks due to the transient nature of wireless clients.
- Create reservations for devices that need IP addresses that do 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	

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 3

## Implementing IPv6

### Contents:

Module Overview	3-1
<b>Lesson 1:</b> Overview of IPv6 addressing	3-2
<b>Lesson 2:</b> Configuring an IPv6 host	3-13
<b>Lesson 3:</b> Implementing IPv6 and IPv4 coexistence	3-22
<b>Lesson 4:</b> Transitioning from IPv4 to IPv6	3-26
<b>Lab:</b> Configuring and evaluating IPv6 transition technologies	3-32
Module Review and Takeaways	3-43

## Module Overview

IPv6 is a technology that helps the Internet support a growing user base and an increasingly large number of IP-enabled devices. IPv4 has been the underlying Internet protocol for almost 30 years. Because of the growing need for new IP addresses, IPv4's robustness, scalability, and limited feature set are challenged. This is largely because of the rapid growth of new network-aware devices.

### Objectives

After completing this module, you will be able to:

- Describe the features and benefits of IPv6.
- Configure an IPv6 host.
- Implement coexistence between IPv4 and IPv6 networks.
- Transition from an IPv4 network to an IPv6 network.

## Lesson 1

# Overview of IPv6 addressing

IPv6 has been included with Windows client operating systems and Windows Servers beginning with Windows Server 2008 and Windows Vista. The use of IPv6 is becoming more common on corporate networks and the Internet.

It is important for you to understand how this technology affects current networks, and how to integrate IPv6 into those networks. This lesson discusses the benefits of IPv6 and how it differs from IPv4.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain why you should use IPv6.
- Describe the differences between IPv4 and IPv6.
- Understand IPv6 addresses.
- Describe the structure of IPv6 addresses.
- Describe the types of IPv6 addresses.
- Describe IPv6 autoconfiguration options.

### Why use IPv6?

The current version of the Internet Protocol (known as IP version 4 or IPv4) has not been substantially altered from the time it was designed in the late 1970s, and it was not altered when RFC 791 was published in 1981. While IPv4 has proven to be robust, easily implementable, and interoperable, and can scale up to the size of today's Internet, the legacy protocol faces some serious challenges that no one could have envisioned decades ago.

Consequently, the Internet Engineering Task Force (IETF) in 1994 initiated the design and development of a suite of protocols and standards now known as Internet Protocol version 6, or IPv6. To understand why organizations should seriously consider using IPv6, it is important to know the limitations of the former version:

- The exponential growth of the Internet and the impending exhaustion of the IPv4 address space.

IPv4 addresses have become relatively scarce, forcing some organizations to use a network address translator (NAT) to map multiple private IP addresses to a single public IP address. While NATs promote the reuse of private address spaces, they do not support standards-based network layer security or the correct mapping of all higher layer protocols. In addition, NATs can create problems when connecting two organizations that use the same private IP address space.

Additionally, the rising pervasiveness of Internet-connected devices and appliances assures that the public IPv4 address space will be depleted eventually.

#### Organizations should consider using IPv6 because:

- The exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- The growth of the Internet and the ability of Internet backbone routers to maintain large routing tables
- The need for simpler configuration
- The requirement for security at the IP layer
- The need for better support for real-time delivery of data (also known as Quality of Service)



- The growth of the Internet and the ability of the Internet backbone routers to maintain large routing tables. Because of the way in which IPv4 network IDs have been and are currently allocated, there are routinely more than 70,000 routes in the routing tables of Internet backbone routers. This is because the current IPv4 Internet routing infrastructure is a combination of both flat and hierarchical routing. Alternatively, the IPv6-based Internet has been designed from its foundation to support efficient hierarchical addressing and routing.



**Note:** Global unicast addresses are equivalent to public IPv4 addresses. They are globally routable and reachable on the IPv6-based Internet.

- The need for simpler configuration. Most current IPv4 implementations must be configured either manually or through a stateful address configuration protocol such as Dynamic Host Configuration Protocol (DHCP). With more computers and appliances using IP, there is a need for a simpler and more automatic configuration of addresses that does not rely on the administration of a DHCP infrastructure. For example, IPv6 uses Stateless Address Auto Configuration (SLAAC) to provide simple plug and play networking.
- The requirement for security at the IP layer. Private communication over a public medium like the Internet requires encryption services that protect the data sent from being viewed or modified in transit. Although a standard now exists for providing security for IPv4 packets (known as Internet Protocol security or IPSec), this standard is optional, and proprietary solutions are prevalent.
- The need for better support for real-time delivery of data (also known as quality of service). While standards for Quality of Service (QoS) exist for IPv4, real-time traffic support relies on the IPv4 Type of Service (ToS) field and the identification of the payload, typically by using a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port. Unfortunately, the IPv4 ToS field has limited functionality and has different interpretations. In addition, payload identification using a TCP and UDP port is not possible when the IPv4 packet payload is encrypted.

IPv6 is intentionally designed for minimal impact on upper- and lower-layer protocols by avoiding the arbitrary addition of new features.

## Differences between IPv4 and IPv6

Designers of the IPv4 address space did not predict that public IPv4 addresses could be exhausted. However, because of the changes in technology and an allocation practice that did not anticipate the growth in the number of Internet hosts, it was clear by 1992 that a replacement would be necessary.

When the IPv6 address space was designed (RFC 2460 was published in 1998), the addresses were made 128 bits long so that the address space could be subdivided into hierarchical routing domains that reflect modern-day Internet topology. With 128 bits, there are enough bits to create multiple levels of hierarchy, and there is flexibility for designing hierarchical addressing and routing. These features are currently lacking in the IPv4-based Internet.

Feature	IPv4	IPv6
Fragmentation	Performed by routers and sending host	Performed only by the sending host
Address resolution	Broadcast ARP request frames	Multicast Neighbor Solicitation messages
Manage multicast group membership	IGMP	Multicast Listener Discovery
Router Discovery	ICMP Router Discovery (optional)	ICMPv6 Router Solicitation and Router Advertisement (required)
DNS host records	A records	AAAA records
DNS reverse lookup zones	IN-ADDR.ARPA	IP6.ARPA
Minimum packet size	576 bytes	1280 bytes



**Note:** A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) which is the result of a committee drafting and subsequent reviews by interested parties. Some RFCs are informational in nature. But in the RFCs that are intended to become Internet standards, the final version of the RFCs become the standard, and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

## Comparing IPv4 and IPv6

The following table highlights additional differences between IPv4 and IPv6.

IPv4	IPv6
Fragmentation is performed by both routers and the sending host.	Fragmentation is not performed by routers but instead only by the sending host.
Address Resolution Protocol (ARP) uses broadcast ARP request frames to resolve an IPv4 address to a link-layer address.	ARP request frames are replaced with multicast neighbor solicitation messages.
Internet Group Management Protocol (IGMP) manages local subnet group membership.	IGMP is replaced with Multicast Listener Discovery messages.
Internet Control Message Protocol (ICMP) Router Discovery—which is optional—determines the IPv4 address of the best default gateway.	ICMP Router Discovery is replaced with required ICMPv6 Router Solicitation and Router Advertisement messages.
Uses host (A) resource records in the DNS to map host names to IPv4 addresses.	Uses IPv6 host (AAAA) resource records in DNS to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

## Overview of IPv6 addressing

The most distinguishing feature of IPv6 is its use of much larger addresses. IPv4 addresses are expressed in four groups of decimal numbers, such as 192.168.1.1. Each grouping of numbers represents a binary octet. In binary, 192.168.1.1 is as follows:

11000000.10101000.00000001.00000001  
(4 octets = 32 Bits)

- 128-bit address in binary:  
00100000000000010000110110111000  
0000000000000000010110101001100  
000000011100110000000000011011101  
00010001001000100001001000110100
- 128-bit address divided into 16-bit blocks:  
0010000000000001 0000110110111000  
0000000000000000 0010110101001100  
0000000111001100 0000000011011101  
0001000100100010 0001001000110100
- Each 16-bit block converted to hexadecimal (base 16):  
2001:0DB8:0000:2D4C:01CC:00DD:1122:1234
- Further simplified by removing leading zeros:  
2001:DB8:0:2D4C:1CC:DD:1122:1234



However, an IPv6 address is four times larger than an IPv4 address. Because of this, IPv6 addresses are expressed in hexadecimal. For example:

```
2001:0DB8:0000:2D4C:01CC:00DD:1122:1234
```

This might seem complex for end users, but the assumption is that users will rely on DNS names to resolve hosts and will rarely enter IPv6 addresses manually. Because the IPv6 address is hexadecimal, it is also easier to convert between binary and hexadecimal than it is to convert between binary and decimal. This simplifies working with subnets and calculating hosts and networks.

### Hexadecimal numbering system (Base 16)

In the hexadecimal numbering system, some letters represent numbers; this is because there must be 16 unique symbols for each position. Because 10 symbols (0 through 9) already exist, there must be six new symbols for the hexadecimal system; hence, the letters A through F are used. The hexadecimal number 10 is equal to the decimal number 16.



**Note:** You can use the Calculator application included with Windows Server 2016 to convert between binary, decimal, and hexadecimal numbers.

To convert an IPv6 binary address that is 128 bits long, you break it into eight blocks of 16 bits. You then convert each of these eight blocks of 16 bits into four hexadecimal characters. For each of the blocks, you evaluate four bits at a time. You should number each section of four binary numbers 1, 2, 4, and 8, starting from the right and moving left. That is:

- The first bit [0010] is assigned the value of 1.
- The second bit [0010] is assigned the value of 2.
- The third bit [0010] is assigned the value of 4.
- The fourth bit [0010] bit is assigned the value of 8.

To calculate the hexadecimal value for this section of four bits, add up the value of each bit that is set to 1. In the example of 0010, the only bit that is set to 1 is the bit assigned the value 2. The rest are set to zero. Therefore, the hexadecimal value of this section of four bits is 2.

### Converting from binary to hexadecimal

The following table describes converting 8 bits of binary into hexadecimal for the binary number [0010][1111]. Technet24.ir

Binary	0010	1111
Values of each binary position	8421	8421
Adding values where the bit is 1	0+0+2+0=2	8+4+2+1=15 or hexadecimal F

The following example is a single IPv6 address in binary system. Note that the binary representation of the IP address is very long. The following two lines of binary numbers represent one IP address:

```
001000000000000100001101101110000000000000000000010110101001100
0000000111001100000000001101110100010001000100001001000110100
```

The 128-bit address is now divided along 16-bit boundaries (eight blocks of 16 bits):

```
0010000000000001 0000110110111000 0000000000000000 0010110101001100
0000000111001100 000000011011101 0001000100100010 0001001000110100
```

Each block is further broken into sections of four bits. The following table shows the binary and corresponding hexadecimal values for each section of four bits:

Binary	Hexadecimal
[0010][0000][0000][0001]	[2][0][0][1]
[0000][1101][1011][1000]	[0][D][B][8]
[0000][0000][0000][0000]	[0][0][0][0]
[0010][1101][0100][1100]	[2][D][4][C]
[0000][0001][1100][1100]	[0][1][C][C]
[0000][0000][1101][1101]	[0][0][D][D]
[0001][0001][0010][0010]	[1][1][2][2]
[0001][0010][0011][0100]	[1][2][3][4]

Each 16-bit block is expressed as four hexadecimal characters and is then delimited with colons. The result is as follows:

```
2001:0DB8:0000:2D4C:01CC:00DD:1122:1234
```

The representation of the IPv6 address can be simplified by removing each leading zero within a 16-bit block. If a block has four zeros, they should be represented with only one zero. If you use zero suppression on the address 2001:0DB8:0000:2D4C:01CC:00DD:1122:1234, the result will be as follows:

```
2001:DB8:0:2D4C:1CC:DD:1122:1234
```

### Compressing zeros

When multiple contiguous zero blocks occur, you can compress these and represent them in the address as a double-colon (::); this further simplifies the IPV6 notation. The computer recognizes the double colon and substitutes it with the number of blocks necessary to make the appropriate IPv6 address.

In the following example, the address is expressed by using zero compression:

```
2001:DB8::2D4C:1CC:DD:1122:1234
```

To determine how many 0 bits are represented by the double colon, use the following procedure:

- Count the number of blocks in the compressed address. In previous example, this number is 7.
- Subtract the number of blocks (7) from 8, which gives the result 1.
- Multiply the result of the subtraction (1) by 16, which gives the result 16.
- Finally, the result 16 means that there are 16 bits, or 16 zeros in binary system, in the address where the double colon is located.

You can use zero compression only once in a given address. If you use it twice or more, there is no way to show how many 0 bits are represented by each instance of the double colon (::).

To convert an address into binary, use the reverse of the method described previously:

1. Add zeros by using zero compression.
2. Add leading zeros.
3. Convert each number into its binary equivalent.

**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
```


## IPv6 address structure

Each IPv6 address is 128 bits long. The *prefix* is the part of the address that contains the bits with fixed values or the subnet prefix's bits. The prefix is equivalent to the network ID for IPv4 addresses.


IPv6 subnets, prefixes, routes, and address ranges are represented in the same way as IPv4 Classless Interdomain Routing (CIDR) notations. An IPv6 prefix is represented in address/prefix-length notation. For example, 2001:DB8::/48 (a route prefix) and 2001:DB8:0:2D4C::/64 (a subnet prefix) are IPv6 address prefixes.

- The number of network bits is defined by the prefix
- Each host has 64 bits allocated to the interface identifier

Type of address	IPv4 address	IPv6 address
Unspecified	0.0.0.0	::
Loopback	127.0.0.1	::1
Autoconfigured	169.254.0.0/16	FE80::/64
Broadcast	255.255.255.255	Uses multicasts instead
Multicast	224.0.0.0/4	FF00::/8

 **Note:** IPv6 uses prefixes instead of a subnet mask.

When a unicast IPv6 address is assigned to a host, the prefix is 64 bits. The remaining 64 bits are allocated to the interface identifier, which uniquely identifies the host on that network. The interface identifier can be generated randomly, assigned by Dynamic Host Configuration Protocol v6 (DHCPv6), or based on the media access control (MAC) address of the network. By default, the host bits are generated randomly unless assigned by DHCPv6.

 **Note:** The routes on an IPv6 router have varying prefix sizes that are determined by the size of the network.

## IPv6 equivalents for IPv4 special addresses

The following table shows IPv6 equivalents to some common IPv4 addresses.

Type of address	IPv4 address	IPv6 address
Unspecified address	0.0.0.0	::
Loopback address	127.0.0.1	::1
Autoconfigured addresses	169.254.0.0/16	FE80::/64
Broadcast address	255.255.255.255	Uses multicasts instead
Multicast addresses	224.0.0.0/4	FF00::/8

## Types of IPv6 addresses

IPv6 supports three types of addresses, which can be categorized based on type and scope:

- **Unicast.** A unicast address identifies a single interface within the scope of the type of unicast address. With the appropriate unicast routing topology, packets addressed to a unicast address are delivered to a single interface. Effectively, a packet is delivered from a single interface to another single interface. To accommodate load-balancing systems, RFC 3513 allows multiple interfaces to use the same address as long as they appear as a single interface to the IPv6 implementation on the host.
- **Multicast.** A multicast address identifies multiple interfaces. With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address. A multicast address is used for one-to-many communication, with delivery to multiple interfaces, or all the interfaces in the set.
- **Anycast.** An anycast address identifies multiple interfaces. With the appropriate routing topology, packets addressed to an anycast address are delivered to a single interface that is also the nearest interface that is identified by the address. The nearest interface is defined as being closest in terms of routing distance. An anycast address is used for one to one-of-many communication, with delivery to a single interface in the set. An example of this would be a proxy server where you might have multiple servers located across your network, but you only want to forward packets to the closest one.

IPv6 supports three types of addresses:

- Unicast
- Multicast
- Anycast

The following are types of unicast IPv6 addresses:

- Global unicast addresses
- Unique local addresses
- Link-local addresses
- Site-local addresses:
  - Formerly deprecated in RFC 3879
  - Superseded by unique local addresses
- Special addresses
- Compatibility or transition addresses



**Note:** IPv6 addresses always identify interfaces, not nodes. A node is identified by any unicast address that is assigned to one of its interfaces.

RFC 3513 does not define a broadcast address. All types of IPv4 broadcast addressing are performed in IPv6 by using multicast addresses. The special IPv6 multicast address will send a packet to all nodes which will accomplish the same result (For example, FF02::1).

The types of unicast IPv6 addresses include the following:

- Global unicast addresses
- Unique local addresses
- Link-local addresses
- Site-local addresses (formerly deprecated in RFC 3879, and superseded by unique local addresses)
- Special addresses
- Compatibility or transition addresses

### Global unicast addresses

*Global unicast addresses* are the IPv6 equivalent to public IPv4 addresses that are available from an Internet service provider (ISP). They are routable and reachable globally on the IPv6 portion of the Internet. A limited number of Internet-addressable IPv4 addresses remain, but many global unicast addresses are available for use.

The global unicast address space is designed to allow each ISP customer to obtain a large number of IPv6 addresses. The first 48 bits are used to identify the customer site. The next 16 bits are allocated for the customer to perform subnetting within its own network.



**Note:** The network 2001:0db8::/32 is reserved for documentation and is not routable.

The structure of a global unicast address has the following parts:

- Fixed portion set to 001. The three high-order bits are set to 001. The address prefix for currently assigned global addresses is 2000::/3. Therefore, all global unicast addresses begin with either 2 or 3.
- Global routing prefix. This field identifies the global routing prefix for a specific organization's site. The combination of the three fixed bits and the 45-bit global routing prefix is used to create a 48-bit site prefix, which is assigned to an organization's individual site. After the assignment occurs, routers on the IPv6 Internet forward IPv6 traffic that matches the 48-bit prefix to the routers of the organization's site.
- Subnet ID. The subnet ID is used within an organization's site to identify subnets. This field's size is 16 bits. The organization's site can use these 16 bits within its site to create 65,536 subnets, or multiple levels of addressing hierarchy, and an efficient routing infrastructure.
- Interface ID. The interface ID identifies the interface on a specific subnet within the site. This field's size is 64 bits. This is either generated randomly or assigned by DHCPv6. In the past, the interface ID was based on the MAC address of the network interface card to which the address was bound.

### Unique local addresses

*Unique local addresses* are the IPv6 equivalent to IPv4 private addresses. These addresses are routable within an organization but not on the Internet.

IPv4 private IP addresses were a relatively small part of the overall IPv4 address space, and many companies used the same address space. This caused problems when separate organizations tried to communicate directly. It also caused problems while merging the networks of two organizations—possibly following a merger or an acquisition.

To avoid the duplication problems experienced with IPv4 private addresses, the IPv6 unique local address structure allocates 40 bits to an organization identifier. The 40-bit organization identifier is randomly generated. The likelihood of two randomly generated 40-bit identifiers being the same is very small. This ensures that each organization has a unique address space.

The first seven bits of the organization identifier have the fixed binary value of 1111110. All unique local addresses have the address prefix of FC00::/7. The Local (L) flag is set to 1 to indicate a local address. An L flag value set to 0 has not yet been defined. Therefore, unique local addresses with the L flag set to 1 have the address prefix of FD::/8.

### Link-local addresses

All IPv6 hosts have a link-local address that is used for communication only on the local subnet. The link-local address is generated automatically and is nonroutable. In this way, a link-local address is the IPv6 equivalent to an IPv4 Automatic Private IP Addressing (APIPA) address (For example, 169.254.x.x). However, a link-local address is an essential part of IPv6 communication.

Link-local addresses are used for communication in many scenarios in which IPv4 would have used broadcast messages. For example, link-local addresses are used when communicating with a DHCPv6 server. Link-local addresses are also used for neighbor discovery, which is the IPv6 equivalent of ARP in IPv4. The prefix for link-local addresses is always FE80::/64. The final 64 bits are the interface identifiers.

## Zone ID

Regardless of the number of network interfaces in the host, each IPv6 host has a single link-local address. If the host has multiple network interfaces, the same link-local address is reused on each network interface. To allow hosts to identify link-local communication on each unique network interface, a zone ID is added to the link-local address. A zone ID is used in the following format:

*Address%zone\_ID*

Each sending host determines the zone ID that it will associate with each interface. There is no negotiation of zone ID between hosts. For example, on the same network, host A might use 3 for the zone ID on its interface, and host B might use 6 for the zone ID on its interface.

Each interface in a Windows-based host is assigned a unique interface index, which is an integer. In addition to physical network cards, interfaces also include loopback and tunnel interfaces. Windows-based IPv6 hosts use the interface index of an interface as the zone ID for that interface. In the following example, the interface ID for the network interface is 3:

fe80::2b0:d0ff:fee9:4143%3

## Special addresses

The following are special IPv6 addresses:

- **Unspecified address.** The unspecified address (0:0:0:0:0:0:0 or ::) is used only to indicate the absence of an address. It is the IPv6 equivalent to the IPv4 unspecified address of 0.0.0.0. The unspecified address is typically used as a source address for packets that are attempting to verify the uniqueness of a tentative address. The unspecified address is never assigned to an interface, and it is never used as a destination address.
- **Loopback address.** The loopback address (0:0:0:0:0:0:0:1 or ::1) is used to identify a loopback interface, enabling a node to send packets to itself. It is the IPv6 equivalent to the IPv4 loopback address of 127.0.0.1. Packets addressed to the loopback address are never sent on a link or forwarded by an IPv6 router.

## Compatibility or transition addresses

These are addresses that help in the migration from IPv4 to IPv6 and facilitate the coexistence of both types of hosts. More information on these types of IPv6 addresses is provided later in the module.

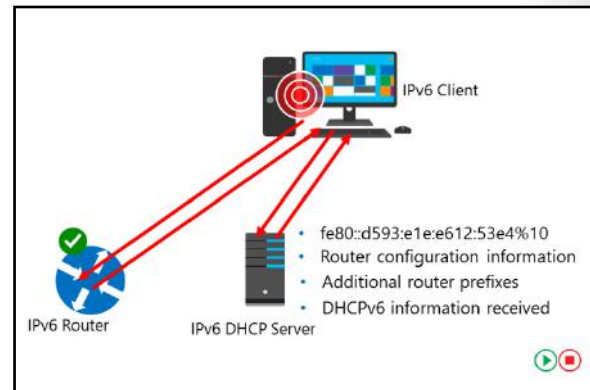
The table below shows the address ranges for each type of IPv6 address:

<b>Global unicast</b>	<b>Any address starting with 0010::/7. Therefore either 2000:: or 3000::</b>
<b>Unique local</b>	Any address starting with FC00::/7, including FC00:: FD00:: and FE00:: (FD00::/7)
<b>Link-Local</b>	Any addresses starting with FE80::
<b>Unspecified</b>	::
<b>Loopback</b>	::1



## Autoconfiguration options for IPv6

A highly useful aspect of IPv6 is its ability to configure itself automatically without the use of a stateful configuration protocol, such as DHCPv6. By default, an IPv6 host can configure a link-local address for each interface. By using router discovery, a host can also determine the addresses of routers, additional addresses, and other configuration parameters. The Router Advertisement message includes an indication of whether a stateful address configuration protocol should be used.



**Note:** Address autoconfiguration can only be performed on multicast-capable interfaces. Address autoconfiguration is described in RFC 2462, "IPv6 Stateless Address Autoconfiguration."

### Types of autoconfiguration

Types of autoconfiguration include:

- Stateless. With stateless autoconfiguration, address configuration is based on the receipt of Router Advertisement messages only. Stateless autoconfiguration includes a router prefix but does not include additional configuration options such as DNS servers.
- Stateful. With stateful autoconfiguration, address configuration is based on the use of a stateful address configuration protocol such as DHCPv6 to obtain addresses and other configuration options. A host uses stateful address configuration when:
  - It receives instructions to do so in a Router Advertisement messages.
  - There are no routers present on the local link.
- Both. With both, configuration is based on both receipt of Router Advertisement messages, and on DHCPv6.

### Stateful configuration

With stateful configuration, organizations can control how IPv6 addresses are assigned by using DHCPv6. If you need to configure any specific scope options—such as the IPv6 addresses of DNS servers—a DHCPv6 server is necessary.

When IPv6 attempts to communicate with a DHCPv6 server, it uses multicast IPv6 addresses. This is different from IPv4, which uses broadcast IPv4 addresses.

### Autoconfigured address states

During autoconfiguration, the IPv6 address of a host goes through several states that define the IPv6 address' life cycle. Autoconfigured addresses are in one or more of the following states:

- **Tentative.** In the *tentative* state, the host uses verification to determine whether the address is unique. The host will use a duplicate address detection algorithm on addresses before assigning them to an interface. Consequently, when an address is in the tentative state, a node cannot receive unicast traffic.
- **Valid.** In the *valid* state, the address has been verified as unique, and can send and receive unicast traffic.

- **Preferred.** In the preferred state, the address enables a node to send and receive unicast traffic to and from it.
- **Deprecated.** In a deprecated state, the address is valid, but its use is discouraged for new communication.
- **Invalid.** In the invalid state, the address no longer allows a node to send or receive unicast traffic.

## Lesson 2

# Configuring an IPv6 host

After you plan a proper design architecture of your IPv6 network, you need to deploy it to your environment. In this lesson, you will learn how to configure IPv6 and which tools to use to make the changes.

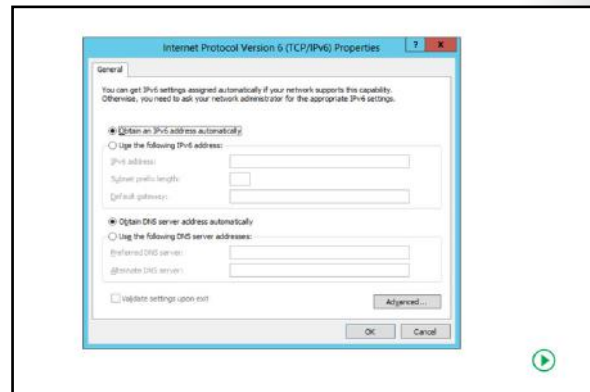
### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the configurable IPv6 settings.
- Explain how to use the tools for IPv6 network configuration.
- Describe how to configure DHCP to support IPv6.


### Configurable IPv6 settings

On IPv4 networks, you can assign addresses to an interface in three ways: manually, by using static addresses, dynamically, by using DHCP, or automatically, by using Automatic Private IP Addressing (APIPA). Administrators of small networks often configure IPv4 addresses manually, and midsize to large organizations typically use DHCP. Automatic address configuration by using APIPA is usually done only on very small networks such as a home or office local area network (LAN) that connects to the Internet by using a personal router.



In contrast, address assignment on IPv6 networks is slightly different. For example, IPv6 addresses can be assigned to an interface in four ways:

- Manually configuring one or more IPv6 addresses on the interface.
- Stateful address autoconfiguration using a DHCPv6 server.
- Stateless address autoconfiguration based on the receipt of Router Advertisement messages.
- Both stateful and stateless address autoconfiguration.

 **Note:** A link-local address is always configured automatically on an interface by the operating system regardless of whether stateful or stateless address autoconfiguration is deployed.

The main difference, however, between address assignment in IPv6 and in IPv4 is that the IPv6 protocol was designed to be configured automatically. This means that in most cases, you do not need to assign addresses manually or deploy a DHCPv6 server; instead, you can use stateless address autoconfiguration for most of your network hosts. Consequently, in contrast to network adapters on IPv4 hosts, which are usually single-homed (have only a single address assigned), most network adapters on IPv6 hosts are multi-homed (have multiple addresses assigned). Specifically, an IPv6 network interface typically has at least two addresses:

- An automatically generated link-local address, which is used for traffic on the local link.
- An additional unicast address (either a global address or a unique local address), which is used for traffic that needs to be routed beyond the local link.

### General tab

When configuring IPv6 settings on a network interface, you have multiple options to choose; default settings are stateful or stateless address autoconfiguration. On the **General** tab of the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, you can configure the following:

- **Obtain an IPv6 address automatically.** Specifies that IPv6 addresses, for this connection, or adapters are automatically determined by stateful or stateless address autoconfiguration.
- **Use the following IPv6 address.** Specifies that an IPv6 address and default gateway for this connection or adapter are manually configured.
- **IPv6 address.** Provides a space for you to type an IPv6 unicast address. You can specify additional IPv6 addresses from the **Advanced TCP/IP Settings** dialog box.
- **Subnet prefix length.** Provides a space for you to type the subnet prefix length for the IPv6 address. For typical IPv6 unicast addresses, this value should be set to 64, the default value.
- **Default gateway.** Provides a space for you to type the IPv6 unicast address of the default gateway.
- **Obtain DNS server address automatically.** Specifies that the IPv6 addresses for DNS servers are automatically determined by stateful address autoconfiguration (DHCPv6).
- **Use the following DNS server addresses.** Specifies that the IPv6 addresses of the preferred and alternate DNS servers for this connection or adapter are manually configured.
- **Preferred DNS server.** Provides a space for you to type the IPv6 unicast address of the preferred DNS server.
- **Alternate DNS server.** Provides a space for you to type the IPv6 unicast address of the alternate DNS server. You can specify additional DNS servers from the **Advanced TCP/IP Settings** dialog box.

### Advanced TCP/IP Settings

From the **General** tab, you can click **Advanced** to access the **Advanced TCP/IP Settings** dialog box. This dialog box is very similar to the **Advanced TCP/IP Settings** dialog box for the Internet Protocol version 4 (TCP/IPv4) component except that there is no **WINS** tab (IPv6 does not use NetBIOS and the Windows Internet Name Service [WINS]) nor **Options** tab (TCP/IP filtering is defined only for IPv4 traffic). For IPv6, the **Advanced TCP/IP Settings** dialog box has **IP Settings** and **DNS** tabs.

### The IP Settings tab

From the **IP Settings** tab, you can configure the following:

- Multiple IPv6 addresses. For each unicast IPv6 address, you must specify an IPv6 address and a subnet prefix length. The **Add** button is available only if **Use the Following Ipv6 Address** has been selected on the **General** tab of the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box.

- Multiple default gateways. For each default gateway, you must specify the IPv6 address of the gateway and whether you want the metric for the default route associated with this default gateway to be manually specified, or to be based on the speed of the connection or adapter.
- Route metrics. You can also specify whether to use a specific metric for the routes associated with the configuration of IPv6 addresses or default gateways, or a metric determined by the speed of the connection or adapter.

### The DNS tab

From the **DNS** tab, you can configure the following settings (these settings are similar to the IPv4 settings):

- **DNS server addresses, in order of use.** The IPv6 addresses of DNS servers to query for resolving DNS domain names. DNS servers are queried in the order in which they are listed here.
- **Append primary and connection specific DNS suffixes.** Specifies that resolution for unqualified names are limited to the domain suffixes of the primary suffix and all connection-specific suffixes. The connection specific DNS suffixes are configured in **DNS suffix for this connection**.
- **Append these DNS suffixes (in order).** Lists the DNS suffixes to search in the order listed.
- **DNS suffix for this connection.** Provides a space for you to specify a DNS suffix for this connection, unless configured by stateful address autoconfiguration (DHCPv6).
- **Register this connection's addresses in DNS.** Specifies that the computer attempt dynamic registration of the IP addresses (through DNS) of this connection with the full computer name of this computer.
- **Use this connection's DNS suffix in DNS registration.** If the check box is selected, this registration is in addition to the DNS registration of the full computer name.

### Tools for configuring IPv6

In most scenarios, a computer with Windows Server 2016 will autoconfigure IPv6 even without DHCP. However, in advanced networking scenarios, you might need to manually configure one or more network interfaces. You can configure IPv6 by using any of the following methods:

- By opening the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box from the properties of a network interface in the Network Connection folder. This method of configuring basic IPv6 settings, such as IPv6 address, subnet prefix length, default gateway, and DNS server addresses, is covered in the previous module.
- By using Windows PowerShell cmdlets, such as **New-NetIPAddress** and **Set-NetIPAddress**.
- By using commands from the netsh interface ipv6 context of the **Netsh.exe** command-line utility.


In advanced networking scenarios, you can configure IPv6 using any of the following methods:

- Basic IPv6 settings through the properties of the TCP/IPv6 component
- Windows PowerShell cmdlets
- Netsh command-line utility

## Windows PowerShell cmdlets

In Windows Server 2016, you can configure IPv6 addresses, default gateways, and DNS servers with Windows PowerShell cmdlets, such as:

Set-NetIPAddress	Modifies IP address configuration properties of an existing IP address
<b>Set-NetIPInterface</b>	Modifies IP interface properties
<b>Set-NetIPv6Protocol</b>	Modifies information about the IPv6 Protocol configuration
<b>Set-NetNeighbor</b>	Modifies a neighbor cache entry
<b>Set-NetRouteWindows</b>	Modifies one or more entries in the routing table
<b>Set-DnsClientServerAddress</b>	Modifies DNS server addresses associated with an interface

 **Note:** Windows Server 2016 also includes the alternative Windows PowerShell cmdlets that correspond to each of these cmdlets. These include, for example, **Get-NetIPAddress**, **New-NetIPAddress**, **Remove-NetIPAddress**, and **Set-NetIPAddress**.

You can use the **Get-NetAdapter** cmdlet to display a list of names and indexes of the network interfaces on computers running Windows Server 2016 as follows:

```
PS C:\> Get-NetAdapter | fl Name,ifIndex
Name      : Ethernet
ifIndex   : 12
```

You can also use the **Get-NetIPAddress** cmdlet as follows to display the address information for the interface named Ethernet:

```
PS C:\> Get-NetIPAddress | where {$_.InterfaceAlias -eq "Ethernet"}
IPAddress      : fe80::2025:61fb:b68:c266%12
InterfaceIndex : 12
InterfaceAlias : Ethernet
AddressFamily  : IPv6
Type           : Unicast
PrefixLength   : 64
PrefixOrigin   : WellKnown
SuffixOrigin   : Link
AddressState   : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore
IPAddress      : 172.16.11.75
InterfaceIndex : 12
InterfaceAlias : Ethernet
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Manual
SuffixOrigin   : Manual
AddressState   : Preferred
ValidLifetime  : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore
```

You can use the **New-NetIPAddress** cmdlet to assign a new global unicast IPv6 address with prefix length 64 and also a default gateway address to the Ethernet interface as follows:

```
PS C:\> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 2001:DB8:3FA9::D3:9C5A `
-PrefixLength 64 -DefaultGateway 2001:DB8:3FA9::0C01
IPAddress           : 2001:db8:3fa9::d3:9c5a
InterfaceIndex      : 12
InterfaceAlias       : Ethernet
AddressFamily        : IPv6
Type                 : Unicast
PrefixLength         : 64
PrefixOrigin         : Manual
SuffixOrigin         : Manual
AddressState         : Tentative
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : ActiveStore
IPAddress            : 2001:db8:3fa9::d3:9c5a
InterfaceIndex      : 12
InterfaceAlias       : Ethernet
AddressFamily        : IPv6
Type                 : Unicast
PrefixLength         : 64
PrefixOrigin         : Manual
SuffixOrigin         : Manual
AddressState         : Invalid
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : PersistentStore
```

To verify the result, you can use the **Get-NetIPAddress** cmdlet with the *-AddressFamily* parameter to display only IPv6 addressing information as follows:

```
PS C:\> Get-NetIPAddress -AddressFamily IPv6 | where {$_.InterfaceAlias -eq "Ethernet"}
IPAddress           : fe80::2025:61fb:b68:c266%12
InterfaceIndex      : 12
InterfaceAlias       : Ethernet
AddressFamily        : IPv6
Type                 : Unicast
PrefixLength         : 64
PrefixOrigin         : WellKnown
SuffixOrigin         : Link
AddressState         : Preferred
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : ActiveStore
IPAddress            : 2001:db8:3fa9::d3:9c5a
InterfaceIndex      : 12
InterfaceAlias       : Ethernet
AddressFamily        : IPv6
Type                 : Unicast
PrefixLength         : 64
PrefixOrigin         : Manual
SuffixOrigin         : Manual
AddressState         : Preferred
ValidLifetime        : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime    : Infinite ([TimeSpan]::MaxValue)
SkipAsSource         : False
PolicyStore          : ActiveStore
```

The interface is now multi-homed because it has one link-local IPv6 address and one global IPv6 address.



**Additional Reading:** For more information on using Windows PowerShell, refer to the list of cmdlets for configuring IPv6 at: <http://aka.ms/Sscfek>

## Netsh

In the same way that you use Windows PowerShell cmdlets, you can configure IPv6 settings from the interface of the Netsh.exe utility. With this tool, you can configure IPv6 addresses, default gateways, and DNS servers at the command line by using commands in the **netsh interface ipv6** context.

For example, you could use the following command to configure the IPv6 unicast address 2001:db8:290c:1291::1 on the interface named Local Area Connection and make the address persistent:

```
netsh interface ipv6 add address "Local Area Connection" 2001:db8:290c:1291::1
```

When adding default gateways, you would use the following command to add a default route (::/0) that uses the interface named Local Area Connection with a next-hop address of fe80::2aa:ff:fe9a:21b8:

```
netsh interface ipv6 add route ::/0 "Local Area Connection" fe80::2aa:ff:fe9a:21b8
```

When adding DNS servers, you would use the following command to add a DNS server with the IPv6 address 2001:db8:99:4acd::8 that uses the interface named Local Area Connection:

```
netsh interface ipv6 add dnsserver "Local Area Connection" 2001:db8:99:4acd::8
```



**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

In most cases, IPv6 is configured dynamically by using DHCPv6 or router advertisements. However, you can also configure IPv6 manually with a static IPv6 address. The process for configuring IPv6 is similar to the process for configuring IPv4.

In this demonstration, you will learn how to:

- View the IPv6 configuration by using IPconfig.
- Configure IPv6 on a domain controller and a server.
- Verify that IPv6 communication is functional.

### Demonstration Steps

#### View IPv6 configuration by using IPconfig

1. On **LON-DC1**, open a Windows PowerShell command prompt.
2. Use **ipconfig** to view the link local IPv6 address on Local Area Connection.
3. Use the **Get-NetIPAddress** cmdlet to view network configuration.



### Configure IPv6 on LON-DC1

1. On **LON-DC1**, use **Server Manager** to open the **Network Connections** dialog box, and then click **Ethernet**.
2. Open the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, and enter the following information:
  - o Use the following IPv6 address
    - IPv6 address: **FD00:AAAA:BBBB:CCCC::A**
    - Subnet prefix length: **64**
  - o Use the following DNS server addresses:
    - Preferred DNS server: **::1**

### Configure IPv6 on LON-SVR1

1. On **LON-SVR1**, use **Server Manager** to open the **Network Connections** dialog box, and then click **Ethernet**.
2. Open the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, and then enter the following information:
  - o Use the following **IPv6** address
    - IPv6 address: **FD00:AAAA:BBBB:CCCC::15**
    - Subnet prefix length: **64**
  - o Use the following DNS server addresses:
    - Preferred DNS server: **FD00:AAAA:BBBB:CCCC::A**

### Verify that IPv6 communication is functional

1. On **LON-SVR1**, open a Windows PowerShell command prompt.
2. Use **ipconfig** to view the IPv6 address for Local Area Connection.
3. Use **ping -6** to test IPv6 communication with **LON-DC1**.
4. Use **ping -4** to test IPv4 communication with **LON-DC1**.



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

## Using DHCPv6

When planning to migrate an IT environment from IPv4 to IPv6, you should consider implementing networking services, such as DHCP and DNS, which support the IPv6 environment. When DHCP and DNS services are installed on a computer running Windows Server 2016, these services are enabled by default, and you can configure them to support the IPv6 environment.

### Configuring DHCP

After the DHCP service is installed on a computer running Windows Server 2016, the DHCP console displays two nodes, one for creating and configuring IPv4 address scopes and the other for creating and configuring IPv6 address scopes. The following options are available for configuring a DHCP scope:

- Creating an IPv6 scope
- Creating an IPv6 prefix and preference
- Creating exclusions
- Configuring lease time

After creating the scope, you can also configure settings, such as reservations, and various options at both the scope and server level.

### Configuring DNS

The DNS service in Windows Server 2016 supports IPv6 records that are needed in an IPv6 environment. Computers that already have an IPv6 address configured will register themselves with an AAAA record, which is the record that maps a computer name to its IPv6 address. Computers can register their IPv6 address in DNS, or the DHCP server can register their addresses.

You can also configure static AAAA record entries in DNS by using the DNS console in Windows Server 2016. In the DNS console, you will be asked to provide an AAAA record and the associated IPv6 address for the computer.

If your organization uses reverse lookup zones, you will have to create one reverse lookup zone for each IPv4 and IPv6 address.

## Demonstration: Configuring DHCP for IPv6

IPv6 nodes, similarly to IPv4 nodes, use dynamic DNS to automatically create host records. You can also manually create host records for IPv6 addresses. An IPv6 host (AAAA) resource record is a unique record type and is different from an IPv4 host (A) resource record.

In this demonstration, you will learn how to:

- Create an IPv6 scope in DHCP.
- Configure an IPv6 host (AAAA) resource record for an IPv6 address.
- Verify name resolution for an IPv6 host (AAAA) resource record.

#### DHCP for IPv6 in Windows Server 2016:

- Supports IPv6 by default
- You can configure DHCP by creating and configuring IPv6 scopes and options

#### DNS for IPv6 in Windows Server 2016:

- Supports IPv6 by default
- Computers or DHCP can register AAAA records in DNS
- You can manually create AAAA records in DNS
- You need to create and configure reverse lookup zones for IPv4 and IPv6

## Demonstration Steps

### Configure a scope and scope options in DHCP

1. On **LON-DC1**, from the taskbar, open **Server Manager**, and from **Server Manager**, start the **DHCP Console**.
2. In the **DHCP Console**, in the navigation pane, expand **LON-DC1.adatum.com**, expand and right-click **IPv6**, and then click **New Scope**.
3. Create a new scope with the following properties:
  - o Name: **Headquarters IPv6**
  - o Prefix: **fd00:0000:0000:0000::**
  - o Exclusions Start IPv6 Address: **fd00:0000:0000:0000:0000**
  - o Exclusions End IPv6 Address: **fd00:0000:0000:0000:00ff**
  - o Use default settings for all other pages, and then activate the scope.

### Configure DNS with an IPv6 host (AAAA) resource record

1. On **LON-DC1**, in **Server Manager**, open the **DNS** tool, and then go to the **Adatum.com** forward lookup zone.
2. In DNS Manager, verify that IPv6 addresses have been registered dynamically for **LON-DC1** and **LON-SVR1**.
3. Create a new host record in Adatum.com with the following settings:
  - o Name: **WebApp**
  - o IP address: **FD00:AAAA:BBBB:CCCC::A**

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

1. On **LON-SVR1**, if necessary, open a Windows PowerShell command prompt.
2. Use **Test-NetConnection** to test communication with **WebApp.adatum.com**.

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

**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?

## Lesson 3

# Implementing IPv6 and IPv4 coexistence

From its inception, IPv6 was designed for long-term coexistence with IPv4; in most cases, your network likely will use both IPv4 and IPv6 for many years. Therefore, you need to understand how they coexist.

This lesson provides an overview of the technologies that support the coexistence of the two IP protocols. This lesson also describes the different node types and IP stack implementations of IPv6. Finally, this lesson explains how DNS resolves names to IPv6 addresses and the various types of IPv6 transition technologies.

### Lesson Objectives

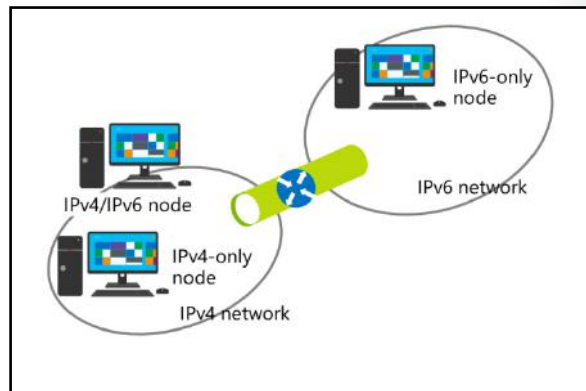
After completing this lesson, you will be able to:

- Describe IP node types.
- Describe the methods that you can use to provide coexistence for IPv4 and IPv6.
- Explain the considerations for planning a native IPv6 environment.
- Explain IPv6 over IPv4 tunneling.

### What are node types?

When planning an IPv6 network, you should know the type of nodes or hosts that are on the network. Describing the nodes in a specific way helps to define their capabilities on the network. It is important to understand the capabilities of each type of node if you use tunneling, because certain kinds of tunnels require specific node types. The descriptions for the various types of nodes are as follows:

- **IPv4-only node.** This is a node that supports only IPv4 and is configured with an IPv4 address only. An IPv4-only node does not support IPv6.
- **IPv6-only node.** This is a node that supports only IPv6 and is configured with an IPv6 address only. An IPv6-only node supports an environment where all other nodes and applications use only IPv6.
- **IPv6/IPv4 node.** This is a node that supports both IPv4 and IPv6. Windows Server 2008 and newer Windows Server operating systems, and Windows Vista and newer Windows client operating systems, use IPv4 and IPv6 by default.
- **IPv4 node.** This is a node that is configured with an IPv4 address, but it can also be an IPv4-only node or an IPv6/IPv4 node.
- **IPv6 node.** This is a node that is configured with an IPv6 address, but it can also be an IPv6-only node or an IPv6/IPv4 node.



You cannot convert all the nodes in an IT infrastructure to IPv6-only nodes because there might be many applications and devices that are still using the IPv4 protocol. Therefore, many organizations deploy IT infrastructures that support coexistence between IPv4 and IPv6 computers, devices, and applications. In a coexistence scenario, you can use various technologies to ensure that IPv4-only nodes can communicate with IPv6-only nodes.

## Options for IPv4 and IPv6 coexistence

Rather than replacing IPv4, most organizations add IPv6 to their existing IPv4 network. Starting with Windows Server 2008 and Windows Vista, Windows operating systems support the simultaneous use of IPv4 and IPv6 through a dual IP layer architecture. The Windows XP and Windows Server 2003 operating systems use dual-stack architecture.

### Dual IP layer architecture

A dual IP layer architecture was implemented beginning with Windows Vista, and is still being used in Windows Server 2016 and Windows 10.

This architecture contains both IPv4 and IPv6 Internet layers with a single implementation of transport layer protocols, such as TCP and UDP. The dual IP layer allows for easier migration to IPv6, and there are fewer files to maintain to provide IPv6 connectivity. IPv6 is also available without adding any new protocols in the network-card configuration.

### Dual stack architecture

Dual stack architecture contains both IPv4 and IPv6 Internet layers, and has separate protocol stacks that contain separate implementations of transport layer protocols, such as TCP and UDP. Tcpi6.sys, the IPv6 protocol driver in Windows Server 2003 and Windows XP, contains a separate implementation of TCP and UDP.

### DNS infrastructure requirements

Just as DNS is used as a supporting service on an IPv4 network, it is also required on an IPv6 network. When you add IPv6 to the network, you need to ensure that you add the records that are necessary to support IPv6 name-to-address and address-to-name resolution. The DNS records that are required for coexistence are:

- Host (A) resource records for IPv4 nodes.
- IPv6 host (AAAA) resource records.
- Reverse lookup pointer (PTR) resource records that map IPv4 and IPv6 nodes to their host names.



**Note:** In most cases, the IPv6 host (AAAA) resource records that IPv6 nodes require are registered in DNS dynamically.

- Windows Server 2012 uses a dual IP layer architecture that supports IPv4 and IPv6 in a single protocol stack
- DNS records required for coexistence are:
  - Host (A) resource records for IPv4 nodes
  - IPv6 host (AAAA) resource records
  - Reverse lookup pointer resource records for IPv4 and IPv6 nodes

When a name can be resolved to both an IPv4 and IPv6 address, both addresses are returned to the client. The client then chooses which address to use based on prefix policies. In these prefix policies, each prefix has a precedence level assigned to it. A higher precedence is preferred over a lower precedence. The following table displays typical prefix policies for Windows Server 2016.

Prefix	Precedence	Label	Description
::1/128	50	0	IPv6 loopback
::/0	40	1	Default gateway
::ffff:0:0/96	10	4	IPv4-compatible address
2002::/16	7	2	6to4
2001::/32	5	5	Teredo
FC00::/7	3	13	Unique local
::/96	1	3	IPv4-compatible address (deprecated)
fec0::/10	1	11	Site local (deprecated)
3ffe::/16	1	12	6Bone (deprecated)



**Note:** You can view the prefix policies in Windows Server 2016 by using the Windows PowerShell **Get-NetPrefixPolicy** cmdlet.

## Considerations for planning a native IPv6 environment

Because of the benefits of IPv6, organizations might plan to migrate all computers and network devices from IPv4 to IPv6. In this scenario, IPv4 will not be used anymore and will be replaced by IPv6 only, which is called a *native IPv6 environment*. However, organizations must ensure that all computers, network devices, and applications support a native IPv6 environment. Some of them, even those that support working with both IPv4 and IPv6, cannot operate in a native IPv6 environment.

Therefore, when planning for a native IPv6 environment, organizations should consider the following:

- **Operating system support.** Windows Vista, Windows Server 2008, and newer Windows client and server operating systems can fully support native IPv6, so organizations can plan their migration to native IPv6 when using Windows 8.1, Windows 10, and Windows Server 2016 operating systems.
- **Router and firewall support.** Organizations must check whether routers and firewalls used in their IT infrastructure support IPv6. In particular, firewall devices or firewall software should be able to detect any type of threat over the IPv6 protocol.

When planning for a native IPv6 environment, organizations should consider the support for:

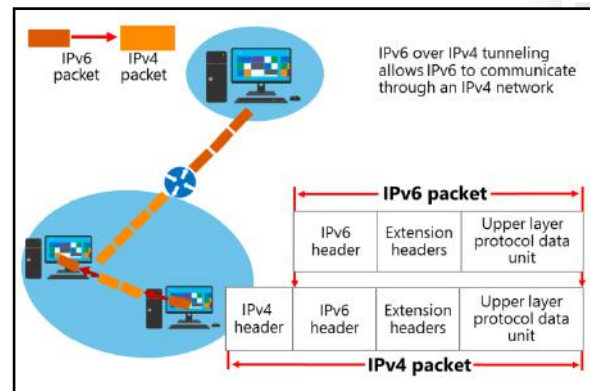
- Operating system
- Routers and firewalls
- Network devices
- Application products
- Custom applications

- **Network device support.** Other network devices such as network printers, network scanners, and network cameras should support IPv6.
- **Application product support.** Some application products support the IPv6 protocol, but they cannot work in a native IPv6 environment. However, they can work in an IPv4 and IPv6 coexistence environment. For example, Microsoft Exchange Server 2013 supports IPv6 but only when IPv4 is also installed and configured, and not in a native IPv6 environment.
- **Custom application support.** Custom applications that are developed in organizations should be designed in a way that supports a native IPv6 environment.

## What is IPv6 over IPv4 tunneling?

*IPv6 over IPv4 tunneling* is the process where IPv6 packets are encapsulated with an IPv4 header so that IPv6 packets can be sent over an IPv4-only infrastructure. Within the IPv4 header:

- The IPv4 Protocol field of the IPv4 header is set to 41 to indicate an encapsulated IPv6 packet.
- The **Source** and **Destination** fields of the IPv4 header are set to IPv4 addresses of the tunnel endpoints. You can configure tunnel endpoints manually as part of the tunnel interface, or they can be derived automatically.



During the IPv6 over IPv4 tunneling process, there is no exchange of messages for tunnel setup, maintenance, or termination. Additionally, tunneled IPv6 packets are not secured. This means that IPv6 tunneling does not need to establish a protected connection first.

You can manually configure IPv6 over IPv4 tunneling, or use automated technologies such as ISATAP, 6to4, or Teredo that implement IPv6 over IPv4 tunneling.

## Lesson 4

# Transitioning from IPv4 to IPv6

Transitioning from IPv4 to IPv6 requires coexistence between the two protocols. Too many applications and services rely on IPv4 for it to be removed quickly. However, several technologies exist that aid in the transition by allowing communication between IPv4-only and IPv6-only hosts. There are also technologies that allow IPv6 communication over IPv4 networks.

This lesson provides information about the ISATAP, 6to4, and Teredo technologies, which help provide connectivity between IPv4 and IPv6 networks. This lesson also addresses PortProxy, which provides compatibility in IPv6 networks for applications that were originally designed for the IPv4 protocol.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe ISATAP, and explain how to configure ISATAP.
- Describe 6to4, and explain how to configure 6to4.
- Describe Teredo, and explain how to configure it.
- Describe PortProxy.
- Describe the transition process from IPv4 to IPv6.

### What is ISATAP?

ISATAP is an address-assignment technology that you can use to provide unicast IPv6 connectivity between IPv6/IPv4 hosts over an IPv4 intranet. IPv6 packets are tunneled in IPv4 packets for transmission over the network. Communication can occur directly between two ISATAP hosts on an IPv4 network, or communication can go through an ISATAP router if one network has only IPv6-only hosts.

An ISATAP address that is based on a private IPv4 address is formatted as shown below:

*[64-bit unicast prefix]:0:5EFE:w.x.y.z*

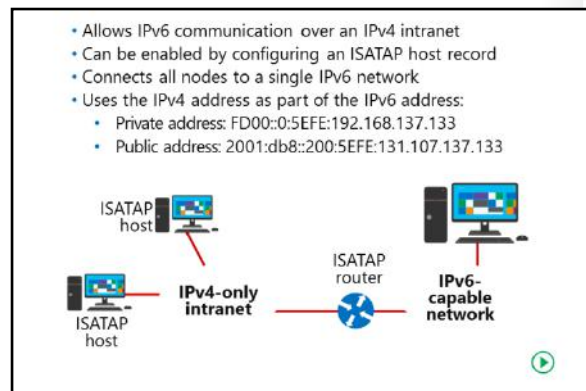
An ISATAP address that is based on a public IPv4 address is formatted as shown below:

*[64-bit unicast prefix]:200:5EFE:w.x.y.z*

For example, FD00::5EFE:192.168.137.133 is an example of a private IPv4 address, and 2001:db8::200:5EFE:131.107.137.133 is an example of a public IPv4 address.


### What is an ISATAP router?

If there are no IPv6-only hosts, the ISATAP router advertises the IPv6 prefix that ISATAP clients use. The ISATAP interface on client computers is configured to use this prefix. When applications use the ISATAP interface to deliver data, the IPv6 packet is encapsulated in an IPv4 packet for delivery to the IPv4 address of the destination ISATAP host.





If there are IPv6-only hosts, the ISATAP router also unpacks IPv6 packets. ISATAP hosts send packets to the IPv4 address of the ISATAP router. The ISATAP router then unpacks the IPv6 packets and sends them on to the IPv6-only network.

 **Note:** All ISATAP nodes are connected to a single IPv6 subnet. This means that all ISATAP nodes are part of the same Active Directory Domain Services (AD DS) site, which might not be desirable. For this reason, you should use ISATAP only for limited testing. For intranet-wide deployment, you should instead deploy native IPv6 support.


## Configuring ISATAP

ISATAP hosts do not require any manual configuration. They can create ISATAP addresses by using standard address autoconfiguration mechanisms. Although the ISATAP component is enabled by default in Windows 8.1 and Windows Server 2016 operating systems, it assigns ISATAP-based addresses only if it can resolve the name ISATAP on your network.

### How to enable ISATAP tunneling

You can initiate ISATAP tunneling in many ways, but the simplest way is to configure an ISATAP host record in DNS that resolves to the IPv4 address of the ISATAP router. Windows hosts that can resolve this name automatically begin by using the specified ISATAP router. By using this method, you can configure ISATAP for several computers simultaneously.

You can also define ISATAP name resolution in a host's file, but we do not recommend this because it is difficult to manage.

 **Note:** By default, DNS servers on Windows Server 2008 or newer Windows Server operating systems have a global query block list that prevents ISATAP resolution, even when the host record is created and properly configured. You need to remove ISATAP from the global query block list in DNS if you are using an ISATAP host record to configure ISATAP clients.

The other ways to configure hosts with an ISATAP router are:

- Use the Windows PowerShell cmdlet **Set-NetIsatapConfiguration Router x.x.x.x**.
- Use **Netsh Interface IPv6 ISATAP Set Router x.x.x.x**.
- Configure the ISATAP **Router Name** Group Policy setting.

### 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?

6to4 is a technology that you can use to provide unicast IPv6 connectivity over the IPv4 Internet. You can use 6to4 to provide IPv6 connectivity between two IPv6 sites or between an IPv6 host and an IPv6 site. However, 6to4 is not suitable for scenarios that require network address translation (NAT). NAT technology translates private IPv4 addresses in a corporate network into public IPv4 addresses.

A 6to4 router provides a site with IPv6 connectivity over the IPv4 Internet. The 6to4 router has a public IPv4 address that is configured on the external interface, and a 6to4 IPv6 address that is configured on the internal interface. To configure client computers, the internal interface advertises the 6to4 network. Any client computer that begins to use the 6to4 network address is a 6to4 host. The 6to4 hosts in the site send 6to4 packets to the 6to4 router for delivery to other sites over the IPv4 Internet.

The IPv6 network address that is used for 6to4 is based on the IPv4 address of the external interface on an IPv6 router. The format of the IPv6 is `2002:WWXX:YYZZ:Subnet_ID:Interface_ID`, where `WWXX:YYZZ` is the colon-hexadecimal representation of `w.x.y.z`, a public IPv4 address.

When a single host on the IPv4 Internet participates in 6to4, it is configured as a host/router. A 6to4 host/router does not perform routing for other hosts, but it does generate its own IPv6 network used for 6to4.

 **Note:** For more information on Network Address Translation – NAT, refer to the topic “Network Address Translation” in Module 5, “Implementing Remote Access,” in this course.

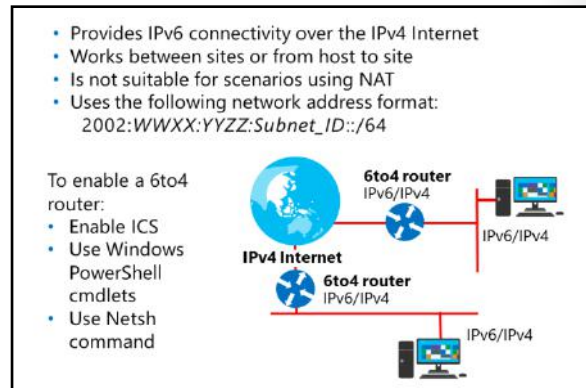
## Configuring 6to4

When configuring 6to4 settings on a computer running Windows 8 or Windows Server 2012, administrators can use `ipconfig/all` command to display the status of the 6to4 tunnel adapter. If the computer is configured with a private IP address, the operating system assumes that the computer is located behind a NAT device. Therefore, the media state of the 6to4 tunnel adapter will have disconnected status because the 6to4 technology cannot work with NAT devices. If the computer is configured with a public IP address, the operating system will enable the 6to4 tunnel adapter so that the computer can be configured to connect to IPv6 by using the 6to4 technology.


## Enabling 6to4 router functionality in Windows operating systems

You can configure Windows Server 2016 as a 6to4 router in the following ways:

- Enable Internet Connection Sharing (ICS). When you enable ICS, Windows Server 2012 is configured automatically as a 6to4 router.




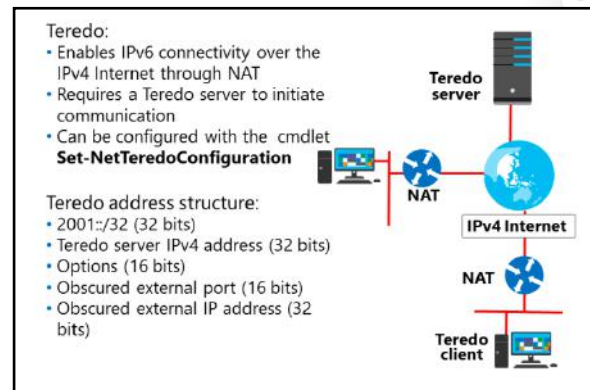
- Use Windows PowerShell. You can use the following Windows PowerShell cmdlets:
  - **Get-Net6to4Configuration** to read the current 6to4 configuration.
  - **Set-Net6to4Configuration** to modify the current 6to4 configuration.
  - **Reset-Net6to4Configuration** to reset the Group Policy Object (GPO) settings for a 6to4 configuration to the state that is not configured. When using Group Policy settings for configuring 6to4, there are three possible states: not configured, enabled, and disabled.
- Use the Netsh command. You can also use the **netsh** command to perform various configuration tasks on 6to4, such as creating and configuring a 6to4 router, relay, and interface.

 **Additional Reading:** For more information about Netsh commands for Interface 6to4, refer to: "Netsh commands for Interface 6to4" at <http://aka.ms/Qqggu7>


## What is Teredo?

*Teredo* is similar to 6to4 in that it allows you to tunnel IPv6 packets over the IPv4 Internet. However, Teredo functions correctly even when NAT is used for Internet connectivity. Teredo is required because many organizations use private IP addresses, which require NAT to access the Internet. If a NAT device can be configured as a 6to4 router, Teredo is not required.

 **Note:** Teredo is used only when native IPv6, 6to4, or ISATAP transitioning technologies do not provide connectivity.



IPv6 communication between two Teredo clients over the IPv4 Internet requires a Teredo server that is hosted on the IPv4 Internet. The Teredo server facilitates communication between the two Teredo clients by acting as a known central point for initiating communication. Typically, hosts behind a NAT device are allowed to initiate outbound communication, but are not allowed to accept inbound communication. To work around this problem, both Teredo clients initiate communication with the Teredo server. After connection is initiated with the Teredo server, and after the NAT device has allowed outbound communication, any further communication occurs directly between the two Teredo clients.

 **Note:** Several public Teredo servers are available for use on the Internet. Windows operating systems use the Microsoft-provided Teredo server at [teredo.ipv6.microsoft.com](http://teredo.ipv6.microsoft.com) by default.

Teredo can also facilitate communication with IPv6-only hosts on the IPv6 Internet by using a Teredo relay. The Teredo relay forwards packets from a Teredo client to the IPv6 Internet.

## Configuring Teredo

You can configure a computer running Windows Server 2016 as a Teredo client, a Teredo relay, or a Teredo server. To configure Teredo, use the Windows PowerShell cmdlet **Set-NetTeredoConfiguration**. The default configuration for Teredo is client. When a computer is configured as a Teredo client, Teredo is disabled when the computer is attached to a domain network. To enable Teredo on the domain network, you must configure the computer as an enterprise client.

By using the **Netsh** command, you can configure Teredo servers other than the default servers on [teredo.ipv6.microsoft.com](http://teredo.ipv6.microsoft.com).

## Teredo address structure

A Teredo address is a 128 bit IPv6 address, but it uses a different structure than typical unicast IPv6 addresses. The structure is as follows:

- **2001::/32 (32 bits)**. This is the Teredo-specific prefix that is used by all Teredo addresses.
- **Teredo server IPv4 address (32 bits)**. This identifies the Teredo server.
- **Options (16 bits)**. There are several options that describe the communication configuration, such as whether the client is behind NAT.
- **Obscured external port (16 bits)**. This is the external port used for communication by the NAT device for this communication. It is obscured to prevent the NAT device from translating it.
- **Obscured external IP address (32 bits)**. This is the NAT device's external IP address. It is obscured to prevent the NAT device from translating it.



**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?

Application developers use specific network application programmer interfaces (APIs) to access network resources when they are writing applications. Modern APIs use either IPv4 or IPv6, and leave the responsibility of choosing the IP version to the operating system. However, some earlier applications use APIs that can use only IPv4.

You use the PortProxy service to allow applications that do not support IPv6 to communicate with IPv6 hosts. You enable PortProxy on the server where the application is running. Incoming IPv6 packets for the application are translated to IPv4 and then passed on to the application.

You can also use PortProxy as a proxy between IPv4-only and IPv6-only hosts. To do this, you must configure DNS to resolve the name of the remote host as the address of the PortProxy computer. For example, an IPv4-only host would resolve the name of an IPv6-only host as the IPv4 address of the PortProxy computer. Packets would then be sent to the PortProxy computer, which would proxy them to the IPv6-only computer.

### Use PortProxy to:

- Provide IPv6-only hosts with access to IPv4-only applications
- Provide access between IPv4-only and IPv6-only hosts

### Limitations of PortProxy:

- Only TCP applications
- Cannot change embedded address information

PortProxy has the following limitations:

- It is limited to TCP connections only. It cannot be used for applications that use UDP.
- It cannot change address information that is embedded in the data portion of the packet. If the application, such as a File Transfer Protocol (FTP) application, embeds address information in the data portion, PortProxy will not work.

You can configure PortProxy on Windows Server 2016 by using **netsh interface portproxy**. However, we generally recommend using a tunneling technology instead of PortProxy.

## Process for transitioning to IPv6-only networks

The industry-wide migration from IPv4 to IPv6 is expected to take considerable time. This was taken into account when IPv6 was designed and, as a result, the transition plan for IPv6 is a multistep process that allows for extended coexistence.

To achieve the goal of designing an IPv6-only environment, you can use the following general guidelines:

- Upgrade your applications to be independent of either IPv6 or IPv4. For example, you can change applications to use new Windows Sockets APIs so that name resolution, socket creation, and other functions are independent regardless of whether you are using IPv4 or IPv6.
- Upgrade routing infrastructure for native IPv6 routing. You must upgrade routers to support both native IPv6 routing and IPv6 routing protocols.
- Upgrade devices to support IPv6. The majority of current networking hardware supports IPv6, but many other types of devices do not. You need to verify that all network attached devices, such as printers and scanners, also support IPv6.
- Update the DNS infrastructure to support IPv6 address and pointer (PTR) resource records. You might have to upgrade the DNS infrastructure to support the new IPv6 host address (AAAA) resource records (required) and pointer (PTR) resource records in the IP6.ARPA reverse domain, but this is optional. Additionally, ensure that the DNS servers support both DNS traffic over IPv6 and DNS dynamic update for IPv6 host address resource records so that IPv6 hosts can register their names and IPv6 addresses automatically.
- Upgrade hosts to IPv6/IPv4 nodes. You must upgrade hosts to use both IPv4 and IPv6. This allows hosts to access both IPv4 and IPv6 resources during the migration process.

To transition from IPv4 to IPv6, you must:

- Update applications to support IPv6
- Update routing infrastructure to support IPv6
- Update devices to support IPv6
- Update DNS with records for IPv6
- Upgrade hosts to IPv4/IPv6 nodes

Most organizations will probably add IPv6 to an existing IPv4 environment and continue to have coexistence for an extended time. Many earlier applications and devices that do not support IPv6 are still in existence, and coexistence is much simpler than using transition technologies such as ISATAP. You should remove IPv4 only after resources that depend on it are either removed or updated to use IPv6.

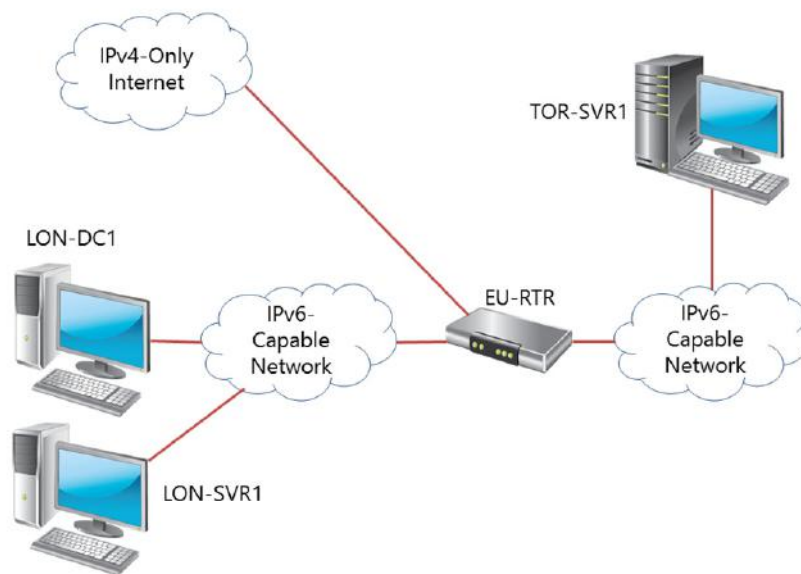
IPv6 is enabled by default for Windows Vista and newer Windows client operating systems, and Windows Server 2008 and newer Windows Server operating systems. As a best practice, you should not disable IPv6 even if your network is IPv4 only. There are operating system components such as Remote Assistance and DirectAccess that will not work if IPv6 is disabled.

## Lab: Configuring and evaluating IPv6 transition technologies

### Scenario

Several key applications that A. Datum Corporation uses have recently implemented IPv6 support. As a result, IT management at A. Datum is considering implementing IPv6 on its internal network. To test various IPv6/IPv4 integration strategies, A. Datum has implemented a test network environment between the three main company locations. You need to configure and test the network connectivity by using various integration technologies.

This is the layout of the completed test environment.



**FIGURE 3.1: END RESULT OF THE LAB**

### Objectives

After completing this lab, you will be able to:

- Review the default IPv6 configuration.
- Create and configure IPv6 configuration.
- Configure network integration by using ISATAP.
- Configure native IPv6 connectivity.
- Configure network integration by using 6to4 integration.

## Lab Setup

Estimated Time: **75 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-TOR-SVR1**, and **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Virtual machine: **20741A-INET1**

User name: **Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - o User name: **Administrator**
  - o Password: **Pa\$\$w0rd**
  - o Domain: **Adatum**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-LON-CL1**, **20741A-EU-RTR**, and **20741A-TOR-SVR1**.
6. Sign in to **20741A-INET1** by using the following credentials:
  - o User name: **Administrator**
  - o Password: **Pa\$\$w0rd**

## Exercise 1: Reviewing the default IPv6 configuration

### Scenario

To understand how IPv6 works and how the planned modifications will affect network traffic, you first must identify and document the default IPv6 configuration at A. Datum Corporation.

The main tasks for this exercise are as follows:

1. Identify the default IPv6 configuration.
2. Test link-local address connectivity.

### ► Task 1: Identify the default IPv6 configuration

1. On **LON-DC1**, from **Server Manager**, open the **DNS** console, and notice that **LON-DC1** has one IPv6 address preconfigured for the lab. Also notice that there are no AAAA records registered for any other computer in the Adatum.com zone.
2. On **LON-DC1**, open a Windows PowerShell command prompt.

3. Use **ipconfig** to view the link-local IPv6 address on **Ethernet**. Note this address.

4. Use the **Get-NetIPAddress** cmdlet to view the network configuration.

5. Repeat steps 2 to 4 on **LON-SVR1** and **TOR-SVR1**.



**Note:** Windows client and server operating systems do not register link-local IPv6 addresses in DNS.

### ► Task 2: Test link-local address connectivity

1. Switch to **LON-DC1**.

2. At the Windows PowerShell command prompt, type the **ping** command, followed by the **LON-SVR1** link-local IPv6 address.



**Note:** The **LON-SVR1** link-local IPv6 address was displayed in step 4 of the previous task.

3. At the Windows PowerShell prompt, type the **Test-NetConnection** cmdlet, followed by the **LON-SVR1** link-local IPv6 address.



**Note:** The **LON-SVR1** link-local IPv6 address was displayed in step 4 of the previous task.

4. "Ping Succeeded: True" from the **LON-SVR1** link-local IPv6 address is displayed.

5. At the Windows PowerShell command prompt, type the **Test-NetConnection** cmdlet followed by the **TOR-SVR1** link-local IPv6 address.



**Note:** Note that the **TOR-SVR1** link-local IPv6 address was in the previous task.



**Note:** When typing the IPv6 address, do not type the percent sign (%) and do not type the numbers after the %.

6. The following is displayed: the warning message "DestinationHostUnreachable," and the result of the diagnostics that displays the message "Ping Succeeded: False." This is because the link-local IPv6 addresses are not routable and can be used for communication only on a local subnet.

**Results:** After completing the exercise, you should have reviewed the default IPv6 configuration and test how computers communicate by using link-local IPv6 addresses.



## Exercise 2: Implementing DHCPv6

### Scenario

The company A. Datum Corporation is planning to implement IPv6 throughout its internal network. To manage the IPv6 addresses assigned to clients, you will configure DHCP to assign the IPv6 addresses.

The main tasks for this exercise are as follows:

1. Create and configure DHCPv6 scopes.
2. Verify configuration by testing allocation of IPv6 addresses.

#### ► Task 1: Create and configure DHCPv6 scopes

1. On **LON-DC1**, from the taskbar, open **Server Manager**, and from **Server Manager**, start the **DHCP** console.
2. In the **DHCP** console, in the navigation pane, expand **lon-dc1.adatum.com**, expand and right-click **IPv6**, and then click **New Scope**.
3. Create a new scope with the following properties:
  - Name: **Headquarters IPv6**
  - Prefix: **fd00:0000:0000:0000::**
  - Exclusions Start IPv6 Address: **fd00:0000:0000:0000:0000**
  - Exclusions End IPv6 Address: **fd00:0000:0000:0000:00ff**
  - Use default settings for all other pages, and then activate the scope.

#### ► Task 2: Verify configuration by testing allocation of IPv6 addresses

1. Switch to **LON-CL1**.
2. Open **Windows PowerShell**, and then run the **Ipconfig /renew6** command.
3. Confirm that the IPv6 address is in the **FD00:0000:0000:0000::/64** range.

**Results:** After completing the exercise, you should have configured DHCP to assign IPv6 addresses, and verified that the addresses are assigned correctly.

## Exercise 3: Configuring network integration by using ISATAP

### Scenario

The first option for testing IPv4 to IPv6 connectivity is to implement an ISATAP router. You will configure an ISATAP router and verify that users can connect to other subnets by using IPv6 with the router in place.

The main tasks for this exercise are as follows:

1. Configure an ISATAP router.
2. Verify the ISATAP configuration on the client.
3. Verify network connectivity to other subnets.

### ► Task 1: Configure an ISATAP router

1. On **LON-DC1**, in the **Windows PowerShell** window, enter the following command.

```
dnscmd /config /globalqueryblocklist wpad
```

This step removes the name **ISATAP** from the default global query block list.

2. In the **DNS** console, restart the **DNS** service.
3. In the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones**, and then in the **Adatum.com** zone, create a new **A** record with the host name **isatap** and IP address **172.16.0.1**.
4. Switch to **EU-RTR**.
5. Use the following **Windows PowerShell** command to configure the IP address of London\_Network as the ISATAP router:

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

6. Use the following command to identify the interface index of the ISATAP interface that has **172.16.0.1** in the link-local address:

```
Get-NetIPAddress | Format-Table  
InterfaceAlias,InterfaceIndex,IPv6Address
```

Record the interface index here:



**Note:** As an optional step, you might consider modifying the preceding cmdlet so that the output of the cmdlet will be stored in a text file. This will make it easier for you to search for the InterfaceIndex value.

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address >  
C:\Results.txt
```

This cmdlet will create the **Results.txt** file in the C drive of **EU-RTR**. The file contains the results from running the cmdlet. Search the **Results.txt** file for the interface that has an IPv6 address, which includes **172.16.0.1**.

7. Use the **Get-NetIPInterface** cmdlet to verify the following on the ISATAP interface:
  - Forwarding is enabled
  - Advertising is disabled

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore |  
Format-List
```

8. The ISATAP interface for an ISATAP router must have forwarding enabled and advertising enabled. Use the following **Set-NetIPInterface** cmdlet to enable router advertisements on the ISATAP interface.

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

9. Create a new IPv6 network that will be used for the ISATAP network. Use the following **New-NetRoute** cmdlet to configure a network route for the ISATAP interface.

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64
-Publish Yes
```

10. Use the following **Get-NetIPAddress** cmdlet to verify that the ISATAP interface has an IPv6 address on the 2001:db8:0:2::/64 network, and then close the **Windows PowerShell** window.

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

### ► Task 2: Verify the ISATAP configuration on the client

1. Restart **TOR-SVR1** and **LON-SVR1**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On **TOR-SVR1**, open a Windows PowerShell command prompt, and then type **Get-NetIPAddress**. Verify that the tunnel adapter has received an IPv6 address starting with **2001**.
3. On **LON-SVR1**, open a Windows PowerShell command prompt, and then type **Get-NetIPAddress**. Verify that the tunnel adapter has received an IPv6 address starting with **2001**.
4. On **LON-DC1**, in the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones**, right-click **Adatum.com**, and then click **Refresh** to verify that there are new AAAA records registered.

### ► Task 3: Verify network connectivity to other subnets

- On **TOR-SVR1**, use the following **Test-NetConnection** command to test connectivity to the ISATAP address for **LON-SVR1**.

```
Test-NetConnection 2001:db8:0:2:0:5efe:172.16.0.11
```

Notice that the message "Ping Succeeded: True" is received from **LON-SVR1** Tunnel ISATAP adapter's IPv6 address.

**Results:** After completing this exercise, you should have configured an ISATAP router to allow communication between an IPv6-only network and an IPv4-only network.

## Exercise 4: Configuring native IPv6 connectivity

### Scenario

The second option for configuring IPv6 connectivity is enabling native IPv6 functionality. You will configure the router to support native IPv6 connectivity between the Sydney office and the London office, and verify that users can connect to other subnets by using native IPv6.

The main tasks for this exercise are as follows:

1. Configure native IPv6 connectivity.
2. Verify the native IPv6 configuration.
3. Verify network connectivity to other subnets.

### ► Task 1: Configure native IPv6 connectivity

Before configuring native IPv6 connectivity, you have to perform steps 1 to 12 to remove the ISATAP that you configured in the previous exercise. This is because ISATAP is not required in the native IPv6 environment.

1. On **EU-RTR**, open the **Windows PowerShell** window.
2. In the **Windows PowerShell** window, run the following cmdlet. In the cmdlet, replace **IndexYouRecorded** with the value recorded in Exercise 3, Task 1, Step 10.

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Disabled
```

3. In the **Windows PowerShell** window, run the following cmdlet.

```
Remove-NetRoute -InterfaceIndex IndexYouRecorded -Publish Yes
```

Type **Y**, and then press Enter each time when asked.

4. On **LON-DC1**, in the **DNS** console tree, in the **DNS\LON-DC1\Forward Lookup Zones \Adatum.com** zone, delete the record for **isatap**.
5. Open the **Windows PowerShell** window, and restart the **IP Helper** service by running the following cmdlet.

```
Restart-Service iphlpsvc
```

6. Switch to **EU-RTR**.
7. Repeat step 5 on **EU-RTR**.
8. Switch to **TOR-SVR1**.
9. Repeat step 5 on **TOR-SVR1**.
10. Switch to **LON-SVR1**.
11. Repeat step 5 on **LON-SVR1**.
12. Switch to **LON-DC1**.
13. In the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones\adatum.com**, and then refresh the information in the **DNS** console to verify that there are no AAAA records registered. If there are still AAAA records registered, repeat steps 4 through 12.

In the following steps, you will configure **EU-RTR** as an advertising and forwarding IPv6 router that advertises native IPv6 prefixes to the London and Toronto subnets.

1. On **EU-RTR**, click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, run the following command.

```
Set-NetIPInterface -AddressFamily ipv6 -InterfaceAlias "London_Network" -Advertising enabled - AdvertiseDefaultRoute enabled
```

3. In the **Windows PowerShell** window, run the following command.

```
Set-NetIPInterface -AddressFamily ipv6 -InterfaceAlias "NA_WAN" -Advertising enabled - AdvertiseDefaultRoute enabled
```

- In the **Windows PowerShell** window, run the following command.

```
New-NetRoute -InterfaceAlias "London_Network" -DestinationPrefix 2001:db8::/64 -Publish Yes
```

- In the **Windows PowerShell** window, run the following command.

```
New-NetRoute -InterfaceAlias "NA_WAN" -DestinationPrefix 2001:db8:0:2::/64 -Publish Yes
```

- In the **Windows PowerShell** window, type the following command, and then press Enter.

```
Get-NetIPAddress
```

- In the **Windows PowerShell** window, document the link-local IPv6 address of **London\_Network** adapter. This IPv6 address will be used in the next step.
- In the **Windows PowerShell** window, type the following command, and then press Enter. When typing the command, replace **link-local address of EU-RTR "London\_Network" interface** with the IPv6 address you documented in previous step. When typing the IPv6 address, do not type the percent sign (%) sign and do not type the numbers after the %.
- In the **Windows PowerShell** window, run the following command.

```
New-NetRoute -InterfaceAlias "London_Network" -DestinationPrefix ::/0 -NextHop link-local address of EU-RTR "London_Network" interface -Publish yes
```

### ► Task 2: Verify the native IPv6 configuration

- Switch to **EU-RTR**, and in the **Windows PowerShell** window, run the following command:

```
Get-NetIPAddress
```

- Notice the new IPv6 address starting with **2001:db8::** assigned to the **London\_Network** interface, and the address starting with **2001:db8:0:2** assigned to the **NA\_Network** interface. Notice the link-local address of the **London\_Network** interface.
- Switch to **LON-SVR1**, and in the **Windows PowerShell** window, run the following command.

```
Get-NetIPAddress
```

- Notice the new IPv6 address starting with **2001:db8::** and the default gateway of **EU-RTR** link-local address.
- Switch to **LON-DC1**, in the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones \Adatum.com**, and refresh the information in the DNS console to verify that there are new AAAA records registered.

### ► Task 3: Verify network connectivity to other subnets

- On **TOR-SVR1**, open the **Windows PowerShell** window.
- In the **Windows PowerShell** window, run the following command.

```
ipconfig /flushdns
```

- In the **Windows PowerShell** window, run the following command.

```
Test-NetConnection LON-DC1
```

A successful name resolution to the **LON-DC1** IPv6 address and the "PingSucceeded:True" reply should be displayed.

4. From the **Start** menu, open Internet Explorer, and in the address bar, type **http://LON-SVR1.adatum.com**. The default **Microsoft Internet Information Services (IIS)** webpage for **LON-SVR1** is displayed.
5. Switch to **LON-SVR1**.
6. On **LON-SVR1**, in the **Windows PowerShell** window, run the following command.

```
ipconfig /flushdns
```

7. In the **Windows PowerShell** window, run the following command.

```
Test-NetConnection EU-RTR
```

You should see a successful name resolution to the **EU-RTR** IPv6 address and the **PingSucceeded:True** reply.

8. In the **Windows PowerShell** window, run the following command.

```
Test-NetConnection TOR-SVR1.adatum.com
```

The successful name resolution to the **EU-RTR** IPv6 address and the "PingSucceeded:True" reply is displayed. Notice that **LON-SVR1** is using the **TOR-SVR1** IPv6 address, rather than the IPv4 address.

**Results:** After completing this exercise, you should have configured native IPv6 connectivity and tested whether the computers can communicate by using IPv6 addresses.

## Exercise 5: Configuring 6to4 Connectivity

### Scenario

The final option for configuring IPv6 integration with IPv4 is configuring 6to4 connectivity so that clients from the IPv4-only Internet can connect to computers on the internal network at A. Datum.

The main tasks for this exercise are as follows:

1. Configure 6to4 connectivity.
2. Verify 6to4 configuration.
3. Verify network connectivity to other subnets.

#### ► Task 1: Configure 6to4 connectivity

1. On **EU-RTR**, open the **Windows PowerShell** window.
2. In the **Windows PowerShell** window, run the following command.

```
Set-Net6to4Configuration -State enabled
```

3. In the **Windows PowerShell** window, run the following command.

```
Set-NetIPInterface -InterfaceAlias "6to4 Adapter" -Forwarding enabled
```

- In the **Windows PowerShell** window, run the following command.

```
Set-NetIPInterface -InterfaceAlias "London_Network" -Forwarding enabled
```

- Switch to **INET1**, and then start **Server Manager**.
- Open the **DNS** console, create a new forward lookup zone named **ipv6.microsoft.com**, and then choose an option where dynamic updates should not be allowed.
- In the **DNS** console, in the **ipv6.microsoft.com** zone, create an **A** record with the name **6to4** and IP address **131.107.0.10**.

### ► Task 2: Verify 6to4 configuration

- On **EU-RTR**, in the **Windows PowerShell** window, run the type **Get-NetIPAddress** command. Notice the **2002:836b:a::836b:a** IPv6 address assigned to the **6TO4 Adapter**.

This is a 6to4 address that **EU-RTR** automatically assigns based on the public IPv4 address **131.107.0.10**, which is assigned to the **Internet** interface.



**Note:** Note the IPv6 address of the **6to4** adapter, where **836b:a** in the hexadecimal system corresponds to **131.107.0.10**. That is:

**83** hexadecimal = **131** decimal

**6b** hexadecimal = **107** decimal

**0** hexadecimal = **0** decimal (preceding zero is skipped)

**a** hexadecimal = **10** decimal

- Switch to **LON-CL1**.
- To move the client from the intranet to the public network, on **LON-CL1**, open **Control Panel**, open **Network and Sharing Center**, and then disable **London\_Network** adapter, and then enable **Internet** adapter.
- Close the **Network Connections** window.
- On **LON-CL1**, in the **Windows PowerShell** window, run the **Get-NetIPAddress** command.  
Notice the address starting with **2002:836b:** assigned to the **6TO4 Adapter**. This is a 6to4 address corresponding to its public IPv4 address. Also notice that the default gateway for the **6TO4 Adapter** is set to **2002:836b:a::836b:a**, a 6to4 address assigned to **EU-RTR**.
- On **EU-RTR**, in the **Windows PowerShell** window, run the **Get-NetIPAddress** command. Notice and document the address starting with **2001:db8::** assigned to the **London\_Network** interface, because it will be used in the next task.
- On **LON-DC1**, in the **Windows PowerShell** window, run the **Get-NetIPAddress** command. Notice and document the address starting with **2001:db8::** assigned to the **Ethernet** interface, because it will be used in the next task.

### ► Task 3: Verify network connectivity to other subnets

- Switch to **LON-CL1**.
- On **LON-CL1**, run the following Windows PowerShell command.

```
Test-NetConnection EU-RTR IPv6 address
```



**Note:** Use the IPv6 address for **EU-RTR** on the London\_Network adapter you documented in the previous task.

3. A message "Ping Succeeded: True" should be displayed in the reply.
4. Run the following Windows PowerShell window command.

```
Test-NetConnection LON-DC1 IPv6 address
```



**Note:** Use the IPv6 address for **LON-DC1** on the Ethernet adapter you documented in the previous task.

5. A message "Ping Succeeded: True" should be displayed in the reply.

**Results:** After completing this exercise, you should have configured 6to4 transition technology and verified the connectivity when using the 6to4 transition technology.

#### ► Task 4: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-EU-RTR**, **20741A-LON-SVR1**, **20741A-LON-CL1**, **20741A-TOR-SVR1**, and **20741A-INET1**.

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

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



## Module Review and Takeaways

### Review Questions

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

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

**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?

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

### 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.

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 4

## Implementing DNS

### Contents:

Module Overview	4-1
<b>Lesson 1:</b> Implementing DNS servers	4-2
<b>Lesson 2:</b> Configuring zones in DNS	4-21
<b>Lesson 3:</b> Configuring name resolution between DNS zones	4-27
<b>Lab A:</b> Planning and implementing name resolution by using DNS	4-33
<b>Lesson 4:</b> Configuring DNS integration with AD DS	4-37
<b>Lab B:</b> Integrating DNS with AD DS	4-44
<b>Lesson 5:</b> Configuring advanced DNS settings	4-46
<b>Lab C:</b> Configuring advanced DNS settings	4-62
Module Review and Takeaways	4-67

## Module Overview

The Domain Name System (DNS) is the foundation name service in the Windows Server 2016 operating system. DNS provides name resolution services, and it enables DNS clients to locate network services, such as Active Directory Domain Services (AD DS) domain controllers, global catalog servers, and messaging servers. If you configure your DNS infrastructure poorly or it does not work correctly, these important network services will be inaccessible to your network servers and clients. Therefore, it is vital that you understand how to deploy, configure, manage, and troubleshoot this critical service.

### Objectives

After completing this module, you will be able to:

- Install and manage a DNS Server.
- Configure DNS zones.
- Configure name resolution between zones.
- Integrate DNS with AD DS.
- Configure advanced DNS settings.

## Lesson 1

# Implementing DNS servers

The DNS infrastructure is the basis for name resolution on the Internet and in Active Directory Domain Services (AD DS) domains that are based on the Windows Server operating system. This lesson provides guidance and information about what you require to configure the DNS server role, and it explains the basic functions of a DNS server.

### Lesson Objectives

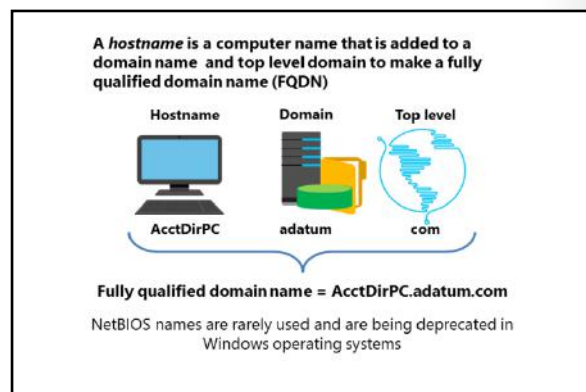
After completing this lesson, you will be able to:

- Describe how DNS name resolution works.
- Describe DNS components.
- Explain DNS zones and records.
- Describe how to install and configure the DNS Server role.
- Describe how DNS client are configured.
- Describe the tools and techniques used to troubleshoot name resolution.
- Describe how to manage DNS services.
- Describe how to troubleshoot name resolution.
- Describe how to test DNS servers.
- Describe how to test for proper functionality of a DNS server.

### How does DNS name resolution work?

The Transmission Control Protocol/Internet Protocol (TCP/IP) set of protocols identifies source and destination computers by their IP addresses. However, computer users generally are much better at using and remembering names than numbers. Because of this, administrators usually assign names to computers. Administrators then link these names to computer IP addresses in a name resolution system such as DNS. These names are in *host name* format, for example, *dc1.contoso.com*.

When you use DNS, users on your network can locate network resources by typing in user-friendly names (for example, *www.microsoft.com*), which the computer then resolves to an IP address. The benefit is that Internet Protocol version 4 (IPv4) addresses might be difficult to remember (for example, *131.107.0.32*), while a domain name typically is easier to remember. In addition, you can use host names that do not change, while you can change the underlying IP addresses to suit your organizational needs. Moreover, users are not the only ones who type in a friendly name in a browser that requires resolution to a IP address; many programs and system components also might be configured with a computer name to make a connection, and these names must also be resolved. Even the DNS server itself, when communicating replies to queries sent by other devices, needs to resolve the device IP address.



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

Originally, there was one file on the Internet that contained a list of all domain names and their corresponding IP addresses. This list quickly became too long to manage and distribute. DNS was developed to solve the problems associated with using a single Internet file. With the adoption of Internet Protocol version 6 (IPv6), DNS becomes even more important, because IPv6 addresses are even more complex than IPv4 addresses, for example, `2001:db8:4136:e38c:384f:3764:b59c:3d97`.

DNS groups information about network resources into a hierarchical structure of domains.



**Note:** Both AD DS and DNS use the term domain. In AD DS, domains are a logical construct of AD DS, which is made up of objects, such as user, group and computer accounts, authentication and authorization services, and other identity-related services. In DNS, a domain refers to a level in the hierarchy that makes up the entire DNS system.

The hierarchical structure of domains is an inverted tree structure. It begins with a root domain at its apex, and descends into separate branches with common levels of parent domains, and then descends downward into individual child domains.

As the Internet has grown, so has the number of domains from different countries/regions. All countries/regions in the DNS registry have top-level country codes. The governing bodies in these countries/regions can further create second-level domains that reflect categories such as `.com`, `.org`, and `.net`. For example, the United Kingdom (UK) has a top-level domain named `.uk`, and has further broken this down to the second level for various activities. A commercial company in the UK might therefore have a fully qualified domain name (FQDN) of `companyname.com.uk`. This domain would not be the same as `companyname.com`, which is at an entirely different level.

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

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

In addition to resolving host names to IP addresses, you can use DNS to:

- Locate domain controllers and global catalog servers. This is used when signing in to AD DS.
- Resolve IP addresses to host names. This is useful when a log file contains only the IP address of a host.
- Locate network services that register their names to DNS.

### Name type

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

## Host names

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

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

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

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

## Creating host names

When you select host names, you should create host names that are intuitive and relatively easy to remember, yet still unique. The following lists some best practices to implement when you create host names:

- Select computer names that are easy for users to remember.
- Identify the owner of a computer in the computer name. For example, JOHN-DOE-01 indicates that John Doe uses the computer.
- Select names that describe the computer's purpose. For example, a file server named PAST-ACCOUNTS-01 indicates that the file server stores information related to past accounts.
- Do not use character case to convey the computer's owner or purpose. DNS is not case-sensitive.
- Match the Active Directory domain name to the primary DNS suffix of the computer name.
- Use unique names for all computers in your organization. Do not assign the same computer name to different computers in different DNS domains.

## How names are resolved on the Internet

A name resolution client query can take many paths, depending on whether it is public or private, and how the DNS infrastructure is designed. This section examines how the process operates in relation to Internet domain names because it is a common scenario that most people have encountered even though they might not be aware of how it operates.

When DNS names are resolved on the Internet, a whole system of computers is used instead of just a single server. There are 13 root servers on the Internet that are responsible for managing the overall structure of DNS resolution. When you register a domain name on the Internet, you are paying for the privilege of being part of this system.

The name resolution process for the name *www.microsoft.com* is as follows:

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

You can change the name resolution process in several ways, but two common options that you can use are as follows:

- **Caching.** After a local DNS server resolves a DNS name, it will cache the results for approximately 24 hours. Later resolution requests for the DNS name are given the cached information.
- **Forwarding.** A DNS server can be configured to forward DNS requests to another DNS server instead of querying root servers. For example, requests for all Internet names can be forwarded to a DNS server at an Internet service provider (ISP), which performs the rest of the resolving chain on behalf of the requesting DNS server and returns the answer. This arrangement works well because the local DNS server does not have to be able to communicate with every DNS server on the Internet.

## DNS components

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

DNS is the Microsoft preferred choice for resolving host names to IP addresses. It is a hierarchical structure and automates the mechanisms of registering, identifying, caching, and resolving host names and IP addresses. It is routable, and it operates successfully across different subnets and the Internet.

The automated nature of this process greatly simplifies and streamlines the maintenance and management of name resolution. However, incorrectly configuring DNS can result in poor network performance and increased computer startup times. That is mainly because of two issues: unable to locate domain controllers, and replication of database information.

Before you learn how DNS works, you first must understand some core concepts.

### DNS naming structure

The naming structure used in DNS is called the *DNS namespace*. It is hierarchical, which means that it starts with a root domain. That root domain can itself have any number of subdomains underneath it. Each subdomain can, in turn, have any number of subdomains underneath it.

The domain names themselves can be either public (Internet facing) or private. If they are private, you can decide on your own how to define your namespace. If they are public, you have to work with the Internet Corporation for Assigned Names and Numbers (ICANN) or other Internet naming registration authorities that can delegate, or sell, unique names to you. From these names, you can create subnames.

At the very root, DNS has a unique namespace, indicated by an empty string space " ". Preceding this is a single dot '.'. Below this, in the public namespace, is one of several other top-level domain namespaces. There are three kinds of top-level domains in the public namespace:

- **Organizational.** This domain is based on the function of an organization. For example, .com, .net, .org, and .edu. There are more than 20 variations, and these are distributed and managed by ICANN.
- **Geographical.** These are designated per country/region. For example, .uk for United Kingdom (co.uk is the .com equivalent for UK-based businesses), .it for Italy, .de for Germany, and .jp for Japan. There are more than 200 of these registered. Typically, each country/region has its own domain registration service.

- DNS namespace is a hierarchical naming structure that provides multiple identifiers for each network node that can be identified relative to the root domain.

computer01.unitedstates.microsoft.com

- DNS infrastructure components include:
  - DNS server
  - DNS zone
  - DNS resolvers
  - Resource records

- Reverse domains. These are special domains used in resolving addresses to names—that is, a reverse lookup. These domains are in the name.name format, such as *addr.arpa* and *ip6.arpa*.

Typically, underneath these top-level domains, there are subdomains. For example, *microsoft.com*, *university.edu*, or *government.gov*. These subdomains can also have subdomains, such as *unitedstates.microsoft.com* or *physicsdept.university.edu*. Every computer and network node can be identified by its FQDN. For example, *Computer01.unitedstates.microsoft.com*.

Some of the main infrastructure components that are spanning a DNS infrastructure, or that you use to build a DNS infrastructure are as follows:

- DNS server. Contains a database of host names and IP addresses. It responds to client requests and provides required mapping information. It can cache information for other domains. When it does not have the needed mapping information, it can forward DNS client requests to another DNS server.
- DNS zones. A DNS infrastructure is broken up into zones, each of which is allocated a DNS server to own, or potentially be an *authoritative* server for and process requests for that particular zone. For example, one DNS server might be responsible for the *paris.europe.microsoft.com* DNS zone and another DNS server might be responsible for the *berlin.europe.microsoft.com*. It is possible to have variations on the number of servers per zone and across multiple zones, and also different authority levels. You can also have different kinds of zones, such as:
  - Forward lookup zones. Resolves host names to IP addresses.
  - Reverse lookup zones. Resolves IP addresses to host names—that is, the opposite of what happens in forward lookup zones. An organization typically controls the reverse lookup zones for its internal network. However, some mappings for external IP addresses obtained from an ISP might be managed by the ISP.

It is important to understand that the zone is the level of naming delegation. If a DNS server holds a zone, either authoritative or not, it will not query other servers about names in that zone. The DNS server considers its information up to date and valid (unless a sub-namespace was delegated). Administrative delegation—who is in charge of doing what with that namespace—is also important. It is also the scope for replication. In other words, a server cannot contain a part of the zone—either it holds a copy or it does not.

- DNS forwarders/delegations
  - DNS forwarders are queries that the DNS server send up stream when it cannot resolve a request locally. A DNS server only forwards data when it has not been able to resolve a query with its own authoritative data or from its own cache.
  - DNS delegation is when a DNS server delegates management of part of its namespace to another DNS server.

How DNS servers forward, delegate, and replicate the name resolution databases can have a significant effect on query response times. This is something that should be carefully considered before deployment.

- DNS resolver. Provides the service to query for host-to-IP address mappings. The DNS client service in the Windows client operating system, Windows 10 for example, provides this functionality and also facilitates the caching of resolved mappings in a local client cache for future use. This cache is called the DNS resolver cache.



Windows operating system computers also contain a **Hosts** file. This is a file that is stored locally in the **%SystemRoot%\System32\Drivers\Etc** directory. The file can contain mappings for host names to IP addresses; however, it is empty by default. The file can be edited manually and the DNS resolver cache can parse it to add its mapped entries to the local DNS resolver cache when the DNS client service is started.

- Resource records. These are the actual entries in the DNS database that are used to answer queries. Each entry contains several items, including Name, Record Type, and Record Data. Defining specific record types allows entries to be classified and provides for faster query responses. Some typical record types are as follows:
  - A. This record is used for resolving host names into IPv4 addresses.
  - AAAA. This record is used for resolving host names into IPv6 addresses.
  - CNAME. This record is used to resolve one name (alias) into another, fully qualified name, such as *www* into *webserver1.microsoft.com*.
  - SRV. This record is used to find servers providing specific services, such as domain controllers.
  - PTR. This record is used in reverse lookup zones for resolving IP addresses into fully qualified host names.

## What are DNS zones and records?

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

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

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

### Forward lookup zones

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

- Host (A) records. Matches a name with an IP Address.
- Alias (CNAME) records. Matches an additional name with one or more FQDNs.
- Service (SRV) records. Stores information about a service in Lightweight Directory Access Protocol (LDAP) format.

- A DNS zone is a specific portion of DNS namespace that contains DNS records
- Zone types:
  - Forward lookup zone
  - Reverse lookup zone
- Resource records in forward lookup zones include: A, MX, SRV, NS, SOA, and CNAME
- Resource records in reverse lookup zones include: PTR

- Mail exchanger (MX) records. Use to identify Simple Mail Transport Service (SMTP) servers.
- Start of authority (SOA) records. Use to identify the Primary DNS server for a zone.
- Name server (NS) records. Use to identify all DNS servers in a zone.

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

### Reverse lookup zones

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

### Resource records

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

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

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

### PTR records

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

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



**Note:** Starting in Windows Server 2008 R2, you can also use Domain Name System Security Extensions (DNSSEC) technology to perform similar type of verification. There are enhancements to DNSSEC starting in Windows Server 2012 in encryption key management. These enhancements will be discussed in the "Configuring advanced DNS settings" lesson in this module.

Many email servers use a reverse lookup as one way of reducing spam. By performing a reverse lookup, email servers try to detect open Simple Mail Transfer Protocol (SMTP) servers (open relays).

Having a reverse lookup zone is important if you have apps that rely on looking up hosts by their IP addresses. Many apps record this information in security or event logs. If you see suspicious activity from a particular IP address, you can look up the host name using the reverse lookup zone information.

## Demonstration: Installing and configuring the DNS role

In this demonstration, you will learn how to:

- Install the DNS server role.
- Configure the DNS Server role to forward requests to LON-DC1.adatum.com.

### Demonstration Steps

#### Install the DNS Server role

1. On **TOR-SVR1**, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use **Server Manager** to install the DNS Server role.

#### Enable Pings

1. On **TOR-SVR1**, open **Windows Firewall with Advanced Security**.
2. In **Windows Firewall with Advanced Security**, enable the **Inbound Rules** for the **Print Sharing (Echo Request - ICMPv4-In)** and **File and Print Sharing (Echo Request - ICMPv6-In)** items.
3. Open Windows PowerShell, and type the following cmdlet and press Enter:

```
Ping 172.168.0.10
```

You should get four replies.

4. Switch to **LON-DC1**, and in Windows PowerShell, type the following cmdlet and press Enter:

```
Ping 172.168.18.20
```

You should get four replies.

#### Configure the DNS Server role

1. On **TOR-SVR1**, open the **DNS** console.
2. Review the properties of the **TOR-SVR1** server:
  - a. On the **Forwarders** tab, configure forwarding to **LON-DC1** by using the **172.16.0.10** IP address.
  - b. Click **OK** to close the **TOR-SVR1** Properties window.
3. Create a new forward lookup zone named **Contoso.com**.
4. Add a new host record to the **Contoso.com** zone named **ATL-SVR1** with the IP address **172.16.18.125**.

## Configuring DNS clients

DNS name resolution is an important aspect of network functionality in a Windows-based network. The primary determiner of name resolution for a Windows computer is the preferred DNS server. The *preferred DNS server* is the first DNS server that is queried when attempting to resolve a DNS host name.

### Configuring DNS client settings

You can configure DNS client settings on a computer running the Windows operating system by using the settings for each network adapter on the client, and for both IPv4 and IPv6, if enabled.

You can specify the DNS server addresses on a per-adapter basis on the **Properties** page of the appropriate TCP/IPv4 or TCP/IPv6 protocol stack.

You can configure DNS server settings manually by performing the following steps:

1. In **Server Manager**, click the **Local Server**, and then click the appropriate network adapter in the **Properties** section.
2. Right-click the network adapter for which you are configuring DNS, and then click **Properties**.
3. In the **Properties** window, click the appropriate TCP protocol stack, and then click **Properties**.
4. In the appropriate TCP protocol stack **Properties** window, select **Use the following DNS server addresses**, and then in the **Preferred DNS server** and **Alternate DNS server** text boxes, type the IP address of the DNS servers.
5. Optionally, you can add additional DNS server addresses and change the priority order for DNS servers by clicking **Advanced**, and then clicking the **DNS** tab in the **Advanced TCP/IP Settings** window. These advanced settings include several options or DNS suffix settings. The DNS suffix of a client specifies the domain namespace in which the client operates. You can also add additional DNS suffixes to enable the client to resolve single-label names for DNS names that exist in other DNS namespaces. Additionally, the advanced settings include the default behavior for the client to register its addresses in DNS, through the check box **Register this connection's addresses in DNS**.

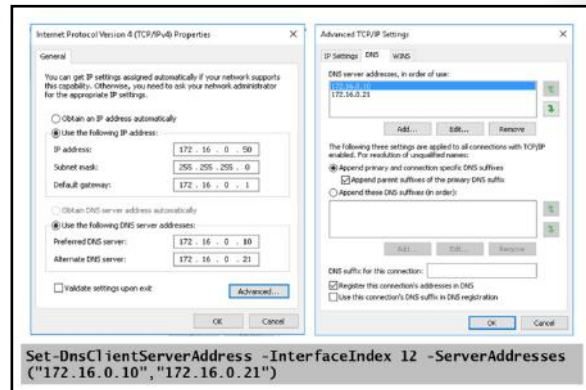


**Note:** Although you can manually configure DNS server information for clients, this information is typically provided to client computers through a Dynamic Host Configuration Protocol (DHCP) server.

You can also set DNS server addresses on client computers by using the following Windows PowerShell cmdlet:

```
Set-DnsClientServerAddress -InterfaceIndex 1 -ServerAddresses ("172.16.0.10", "172.16.0.21")
```

The preceding command would set the DNS servers addresses 172.16.0.10 and 172.16.0.21 for the network adapter referred to by index 1, with 172.16.0.10 as the preferred server for the interface because it is listed first in the cmdlet. When you specify multiple potential DNS servers on a client, any DNS query issued from the client will follow a preferred order when selecting the server to query.



## DNS server query order

The DNS Client service enables a client to resolve DNS names by querying DNS servers. The DNS Client service queries the DNS servers in the following order:

1. The DNS Client service sends the name query to the first DNS server on the preferred adapter's list of DNS servers and waits one second for a response.
2. If the DNS Client service does not receive a response from the first DNS server within one second, it sends the name query to the first DNS servers on all adapters that are still under consideration and waits two seconds for a response.
3. If the DNS Client service does not receive a response from any DNS server within two seconds, the DNS Client service sends the query to all DNS servers on all adapters that are still under consideration, and waits another two seconds for a response.
4. If the DNS Client service still does not receive a response from any DNS server, it sends the name query to all DNS servers on all adapters that are still under consideration, and waits four seconds for a response.
5. If the DNS Client service does not receive a response from any DNS server, the DNS client sends the query to all DNS servers on all adapters that are still under consideration, and waits eight seconds for a response.

## Tools and techniques for troubleshooting name resolution

Name resolution, like most other technologies, sometimes requires troubleshooting. Issues can occur when the DNS server, its zones, and its resource records are not configured properly. When resource records are causing issues, it can sometimes be difficult to identify the issue because configuration problems are not always obvious.

You have a number of tools available to configure, manage, and troubleshoot DNS server and name resolution issues.

- Windows Server 2012 R2 introduced a new Windows PowerShell DNS module with numerous cmdlets, including the **Get-DnsServerStatistics** cmdlet:
  - `$statistics = Get-DnsServerStatistics -ZoneName Adatum.com`
  - `$statistics.ZoneQueryStatistics`
  - `$statistics.ZoneTransferStatistics`
  - `$statistics.ZoneUpdateStatistics`
- Command-line tools to troubleshoot configuration issues:
  - `nslookup`
  - `DNSCmd`
  - `DNSLint`
  - `Ipconfig`
- The troubleshooting process:
  - Identify client DNS server with `nslookup` or `Resolve-DnsName`
  - Communicate via ping
  - Use `nslookup` to verify records

### Windows Server 2016 cmdlets

Windows PowerShell has extended functionality in Windows Server 2016, with enhanced zone-level statistics that are accessible through the **Get-DnsServerStatistics** cmdlet.



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

The following table details the **ZoneTransferStatistics** cmdlet, which returns information about full and incremental zone transfers.

Parameter	Functionality
<b>RequestReceived</b>	Received when the DNS server is a primary server for a zone
<b>RequestSent</b>	Sent when the DNS server is a secondary server for a zone
<b>ResponseReceived</b>	Received when the DNS server is a secondary server for a zone
<b>SuccessReceived</b>	Successful and received when the DNS server is a secondary server for a zone
<b>SuccessSent</b>	Successful and received when the DNS server is a primary server for a zone

The following table details the **ZoneUpdateStatistics** cmdlet.

Parameter	Functionality
<b>DynamicUpdateReceived</b>	Dynamic update requests that are received by the DNS server
<b>DynamicUpdateRejected</b>	Dynamic updates that are rejected by the DNS server

To get zone-level statistics, type the following code at an elevated Windows PowerShell prompt:

```
PS C:\> $statistics = Get-DnsServerStatistics -ZoneName Adatum.com
$statistics.ZoneQueryStatistics
$statistics.ZoneTransferStatistics
$statistics.ZoneUpdateStatistics
```

### Command-line tools and commands for troubleshooting

The command-line tools and commands that you use to troubleshoot name resolution and configuration issues are as follows:

- **Nslookup.** Use this tool to query DNS information. The tool is flexible and can provide valuable information about DNS server status. You also can use it to look up resource records and validate their configuration. Additionally, you can test zone transfers, security options, and MX record resolution.
- **DNSCmd.** Use this command-line tool to manage the DNS server role. This tool is useful in scripting batch files to help automate routine DNS management tasks or to perform simple unattended setup and configuration of new DNS servers on your network.
- **DNSLint.** Use this tool to diagnose common DNS issues. This tool diagnoses configuration issues in DNS quickly, and can generate a report in HTML format regarding the status of the domain that you are testing.



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

- **Ipconfig.** Use this command to view and modify IP configuration details that the computer uses. This command includes additional command-line options that you can use to troubleshoot and support DNS clients. You can view the local DNS cache for the client computer by using the command **ipconfig /displaydns**, and you can clear the local DNS cache using the **ipconfig /flushdns** command. If you want to reregister a host in DNS, you can use the **ipconfig /registerdns** command.
- Monitoring on DNS server. Perform simple local queries and recursive queries from the **Monitoring** tab in the **DNS Server Properties** dialog box to test if the server can communicate with upstream servers. You also can schedule these tests for regular intervals.

In Windows Server 2016, there is a new set of Windows PowerShell cmdlets that you can use for DNS client and server management. Some of the most commonly used cmdlets are as follows:

- **Clear-DNSClientCache.** This cmdlet clears the client cache, similar to the **ipconfig /flushdns** command.
- **Get-DNSClient.** This cmdlet displays the details of the network interfaces.
- **Get-DNSClientCache.** This cmdlet displays the content of the local DNS client cache.
- **Register-DNSClient.** This cmdlet registers all of the IP addresses on the computer onto the configured DNS server.
- **Resolve-DNSName.** This cmdlet performs a DNS name resolution for a specific name, similar to the way **nslookup** works.
- **Set-DNSClient.** This cmdlet sets the interface-specific DNS client configurations on the computer.
- **Test-DNSServer.** This cmdlet tests that a specified computer is a functioning DNS server.

### The troubleshooting process

When you troubleshoot name resolution, you must understand the name resolution methods that the computer uses, and the order in which the computer uses them. Be sure to clear the DNS resolver cache between resolution attempts.

If you cannot connect to a remote host and suspect a name resolution problem, you can troubleshoot the name resolution by performing the following steps:

1. Open an elevated command prompt, and then clear the DNS resolver cache by typing the following command at a command prompt:

```
ipconfig /flushdns
```

Alternatively, you can open Windows PowerShell and type the equivalent cmdlet at a Windows PowerShell command prompt:

```
Clear-DNSClientCache
```

2. Attempt to ping the remote host by its IP address. This helps identify whether the issue is related to name resolution. If the ping succeeds by using the IP address but fails by using its host name, then the problem is related to name resolution.
3. Attempt to ping the remote host by using its host name. For example, if you were working at Contoso, Ltd., you would enter the following command at a command prompt:

```
Ping LON-DC1.contoso.com
```

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

```
Nslookup.exe -d LON-DC1.contoso.com. > filename.txt
```

Examine the contents of the filename.txt file to identify the failed stage in name resolution.



**Note:** You also should know how to interpret the DNS resolver cache output so that you can identify whether the name resolution problem is associated with the client computer's configuration, the name server, or the configuration of records within the name server zone database. Interpreting the DNS resolver cache output is beyond the scope of this lesson.

## Managing DNS services

DNS management consists of the following tasks:

- Delegating administration of DNS.
- Configuring logging for DNS.
- Aging and scavenging.
- Backing up the DNS database.

### Delegating administration of DNS

By default, the Domain Admins group has full permissions to manage all aspects of the DNS server in its home domain, and the Enterprise Admins group has full permissions to manage all

aspects of all DNS servers in any domain in the forest. If you need to delegate the administration of a DNS server to a different user or group, you can add that user or global group to the DNS Admins group for a given domain in the forest. Members of the DNS Admins group can view and modify all DNS data, settings, and configurations of DNS servers in their home domain. The DNS Admins group is a Domain Local security group, and by default has no members in it.

### Configuring DNS logging

By default, DNS maintains a DNS server log, which you can view in the Event Viewer. This event log is located in the **Applications** and **Services Logs** folder in Event Viewer. It records common events such as:

- Starting and stopping of the DNS service.
- Background loading and zone signing events.
- Changes to DNS configuration settings.
- Various warnings and error events.

For more verbose logging, you can enable debug logging. Debug logging options are disabled by default, but you can enable them as needed. Debug logging options include the following:

- Direction of packets.
- Contents of packets.
- Transport protocol.
- Type of request.
- Filtering based on IP address.

- You can manage DNS services by:
  - Delegating DNS administration through membership in the DNS Admins group
  - Viewing DNS logs in Event Viewer
  - Enabling DNS debug logging in the DNS server properties
  - Enabling aging and scavenging to remove stale records
- Backup methods for the DNS database depend on how the database is deployed:
  - Back up Active Directory-integrated zones through System State backups by using **dnscmd** or by using Windows PowerShell
  - Copy or back up primary zone files that are not using AD DS integration



- Specifying the name and location of the log file, which is located in the **%windir%\System32\DNS** directory.
- Log file maximum size limit.

Debug logging can be resource intensive. It can affect overall server performance and consume disk space. Therefore, you should enable it only temporarily when you require detailed information about server performance. To enable debug logging on the DNS server, do the following:


1. Open the DNS Manager console.
2. Right-click the applicable DNS server, and then click **Properties**.
3. In the **Properties** dialog box, click the **Debug Logging** tab.
4. Select **Log packets for debugging**, and then select the events for which you want the DNS server to record debug logging.

### Aging and scavenging

DNS dynamic updates add resource records to the zone automatically, but in some cases those records are not deleted automatically when they are no longer required. For example, if a computer registers its own host (A) resource record and is improperly disconnected from the network, the host (A) resource record might not be deleted. These records, known as *stale records*, take up space in the DNS database and might result in an incorrect query response being returned. Windows Server operating systems can search for those stale records and, based on the aging of the record, scavenge them from the DNS database.

Aging and scavenging is disabled by default. You can enable aging and scavenging in the advanced properties of the DNS server, or you can enable it for selected zones in the zone's **Properties** window.

Aging is determined by using two parameters, the refresh interval and the no-refresh interval. The *refresh interval* is the date and time that the record is eligible to be refreshed by the client. The default is seven days. The *no-refresh interval* is the period of time that the record is not eligible to be refreshed. By default, this is seven days. In the normal course of events, a client host record cannot be refreshed in the database for seven days after it is first registered or refreshed. However, it then must be refreshed within the next seven days after the no-refresh interval, or the record becomes eligible to be scavenged out of the database. A client will attempt to refresh its DNS record at startup, and every 24 hours while the system is running.

 **Note:** Records that are added dynamically to the database are time stamped. Static records that you enter manually have a time-stamp value of 0, therefore they will not be affected by aging, and will not be scavenged out of the database.

### Backing up the DNS database

How you back up the DNS database depends on how DNS was implemented into your organization. If your DNS zone was implemented as an Active Directory–integrated zone, your DNS zone is included in the Active Directory database **ntds.dit** file. If the DNS zone is a primary zone and is not stored in AD DS, the file is stored as a **.dns** file in the **%SystemRoot%\System32\Dns** folder.

### Backing up AD DS integrated zones

AD DS integrated zones are stored in AD DS and are backed up as part of a System State or a full server backup. Additionally, you can back up just the Active Directory–integrated zone by using the **Dnscmd.exe** command-line tool.

To back up an Active Directory–integrated zone, perform the following steps:

1. Open an elevated command prompt.
2. Run the following command.

```
dnscmd /ZoneExport <zone name> <zone file name>
```

In this command, *<zone name>* is the name of your DNS zone, and *<zone file name>* is the file that you want to create to hold the backup information.

The Dnscmd.exe tool exports the zone data to the file name that you designate in the command, to the **%windir%\System32\DNS** directory.

You can also use Windows PowerShell to perform the same task. In Windows PowerShell, you use the **Export-DnsServerZone** cmdlet. For example, if you want to export a zone named **contoso.com**, run the following command.

```
Export-DnsServerZone -Name contoso.com -Filename contoso
```

### Backing up primary zones

You can back up a primary zone that is not stored in AD DS by copying or backing up the individual zone file, **zonename.dns**, which is located in the **%windir%\System32\DNS** directory. For example, if your DNS primary zone is named **Adatum.com**, the DNS zone file will be named **Adatum.com.dns**.

## Demonstration: Troubleshooting name resolution

In this demonstration, you will learn how to:

- Use Windows PowerShell cmdlets to troubleshoot DNS.
- Use command-line tools to troubleshoot DNS.

### Demonstration Steps

#### Use Windows PowerShell cmdlets to troubleshoot DNS

1. On **LON-CL1**, open Windows PowerShell, run the following cmdlets, and then make a note of the results:

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

2. Note the **Interface Index** value of the London\_Network interface **IPv4** row.
3. Run the following cmdlet:

```
Resolve-DnsName 1on-dc1
```

Note the address returned.

4. Open the **Network and Sharing Center** and then view the details for the London\_Network connection.
5. Open the **Properties** for the London\_Network adapter and configure the adapter to obtain both the IP address and DNS server address automatically.

- From the PowerShell prompt, run the following cmdlets, where *X* is the Interface Index value that you wrote down in step 2:

```
Set-DnsClientServerAddress -InterfaceIndex X -ResetServerAddresses
Clear-DnsClientCache
Get-DnsClientServerAddress
```

Notice that there is no IPv4 address.

- From the PowerShell prompt, run the following cmdlets, where *X* is the Interface Index value that you wrote down in step 2:

```
Set-DnsClientServerAddress -InterfaceIndex X -ServerAddress 172.16.0.10
Get-DnsClientServerAddress
Resolve-DnsName lon-dc1
```

Notice that the IPv4 address is now assigned.

- Switch back to the **Network and Sharing Center**, and enter the following:
  - o IP address: **172.16.0.50**
  - o Subnet mask: **255.255.0.0**
  - o Default gateway: **172.16.0.1**
- At Windows PowerShell command prompt, run the following cmdlets:

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

- Close both the **Windows PowerShell** and the **Network and Sharing Center** windows.

### Use command line tools to troubleshoot DNS

- Run an elevated command prompt as **Administrator**, and then run the **ipconfig /all** command.
- Run the **nslookup** command, and then search for the **LON-CL1** address. Exit from the **nslookup** command.
- Switch to **LON-DC1**, and then open an elevated command prompt as **Administrator**.
- Run the **dnscmd /?** command, and then note the options.
- Run the **ipconfig /displaydns** command, and then note the output values displayed.
- Run the **ipconfig /flushdns** command, and then run the **ipconfig /displaydns** command again.
- Run the **ping** command on **LON-CL1**.
- Use the **ipconfig /displaydns** command to display the host record for **LON-CL1**.



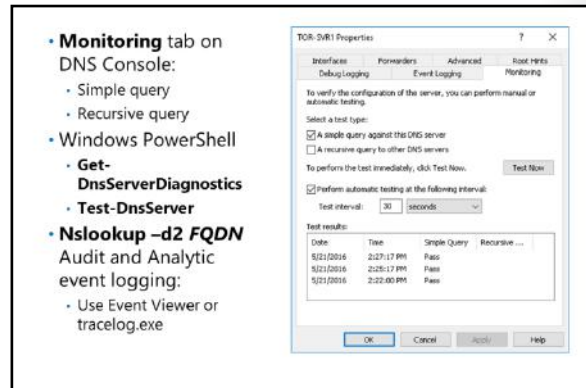
**Note:** Note that the command returned the FQDN, which proves that the name resolution was successful.

- Close all open windows.

## Testing DNS servers

Issues can occur when you do not configure the DNS server, its zones, and its resource records properly. When resource records cause issues, it can sometimes be more difficult to identify the issue because configuration problems are not always obvious.

The following table lists possible configuration issues that can cause DNS problems.



Issue	Result
Missing records	Records for a host are not on the DNS server. They might have been scavenged prematurely. This can result in workstations not being able to connect with each other.
Incomplete records	Records that are missing the information required to locate the resource they represent can cause clients requesting the resource to use invalid information. For example, a service record that does not contain a needed port address is an example of an incomplete record.
Incorrectly configured records	Records that point to an invalid IP address or have invalid information in their configuration will cause problems when DNS clients try to find resources.

The tools that you can use to troubleshoot the above mentioned issues and other configuration issues are:

- **Nslookup.** Use this tool to query DNS information. The tool is flexible, and it can provide valuable information about DNS server status. You also can use it to look up resource records and validate their configuration. Additionally, you can test zone transfers, security options, and MX record resolution. To get detailed debugging information, run the following command:

```
Nslookup -d2 FQDN of the DNS server
```

For example:

```
Nslookup -d2 LON-DC1.adatum.com
```

All fields of every packet are then printed.

- **Windows PowerShell.** You can use Windows PowerShell cmdlets to configure and troubleshoot various DNS aspects.
  - **Get-DnsServerDiagnostics.** Returns DNS server diagnostic and logging parameters.
  - **Test-DnsServer.** Can perform a variety of tests on a functioning DNS server depending on cmdlet parameters.
- **Dnscmd.** Manage the DNS server service with this command-line interface. This utility is useful in scripting batch files to help automate routine DNS management tasks, or to perform simple unattended setup tasks and configure new DNS servers on your network.

- **IPconfig.** Use this command to view and modify IP configuration details that the computer uses. This command includes additional command-line options that you can use to troubleshoot and support DNS clients. You can view the client local DNS cache by using the command **ipconfig /displaydns**, and you can clear the local cache by using the **ipconfig /flushdns** command.



**Note:** You also can use the following Windows PowerShell cmdlets:

- **clear-DnsClientCache** deletes the DNS resolver cache.
- **get-DnsClientCache** displays the resolver cache.
- The **Monitoring** tab on the **DNS server Properties** dialog box. In this tab, you can configure a test that allows the DNS server to determine whether it can resolve simple local queries and perform a recursive query to ensure that the server can communicate with upstream servers. You also can schedule these tests for regular intervals.

These are basic tests, but they provide a good place to start troubleshooting the DNS service. Possible causes for a test failure include:

- The DNS server service has failed.
- The upstream server is not available on the network.

### Audit and analytic event logging

Microsoft introduced enhanced DNS logging and diagnostics in Windows Server 2012 R2. This is continued in Windows Server 2016. While DNS server performance can be affected when additional logging is enabled, the enhanced DNS logging and diagnostics features are designed to have a very low impact on performance. Enhanced logging and diagnostics include DNS Audit and DNS Analytic events. DNS audit logs are enabled by default, and do not affect DNS server performance significantly. DNS analytical logs are not enabled by default, and typically will only affect DNS server performance at very high DNS query rates. For instance, a DNS server running on current hardware getting 100,000 queries per second (QPS) can experience a 5% performance degradation when analytic logs are enabled. There is no noticeable performance impact for query rates of 50,000 QPS and lower. However, it is a good practice to monitor DNS server performance when additional logging is enabled.

DNS server audit events permit you to track changes on the DNS server. An audit event gets logged every time there are changes to server, zone, or resource record settings. This includes operational events like dynamic updates, zone transfers, and DNSSEC zone signing and unsigned. DNS server analytic events allow you to track activity on the DNS server. An analytic event gets logged every time the server sends or receives DNS information.



**Note:** For a comprehensive list of all audit and analytic events, refer to: "Expand DNS Logging and Diagnostics" at <http://aka.ms/tenpbr>

DNS audit and analytic events can be viewed in the Event Viewer. You can also use an Event Tracing for Windows (ETW) consumer applications such as logman, tracelog, and message analyzer to view further details. Tracelog.exe is available for free by downloading and installing the Windows Driver Kit (WDK).



**Note:** You can download the WDK from "Download the WDK, WinDbg, and associated tools" at: <http://aka.ms/rhwnfd>

## Demonstration: Testing the DNS server

In this demonstration, you will learn how to:

- Test the DNS server.
- Configure auditing and analytical logging of events.

### Demonstration Steps

#### Test the DNS server

1. On **TOR-SVR1**, in the **DNS Management Console**, open and review the server properties.
2. On the **Monitoring** tab, perform a simple query test.
3. Open Windows PowerShell, and then run the following commands, observing the results of each command:

```
nslookup -d2 LON-DC1.Adatum.com
Test-DnsServer -IpAddress 172.158.18.20
Get-DNSServerDiagnostics
```

#### Use audit and analytic event logging

1. Open **Event Viewer**.
2. Navigate down the console tree to **Applications and Service Logs, Microsoft, Windows**, and then select **DNS-Server**.
3. Right-click **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**.
4. In the analytical log, right-click **Analytical**, and then click **Properties**.
5. Under **When maximum event log size is reached**, choose **Do not overwrite events (Clear logs manually)**, select the **Enable logging** check box, and then click **OK**, when you are asked if you want to enable this log.
6. Return to Windows PowerShell, and run the following commands:

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

7. Return to **Event Viewer**, refresh the **DNS-Server** log, and then review the events in the **Analytical** sub log. Find the event showing the successful query of the IP address of **ATL-SVR1.contoso.com**.
8. Close all open windows. Do not sign out.

### Categorize Activity

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

## Lesson 2

# Configuring zones in DNS

*DNS zones* host the record information that enables a DNS server to respond to queries and assist in the name resolution process. A DNS server maintains the zone data and stores it in one of the two ways—in a flat zone file that contains mapping lists, or integrated into AD DS. In this lesson, you will learn about DNS zones, how they function, and how to configure them.

### Lesson Objectives

After completing this lesson, you should be able to:

- Describe DNS resource record types.
- Explain how to create resource records.
- Describe how to configure DNS zones.
- Describe primary and secondary zones.
- Explain how to configure zone replication.

### DNS resource record types

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

Resource records also help find resources for a particular domain. For instance, when an Exchange server needs to find the server that is responsible for delivering mail for another domain, the Exchange server will request that domain's mail exchange (MX) record, which points to the A record of the host that is running the Simple Mail Transfer Protocol (SMTP) mail service.

Resource records also can contain custom attributes. MX records, for instance, have a preference attribute, which is useful if an organization has multiple mail servers. This will inform the sending server which mail server the receiving organization prefers. Service locator (SRV) records also contain information regarding which port the service is listening to and the protocol that you should use to communicate with the service.

#### DNS resource records include:

- SOA: Start-of-authority resource record
- A: IPv4 host address resource record
- CNAME: Alias resource record
- MX: Mail exchange resource record
- SRV: Service locator resource record
- NS: Name server resource record
- AAAA: IPv6 host address resource record
- PTR: Pointer resource record



The following table describes the most common resource records.

DNS resource records	Description
Start-of-authority (SOA) resource record	The record identifies the primary name server for a DNS zone, in addition to other specifics, such as Time to Live (TTL) and refresh.
Host address (A) resource record	The main record that resolves a host name to an IPv4 address.
Canonical name (CNAME) resource record	An alias record type that maps one name to another (for example, www.microsoft.com is a CNAME of the A record microsoft.com).
MX resource record	The record is used to specify an email server for a particular domain.
SRV resource record	The record identifies a service that is available in the domain. Active Directory uses these records extensively.
Name server (NS) resource record	The record identifies a name server for a domain.
AAAA	The main record that resolves a host name to an IPv6 address.
Pointer (PTR) resource record	The record is used to look up and map an IP address to a domain name. The reverse lookup zone stores the names.

## Creating records in DNS

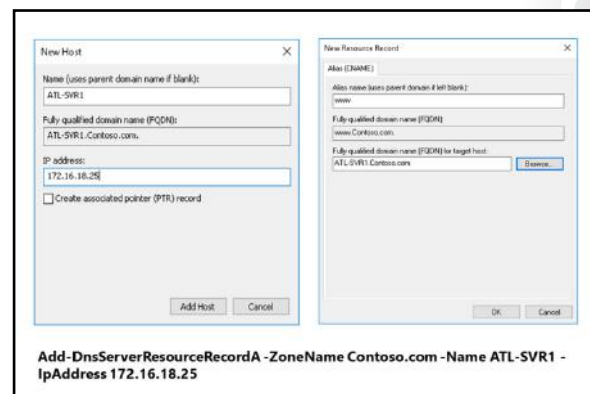
You must create DNS resource records before they can be referenced within the DNS infrastructure. When you create a DNS resource record, it exists within a DNS zone. A DNS zone is made up of several related records. You can create a resource record in a DNS zone in two ways: dynamically and manually.

### Dynamic creation

When dynamic updates are allowed for a DNS zone, clients that use DNS will register with the DNS server, and then the resource records for each client are created automatically. This configuration is known as *dynamic updates*, and it is covered in more detail later in this module.

### Manual creation

If dynamic updates are not enabled for a DNS zone, you must create resource records manually. Even when dynamic updates is enabled, you must still manually create some records. Alias, or CNAME records, for example, are commonly created manually to provide an alias DNS name for a node on the network.



## Creating DNS records

To create a resource record in the GUI, perform the following steps:

1. Open the **DNS Manager** console.
2. Locate the zone for which you are creating the record.
3. Right-click the zone, and then click one of the following: **New Host**, **New Alias**, **New Mail Exchanger**, or **Other New Records**.
4. Type a host name for the new record, and fill in the other details for the record, depending on the record type.

You can also create host records by using the following Windows PowerShell cmdlets for DNS:

- **Add-DnsServerResourceRecord**. Creates any resource record, specified by type.
- **Add-DnsServerResourceRecordA**. Creates a type A resource record.
- **Add-DnsServerResourceRecordCNAME**. Creates a CNAME alias resource record.
- **Add-DnsServerResourceRecordMX**. Creates an MX resource record.
- **Add-DnsServerResourceRecordPtr**. Creates a PTR resource record.

For example, the following command uses the **Add-DNSServerResourceRecordA** cmdlet to add the host name **LON-SVR3** to the Adatum.com zone for the IP address 172.16.0.24.

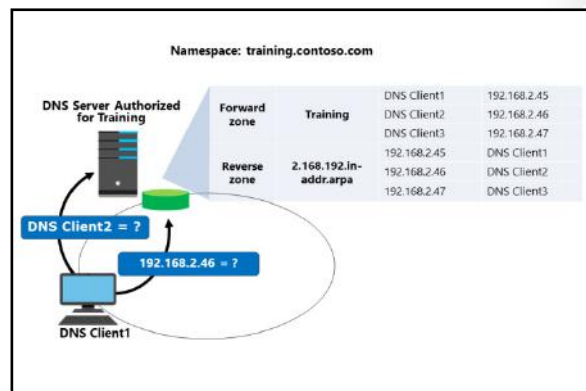
```
Add-DNSServerResourceRecordA -Name "LON-SVR3" -ZoneName "Adatum.com" -IPv4Address "172.16.0.24"
```

## Configuring DNS zones

You can host DNS resource records on more than one DNS server. A *DNS zone* contains the DNS records for one or more namespaces, and you can replicate zone data to more than one server. This adds redundancy to a zone, because the information needed to find resources in the zone now exists on more than one server. If you have a zone that hosts critical server resource records, this zone is likely to have a higher level of redundancy than a zone that defines noncritical devices.

Some companies create one DNS zone for workstations and another for servers. Administrators then can choose different strategies when defining how the zones will replicate.

A DNS server is authoritative for a zone if it hosts the resource records for the names and IP addresses that the clients request in the zone file. Zones can be either forward or reverse. A reverse zone sometimes is known as an inverse zone.



## Forward lookup zone

The forward lookup zone resolves host names to IP addresses and hosts the common resource records: A, CNAME, SRV, MX, SOA, TXT, and NS. This zone type must exist for a DNS zone to be considered authoritative. Client computers send host names or FQDNs of the DNS server's domain to the DNS server. The DNS server uses the FQDN to look up a corresponding IP address or to find any resource record type that the client prescribes, such as a domain controller's SRV records. The DNS server returns the IP address or addresses to the client in the DNS response.

## Reverse lookup zone

The reverse lookup zone resolves an IP address to a domain name, and hosts start of authority (SOA), name server (NS), and pointer (PTR) resource records. A forward lookup zone returns an IP address when presented with a particular hostname. A reverse zone does the opposite; it returns the host name given a particular IP address. Reverse zones are not always configured, but you should configure them to reduce warning and error messages. Many standard Internet protocols rely on reverse zone lookup data to validate forward zone information. For example, if the forward lookup indicates that training.contoso.com resolves to 192.168.2.45, you can use a reverse lookup to confirm that 192.168.2.45 is associated with training.contoso.com.

Having a reverse zone is important if you have applications that rely on looking up hosts by their IP addresses. Many applications log this information in security or event logs. If you see suspicious activity from a particular IP address, you can resolve the host by using the reverse lookup zone information. Many email security gateways use reverse lookups to validate that the IP address that is sending messages is associated with a domain.

## What are primary and secondary zones?

There are four DNS zone types:

- Primary
- Secondary
- Stub
- Active Directory–integrated

Zones	Description
Primary	Read/write copy of a DNS database
Secondary	Read-only copy of a DNS database
Stub	Copy of a zone that contains only records used to locate name servers
Active Directory-integrated	Zone data is stored in AD DS rather than in zone files

### Primary zone

When the DNS server is both the host and the primary source for information about a zone, the zone is a *primary zone*. In addition, the DNS server stores the master copy of the zone data either in a local file or in AD DS. When the DNS server stores the zone data in a file, the primary zone file by default is named **zone\_name.dns**, and is located on the server in the **%windir%\System32\Dns** folder. When the zone is not stored in AD DS, the primary zone server is the only DNS server that has a writable copy of the database.

### Secondary zone

When the DNS server is the host, but is the secondary source for zone information, the zone is a secondary zone. The zone information at this server must be obtained from another DNS server that also hosts the zone. This DNS server must have network access to the DNS server to receive updated zone information. Because a secondary zone is a copy of a primary zone that another server hosts, the secondary zone cannot be stored in AD DS. Secondary zones can be useful if you are replicating data from non-Windows DNS zones.

## Stub zone

A *stub zone* is a replicated copy of a zone that contains only those resource records necessary to identify that zone's authoritative DNS servers. Stub zones will be covered in a later lesson in this module.

## Active Directory–integrated zone

If AD DS stores the zone data, DNS can use the multi-master replication model to replicate the primary zone data. This enables you to simultaneously edit zone data on more than one DNS server. Active Directory–integrated zones will be covered in a subsequent lesson in this module.

## Configuring zone replication

Because zones are an important aspect of DNS, zones must be available from more than one DNS server on the network to provide availability and fault tolerance when resolving name queries. Zone transfers occur in a traditional DNS zone. Zone replication occurs in an Active Directory–integrated zone.

### Zone transfers

Zone transfers are used to transfer zone records from a master server to a secondary server. A master server can be any other DNS server that loads the zone, such as the primary server for the zone or another secondary server. When the master server receives the request for the zone, it can reply with either a partial or a full transfer of the zone to the secondary server. The types of zone transfers include:

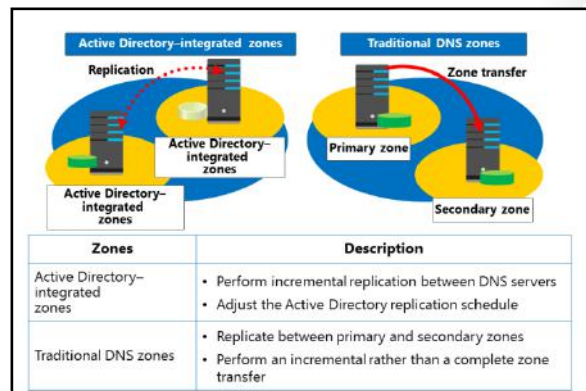
- Full zone transfer. A *full zone transfer* occurs when you copy the entire zone from one DNS server to another. A full zone transfer is known as an *all zone transfer* (AXFR).
- Incremental zone transfer. An *incremental zone transfer* occurs when there is an update to the DNS server and only the resource records that were changed are replicated to the other server. This is known as an *incremental zone transfer* (IXFR).
- Fast zone transfer. Windows DNS servers perform fast transfers, which are a type of zone transfer that uses compression and sends multiple resource records in each transmission.

Not all DNS server implementations support incremental and fast zone transfers. When integrating a Windows Server 2016 DNS server with a Berkeley Internet Name Domain (BIND) DNS server, you must ensure that the features you need are supported by the BIND version that is installed.

### Zone replication

Active Directory replication provides an advantage over standard DNS replication. With standard DNS replication, only the primary server for a zone can modify the zone. With AD DS replication, all domain controllers for the domain can modify the zone and then replicate the changes to other domain controllers. This replication process is known as *multi-master replication* because multiple domain controllers, or *masters*, can update the zone.

Active Directory–integrated zones replicate by using multi-master replication. This means that any standard domain controller that also holds the DNS role can update the DNS zone information, which then replicates to all DNS servers that host the DNS zone.





**Note:** *DNS notify* is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur. This is useful in a time-sensitive environment, where data accuracy is important.

### Performing zone transfers

You perform zone transfers and replication within the **DNS Manager** console, or by using Windows PowerShell cmdlets. To perform a zone transfer, you must allow the transfer from the DNS server hosting the primary zone. To enable zone transfers, perform the following steps:

1. In the **DNS Manager** console, right-click the zone you are configuring, and then click **Properties**.
2. In the **Properties** window, click the **Zone Transfers** tab.
3. On the **Zone Transfers** tab, select the **Allow zone transfers** check box.
4. Optionally, select whether to allow zone transfers for any server, for only those servers specified in the **Name Servers** tab, or for a list of servers that you specify.

After you perform these steps, you can transfer and optionally replicate the zone from any of the servers you specified in step 4 by installing the DNS Server role and performing the following steps on the new DNS server:

1. Open the **DNS Manager** console.
2. Create a new secondary zone.
3. Name the new secondary zone the same as the zone that you will be transferring.
4. Specify the name of the server from which you are transferring the zone.

After you perform these steps, the zone will transfer to the new DNS server. It might take several minutes for the initial full zone transfer to complete.

### Check Your Knowledge

Question	
A DNS server is authoritative for a zone if:	
Select the correct answer.	
<input type="checkbox"/>	It is set to Authoritative in the DNS Server Properties.
<input type="checkbox"/>	It hosts the resource records in the zone file that is named for the zone.
<input type="checkbox"/>	It has multiple CNAME resource records.
<input type="checkbox"/>	It is set to Authoritative in the Zone Properties.
<input type="checkbox"/>	It is the secondary zone server.

## Lesson 3

## Configuring name resolution between DNS zones

You can configure your DNS server infrastructure in various ways to resolve names and IP addresses beyond your own networks. In this lesson, you will learn how to provide DNS name resolution between zones, including DNS caching, forwarding, conditional forwarding and stub zones. You will also learn about DNS zone delegation.

### Lesson Objectives

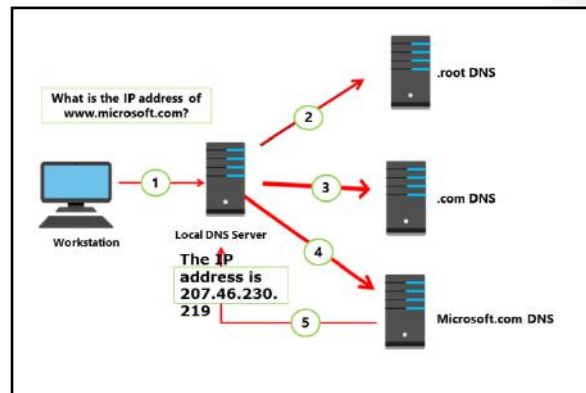
After completing this lesson, you will be able to:

- Explain how to resolve DNS names between zones.
- Describe a stub zone.
- Describe DNS caching.
- Describe DNS forwarding.
- Explain when to use forwarding.
- Describe how to configure zone delegation.

### Resolving DNS names between zones

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

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



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

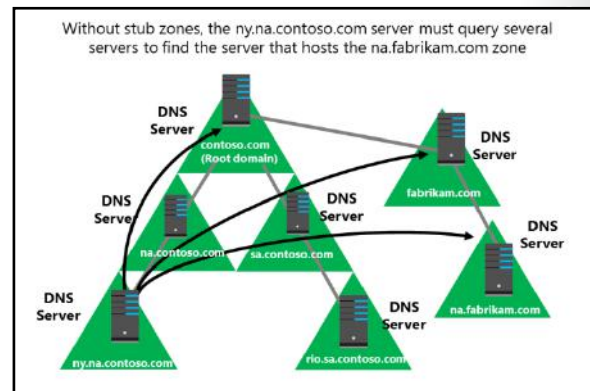
You can modify the name resolution process by configuring caching or forwarding:

- **Caching.** After a local DNS server resolves a DNS name, it caches the results for the period of time defined by the time to live (TTL) value in the SOA record for the DNS zone. The default TTL is one hour. Subsequent resolution requests for the DNS name are given the cached information. Note that the TTL is not set by the caching server, but instead by the authoritative DNS server that resolved the name from its zone. When the TTL expires, the caching server must delete it. Subsequent requests for the same name would require a new name resolution request to the authoritative server.
- **Forwarding.** Instead of querying root servers, you can configure a DNS server to forward DNS requests to another DNS server. For example, requests for all Internet names can be forwarded to a DNS server at an Internet service provider (ISP).

## What is a stub zone?

A stub zone resolves names between separate DNS namespaces, which might be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces. A stub zone consists of the following:

- The delegated zone's Start of Authority resource record, NS resource records, and A resource records.
- The IP address of one or more master servers that you can use to update the stub zone.



The master servers for a stub zone are one or more DNS servers that are authoritative for the child zone, usually the DNS server that is hosting the primary zone for the delegated domain name.

## Stub zone resolution

When a DNS resolver performs a recursive query operation on a DNS server that is hosting a stub zone, the DNS server uses the resource records in the stub zone to resolve the query. The DNS server sends an iterative query to the authoritative DNS servers that the stub zone's NS resource records specify as if it were using NS resource records in its cache. If the DNS server cannot find the authoritative DNS servers in its stub zone, the DNS server that is hosting the stub zone attempts standard recursion by using root hints.

The DNS server stores the resource records it receives from the authoritative DNS servers that a stub zone in its cache lists, but it does not store these resource records in the stub zone itself. Only the Start of Authority, NS record, and just the A resource records that resolve the NS records returned in response to the query are stored in the stub zone. The resource records that the cache stores are cached according to the time to live (TTL) value in each resource record. The Start of Authority, NS record, and glue A resource records, which are not written to cache, expire according to the expire interval that the stub zone's Start of Authority record specifies. During the stub zone's creation, the Start of Authority record is created. Start of Authority record updates occur during transfers to the stub zone from the original, primary zone. If the query was an iterative query, the DNS server returns a referral containing the servers that the stub zone specifies.

## Communication between DNS servers that host parent and child zones

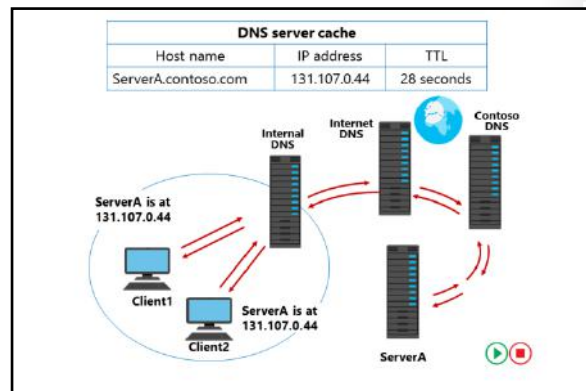
A DNS server that delegates a domain to a child zone on a different DNS server is made aware of new authoritative DNS servers for the child zone only when resource records for them are added to the parent zone that the DNS server hosts. This is a manual process that requires administrators for the different DNS servers to communicate often. Stub zones enable a DNS server that is hosting a stub zone for one of its delegated domains to obtain updates of the authoritative DNS servers for the child zone when the stub zone is updated. The update is performed from the DNS server that is hosting the stub zone, and the administrator for the DNS server that is hosting the child zone does not need to be contacted.

## What is DNS caching?

*DNS caching* increases the performance of an organization's DNS by decreasing the time it takes to resolve a DNS host name. When a DNS server resolves a DNS name successfully, it adds the name to its cache. Over time, this builds a cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.



**Note:** The default time to cache DNS data is one hour. You can configure this by changing the **TTL** value of an SOA record for the appropriate DNS zone. To view and edit **TTL** values, you must select the **Advanced View** option in the **DNS Manager** console.



A caching-only server does not host any DNS zone data; it only answers lookups for DNS clients. The *DNS client cache* is a DNS cache that the DNS client service stores on the local computer. To view the current client-side cache, run the **ipconfig /displaydns** command at the command prompt. If you want to clear the local cache, such as when you are troubleshooting name resolution, you can use the **ipconfig /flushdns** command.



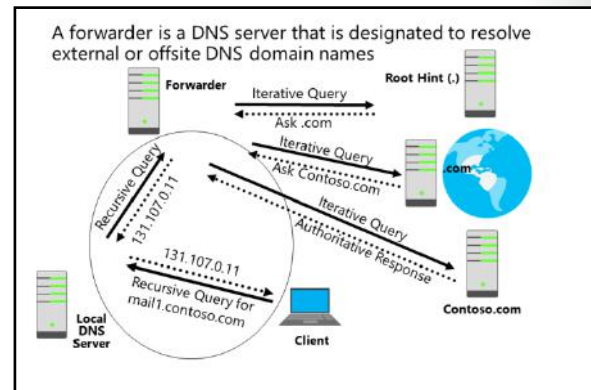
**Note:** You also can use the following Windows PowerShell cmdlets:

- **Get-DnsClientCache** to view the DNS Resolver Cache.
- **Clear-DnsClientCache** to delete the DNS Resolver Cache.




## What is DNS forwarding?

Forwarding provides a way for namespaces or resource records not contained in a DNS server's zone to be passed on to another DNS server for resolution. For example, you might want to send all external name resolution requests to the DNS servers of the Internet service provider rather than directly to the root hints. Alternatively, you might want to send external DNS queries from a branch office DNS server to the head office DNS servers, which then go to the root hints to resolve the name. You also can use conditional forwarders to forward queries according to specific domain names.



A network DNS server is designated a forwarder when the network's other DNS servers forward to it the queries that they cannot resolve. By using a forwarder, you can manage name resolution for names outside your network, such as names on the Internet, and improve the efficiency of name resolution for your network's computers.

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

### Configuring forwarding

You can configure forwarders on a DNS server by using the following steps:

1. In the **DNS Manager** console, right-click the DNS server name, and then click **Properties**.
2. On the **Forwarders** tab, click **Edit**, and then add DNS servers that can be used to forward DNS queries for external DNS names.

## DNS forwarding and stub zone guidance

### Comparing stub zones and conditional forwarders

There might be some confusion about when to use conditional forwarders rather than stub zones. This is because both DNS features allow a DNS server to respond to a query with a referral for, or by forwarding to, a different DNS server.

- When to use conditional forwarding
  - Points to a different domain name
  - Name can even be in a different top level
  - When you want all name resolution for that name to take a particular path
- When to use stub zones
  - Usually when the domain name is below a higher level
  - Delegation below a delegation

However, these settings have different purposes:

- A conditional forwarder setting configures the DNS server to forward a query that it receives to a DNS server, depending on the DNS name that the query contains.
- A stub zone keeps the DNS server that is hosting a parent zone aware of all the DNS servers that are authoritative for a child zone.

### When to use conditional forwarders

If you want DNS clients on separate networks to resolve the names of each other without having to query Internet DNS servers, such as when a company merger occurs, you should configure each network's DNS servers to forward queries for names in the other network. DNS servers in one network will forward names for clients in the other network to a specific DNS server, which builds a large information cache about the other network. This allows you to create a direct point of contact between two networks' DNS servers, which reduces the need for recursion.

Stub zones do not provide the same server-to-server benefit, however. This is because a DNS server that is hosting a stub zone in one network replies to queries for names in the other network with a list of all authoritative DNS servers for the zone with that name, rather than the specific DNS servers that you designated to handle this traffic. This configuration complicates any security settings that you want to establish between specific DNS servers that are running in each of the networks.

### When to use stub zones

Use stub zones when you want a DNS server to remain aware of the authoritative DNS servers for a foreign zone. A conditional forwarder is not an efficient way to keep a DNS server that is hosting a parent zone aware of the authoritative DNS servers for a child zone. This is because whenever the authoritative DNS servers for the child zone change, you have to configure the conditional forwarder setting manually on the DNS server that hosts the parent zone. Specifically, you must update the IP address for each new authoritative DNS server for the child zone.

## Discussion: When to use DNS forwarding

Participate in a discussion in the class, and answer the question displayed on the slide.

### Scenario 1


Northwind Traders Inc., has recently acquired the Beyond Blue Airline Corporation, and you are tasked with setting up the DNS infrastructure. You will have an AD DS forest named **Northwind.com**, and a separate tree named **Beyondblueair.com**. Users will regularly need to resolve names to IP addresses for servers within each domain name. You want to ensure that the DNS queries remain within the corporate infrastructure.

**Question:** What DNS resolution method do you use?


What DNS resolution method do you use?

**Scenario 1:** Northwind Traders Inc., has recently acquired the Beyond Blue Airline Corporation and you are tasked with setting up the DNS infrastructure. You will have an Active Directory Domain Services (AD DS) forest named Northwind.com, and a separate tree named Beyondblueair.com. Users will regularly need to resolve names to IP addresses for servers within each domain name. You want to ensure that the DNS queries remain within the corporate infrastructure.

**Scenario 2:** Contoso LTD has diversified into several product lines, and the AD DS domain structure is being extended. Contoso.com has three existing sub domains: NA.contoso.com, EU.contoso.com and Asia.contoso.com. Plans are under way to create sub domain in each of the geographical domains, with an automotive domain under each with a two separate subdomains under each automotive domain. You need to ensure the faster possible name resolution path for internal clients.



10 minutes



## Scenario 2

Contoso LTD has diversified into several product lines, and the AD DS domain structure is being extended. Contoso.com has three existing sub domains: NA.contoso.com, EU.contoso.com and Asia.contoso.com. Plans are under way to create sub domain in each of the geographical domains, with an automotive domain under each with a two separate subdomains under each automotive domain. You need to ensure that you provide the faster possible name resolution path for internal clients.

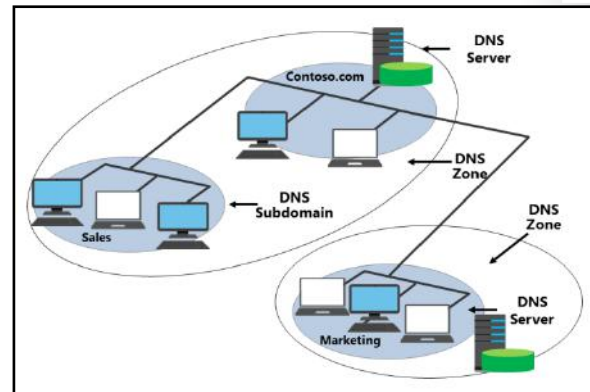
**Question:** What DNS resolution method do you use?

## Configuring delegation

DNS is a hierarchical system, and *zone delegation* connects the DNS layers. A zone delegation points to the next hierarchical level down and then identifies the name servers that are responsible for the lower-level domain.

When deciding whether to divide a DNS namespace to make additional zones, consider the following scenarios in which you might use additional zones:

- You need to delegate management of a part of the DNS namespace to another organizational location or department.
- You need to divide one large zone into smaller zones so you can distribute traffic loads among multiple servers. This improves DNS name-resolution performance, and it creates a more fault-tolerant DNS environment.
- You need to extend the namespace by adding numerous subdomains immediately to accommodate the opening of a new branch or site.



Zone delegation works similar to a top-level domain with a secondary-level domain. For example, the .com DNS servers refer all requests for Microsoft.com zone name resolution to the DNS servers at Microsoft. In this way, you delegate the Microsoft DNS zone from the .com zone. In a scenario where Microsoft has a very large sales department with numerous computers and other devices with IP addresses, it would make sense to create a zone named Sales.Microsoft.com to handle the extensive DNS workload for the sales department.

To create a delegation, within the **DNS Manager** console, in the **zones** node, in the console tree, the administrator right-clicks the **Microsoft.com** forward lookup zone and clicks the **New Delegation** item, which opens the **New Delegation Wizard**. The wizard walks the administrator through the steps to delegate authority for a subdomain to a different zone, either on the current DNS server or on another DNS server.

**Check Your Knowledge**

Question	
A stub zone consists of which of the following (choose two answers)?	
Select the correct answer.	
<input type="checkbox"/>	The IP address of one or more master servers that you can use to update the zone.
<input type="checkbox"/>	Resource records not contained in a DNS server's zone.
<input type="checkbox"/>	A cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.
<input type="checkbox"/>	Requests for all Internet names forwarded to a DNS server at an Internet service provider (ISP).
<input type="checkbox"/>	The delegated zone's Start of Authority resource record, NS resource records, and A resource records.

# Lab A: Planning and implementing name resolution by using DNS

## Scenario

Users in the A. Datum Corporation's Sydney office have been complaining about slowness and errors when connecting to internal and external websites and servers. Currently, the Sydney office only hosts client computers. Wide area network (WAN) communication between Sydney and London, where infrastructure servers are hosted, has been intermittent and is the primary cause of the issues. You have been asked to implement DNS infrastructure in Sydney by using one server that will resolve the majority of these issues.

The current DNS structure for A. Datum Corporation is as follows:

- Your Internet service provider's DNS server (131.107.0.100) provides DNS resolution and forwarding for Internet-based domain names.
- The Contoso.com domain namespace hosts web and mail services that are accessible from the Internet. These servers are also accessible from inside the A. Datum Corporation network.
- The Treyresearch.net namespace contains resources used by A. Datum Corporation employees. However, the DNS records for the Treyresearch.net zone are not located on the DNS server that clients are configured to use. They are located on **LON-SVR1**.
- **LON-DC1** provides DNS resolution for Adatum.com.

You must configure a DNS server in the Sydney location to enable more efficient name resolution for Sydney clients. The DNS server must resolve queries for local clients, and provide access to name resolution for the Internet sites, as provided by **LON-SVR1**. Sydney clients should be forwarded to an authoritative server for Adatum.com to resolve internal queries.

The requirements are as follows:

- Configuring forwarding for all DNS lookups for Internet access from Sydney to your ISP's DNS server.
- Configuring conditional forwarding on **SYD-SVR1** for the Treyresearch.net zone.
- Hosting and resolving queries for the Adatum.com domain within the Sydney location.

The virtual machines used in this lab provide the following services:

- **INET** (131.107.0.100). DNS server providing name resolution for Internet-based DNS names.
- **LON-DC1** (172.16.0.10). Domain controller and DNS server hosting the Adatum.com namespace.
- **LON-SVR1** (172.16.0.11). DNS server hosting the Treyresearch.net namespace.
- **SYD-SVR1** (172.16.19.20). The server that you will configure with DNS to provide name resolution for client computers in Sydney.

## Objectives

After completing this lab, you should be able to:

- Plan the DNS infrastructure.
- Implement DNS servers and zones.

## Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-EU-RTR**, **20741A-INET**, **20741A-LON-SVR1**, and **20741A-SYD-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - o User name: **Administrator**
  - o Password: **Pa\$\$w0rd**
  - o Domain: **Adatum**
5. Repeat steps 2 through 4 for **20741A-EU-RTR**, **20741A-INET**, **20741A-LON-SVR1** and **20741A-SYD-SVR1**.

## Exercise 1: Planning DNS name resolution

### Scenario

You must create a plan for implementing DNS name resolution according to the directions given in the lab scenario. You will be presented with a number of questions in this exercise. Write down the answers to these questions. This will help you decide how to implement the design.

The main task for this exercise is as follows:

1. Plan the DNS infrastructure to support name resolution.

#### ► Task 1: Plan the DNS infrastructure to support name resolution

Read the scenario and answer the following:

1. What is the first step in implementing your new DNS plan for the Sydney office?
2. How will you configure **SYD-SVR1** to resolve DNS queries for Internet-based addresses?
3. How will you configure **SYD-SVR1** to resolve DNS queries for the internal web server?
4. How will you configure **SYD-SVR1** to resolve queries for the Treyresearch.net DNS namespace?
5. How will you configure **SYD-SVR1** to resolve queries for the Adatum.com domain?

**Results:** After completing this exercise, you should have created a plan for implementing DNS name resolution successfully.

## Exercise 2: Implementing DNS servers and zones

### Scenario

You must install and configure the DNS infrastructure in **SYD-SVR1** according to your DNS implementation plan. Your implementation process will involve the following steps:

- Install the DNS Server role on **SYD-SVR1**.
- Configure forwarding for Internet and external queries. All external queries should be directed to your ISP's DNS servers (131.107.0.100).
- Configure the forwarding for the contoso.com domain. All DNS queries for contoso.com should be directed to **LON-SVR1** (172.16.0.11).
- Configure the forwarding for the TreyResearch.net domain. All DNS queries for TreyResearch.net should be directed to **LON-SVR1** (172.16.0.11).

The main tasks for this exercise are as follows:

1. Install the DNS server role.
2. Configure DNS forwarding.
3. Configure DNS conditional forwarding.
4. Configure zones and resource records.
5. Configure name resolution between zones.

#### ► Task 1: Install the DNS server role


- On **SYD-SVR1**, open **Server Manager** and add the DNS Server role.

#### ► Task 2: Configure DNS forwarding

1. On **SYD-SVR1**, open the **DNS** console.
2. Review the properties of the **SYD-SVR1** server:
  - a. On the **Forwarders** tab, configure forwarding to **INET1**, by using the **131.107.0.100** IP address.
  - b. Click **OK** to close the **SYD-SVR1 Properties** window.

#### ► Task 3: Configure DNS conditional forwarding

1. On **SYD-SVR1**, open the **DNS Manager** console.
2. Right-click **Conditional Forwarders**, and then create the following two condition forwarders:
  - **Adatum.com**, by using the **172.16.0.10** IP address.
  - **Contoso.com**, by using the **131.107.0.100** IP address.

 **Note:** You might see a red **X** icon beside the IP address after you press Enter. This is normal. Continue by selecting **OK** in the window. The Red **X** icon will resolve after this. You can return to the **Conditional Forwarder** dialog box, and click **Edit**, which will now show a green **Check Mark** icon in place of the red **X** icon.

**► Task 4: Configure zones and resource records**

1. On **SYD-SVR1**, create a secondary forward lookup zone for the following:
  - Name: **TreyResearch.net**
  - Master: **172.16.0.11**
2. Switch to **LON-SVR1**, and then start **Server Manager**.
3. From **Server Manager**, start the **DNS Manager**.
4. On **LON-SVR1**, in **DNS Manager**, open the **Properties** for the **TreyResearch.net** zone.
5. On the **Zone Transfers** tab, add the IP address **172.16.19.20** to **Only to the following servers** in the **Allow zone transfers** area, and to **Notify** in **The following servers** area.
6. Switch to **SYD-SVR1**, and then verify that the **Start of Authority (SOA)** and **Name Server (NS)** resource records for LON-SVR1.Adatum.com appear.

**► Task 5: Configure name resolution between zones**

1. On **LON-SVR1**, in the **TreyResearch.net** zone, add a **New Host (A or AAAA)...** resource record with the following attributes:
  - Name: **ATL-SVR1**
  - IP Address: **172.16.18.125**
2. On **SYD-SVR1**, refresh the **TreyResearch.net** secondary zone, and then confirm that the **ATL-SVR1** resource record is now present.

**Results:** After completing this exercise, you should have installed and configured DNS on **20741A-SYD-SVR1** successfully.

**► Task 6: Prepare for the next lab**

- After you finish this lab, leave the virtual machines running for the next lab.

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

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

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



## Lesson 4

# Configuring DNS integration with AD DS

When you implement DNS, one of the primary querying components in your network will be AD DS. AD DS relies on the DNS functionality for its communication between domain members. In this lesson, you will learn about the purpose of integrating DNS with AD DS, and how to integrate DNS with AD DS.

## Lesson Objectives

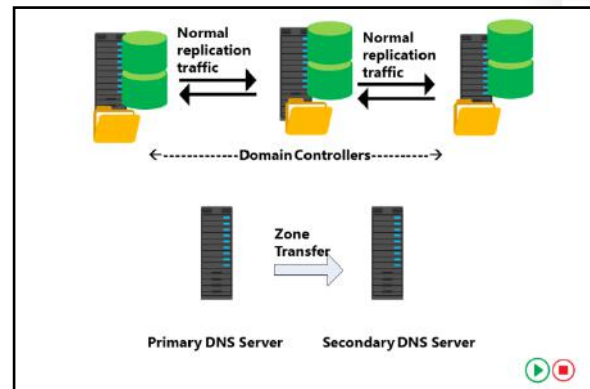
After completing this lesson, you will be able to:

- Describe AD DS and DNS integration.
- Describe SRV resource locator records.
- Explain the benefits of SRV resource locator records.
- Explain Active Directory-integrated zones.
- Describe application partitions in AD DS for DNS.
- Explain how dynamic updates work.
- Describe how to configure AD DS-integrated zones.
- Describe DNS queries.

## Overview of AD DS and DNS integration

Integrating DNS and AD DS is essential because all clients and servers use DNS to locate a domain controller so that users can sign in to a domain and use the AD DS services. Computers locate domain controllers and services by using the following records:

- Host (A) resource records. The *host (A) resource record* contains the FQDN and IP address for the domain controller.
- SRV resource records. The *SRV resource record* contains the FQDN for the domain controller and the name of the service that the domain controller provides.



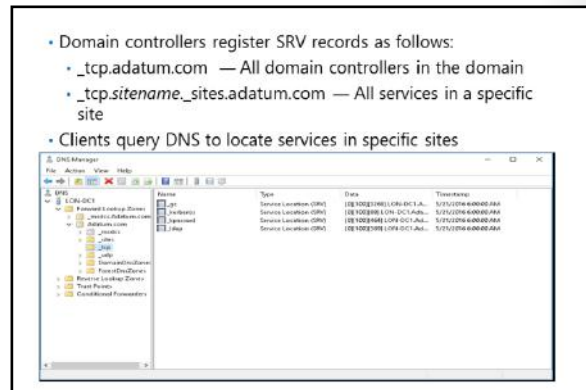
When you install an AD DS domain controller, DNS installs automatically. The integration between AD DS and DNS requires you to plan for the design of both DNS and AD DS. The number and placement of DNS servers can influence the AD DS functionality and performance greatly.

One of the most important decisions that you must make when planning for DNS is how to store DNS zone data. After installing AD DS, you can use one of the following methods for storing and replicating your zones when operating the DNS server at the new domain controller:

- Standard zone storage by using a text-based file.
- Directory-integrated zone storage by using the Active Directory database.

## What are Service Resource Locator records?

When you add a domain controller to a domain, the domain controller advertises its services by creating SRV resource records (also known as *locator records*) in DNS. Unlike host (A) resource records, which map host names to IP addresses, SRV records map services to host names. For example, to publish its ability to provide authentication and directory access, a domain controller registers Kerberos v5 protocol and Lightweight Directory Access Protocol (LDAP) SRV records. These SRV records are added to several folders within the forest's DNS zones.



For example, within the domain zone, a folder, named **name\_tcp**, contains the SRV records for all domain controllers in the domain. Additionally, within the domain zone is a folder, named **name\_sites**, which contains subfolders for each site configured in the domain. Each site-specific folder contains SRV records that represent services available in the site. For example, if a domain controller is located in a site, an SRV record will be located at the path **\_sites\sitename\\_tcp**, where *sitename* is the name of the site.

A typical SRV record contains the following information:

- The service name and port. This portion of the SRV record indicates a service with a fixed port. It does not have to be a well-known port. SRV records in Windows Server 2012 include LDAP (port 389), Kerberos (port 88), Kerberos password protocol (KPASSWD, port 464), and global catalog services (port 3268).
- Protocol. The TCP or User Datagram Protocol (UDP) is indicated as a transport protocol for the service. The same service can use both protocols in separate SRV records. Kerberos records, for example, are registered for both TCP and UDP. Microsoft clients use only TCP, but UNIX clients can use both UDP and TCP.
- Host name. The host name corresponds to the host (A) record for the server hosting the service. When a client queries for a service, the DNS server returns the SRV record and associated host (A) records, so the client does not need to submit a separate query to resolve the IP address of a service.

The service name in an SRV record follows the standard DNS hierarchy with components separated by dots. For example, a domain controller's Kerberos service is registered as `kerberos._tcp.sitename._sites.domainName`, where:

- `kerberos` is a Kerberos Key Distribution Center (KDC) that uses TCP as its transport protocol.
- `_tcp` is any TCP-based services in the site.
- `sitename` is the site of the domain controller registering the service.
- `_sites` is all sites registered with DNS.
- `domainName` is the domain or zone, for example, `contoso.com`.

## Benefits of Service Resource Locator records

DNS supports dynamic registration of SRV resource records registered by an AD DS domain controller during promotion. With the help of SRV records, client devices can find domain controllers in the network.

In certain situations, an organization might have computers in a location that does not have, nor would it be desirable to have, domain controllers. Sites can be created without domain controllers; however, as noted above, the site would not have a corresponding domain controller listing in the `_sites\sitename\_tcp` path.

### Benefits of SRV Resource Records

- Domain controllers register their SRV resource records dynamically, by service and site location
- Client systems in sites use SRV resource records recorded in a site to find domain controllers in their own site before attempting to connect to domain controllers across wide area network links
- Keeps network traffic across links down and manageable

### Benefit of SRV records

SRV records are used to locate services such as domain controllers and mail servers, and to integrate SRV records and AD DS sites. One of the main reasons to create a site is to ensure clients authenticate first against their local domain controllers, rather than any domain controller in the domain. The SRV records can identify the specific site in which a domain controller is located.

When you join a Windows operating system client to a domain and then restart it, the client completes a domain controller location and registration process. The goal of this registration process is to locate the domain controller with the most efficient and closest location to the client's location, based on IP subnet information.

The process for locating a domain controller is as follows:

1. The new client queries for all domain controllers in the domain. As the new domain client restarts, it receives an IP address from a DHCP server, and is ready to authenticate to the domain. However, the client does not know where to find a domain controller. Therefore, the client queries for a domain controller by querying the `_tcp` folder, which contains the SRV records for all domain controllers in the domain.
2. The client attempts an LDAP ping to all domain controllers in a sequence. DNS returns a list of all matching domain controllers and the client attempts to contact all of them on its first startup.
3. The first domain controller responds. The first domain controller that responds to the client examines the client's IP address, cross-references that address with subnet objects, and informs the client of the site to which the client belongs. The client stores the site name in its registry, and then queries for domain controllers in the site-specific `_tcp` folder.
4. The client queries for all domain controllers in the site. DNS returns a list of all domain controllers in the site.
5. The client attempts an LDAP ping sequentially to all domain controllers in the site. The domain controller that responds first authenticates the client.
6. The client forms an affinity. The client forms an affinity with the domain controller that responded first, and then attempts to authenticate with the same domain controller in the future. If the domain controller is unavailable, the client queries the site's `_tcp` folder again, and again attempts to bind with the first domain controller that responds in the site.

If the client moves to another site, which might be the case with a mobile computer, the client attempts to authenticate to its preferred domain controller. The domain controller notices that the client's IP address is associated with a different site, and then refers the client to the new site. The client then queries DNS for domain controllers in the local site to find the specific SRV record for its new site. You also can configure site coverage and SRV record priority manually if you want to control authentication in sites without domain controllers.

## What are Active Directory–integrated zones?

A primary zone server is a single point of failure. If it goes down, because the secondary zone servers are read-only, they can resolve names, but cannot store additional records or accept changes to records.

You can make a DNS zone fault tolerant by integrating it into AD DS. By doing this, it makes the DNS zone an AD DS–integrated zone. A DNS server can store zone data in the AD DS database if the DNS server is a domain controller. When the DNS server stores zone data in this way, the records in the zone file are stored as AD DS

objects, and the various properties of these objects are considered AD DS attributes. All domain controllers that host the DNS zone in the AD DS database are considered primary zone servers for the zone, and they can accept changes to the DNS zone and then replicate those changes to all other domain controllers. Because it uses AD DS replication, each change is sent securely via encrypted replication traffic. If a domain controller with an Active Directory–integrated DNS zone fails, as long as there are other domain controllers with the Active Directory–integrated zone, DNS functionality for that zone and the domain continue to operate correctly.

A DNS server can store zone data in the AD DS database provided that the DNS server is an AD DS domain controller. When the DNS server stores zone data in this way, this creates an Active Directory–integrated zone.

The benefits of an Active Directory–integrated zone are significant:

- **Multi-master updates.** Unlike standard primary zones, which can only be modified by a single primary server, Active Directory–integrated zones can be written to by any writable domain controller to which the zone is replicated. This builds redundancy into the DNS infrastructure. In addition, multi-master updates are particularly important in organizations that use dynamic update zones and have locations that are distributed geographically. Clients can update their DNS records without having to connect to a potentially geographically distant primary server.
- **Replication of DNS zone data by using AD DS replication.** One characteristic of Active Directory replication is attribute-level replication, in which only changed attributes are replicated. An Active Directory–integrated zone can thus avoid replicating the entire zone file as in traditional DNS zone transfer models.
- **Secure dynamic updates.** An Active Directory–integrated zone can enforce secure dynamic updates.
- **Detailed security.** As with other Active Directory objects, an Active Directory–integrated zone enables you to delegate administration of zones, domains, and resource records by modifying the access control list (ACL) on the zone.

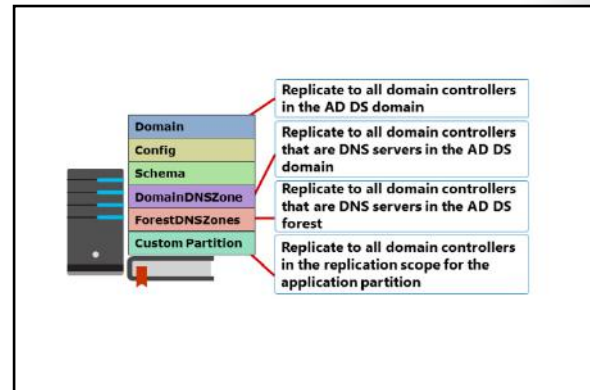
**Question:** Are there any disadvantages to storing DNS information in AD DS?

### An Active Directory–integrated zone:

- Allows multi-master writes to zone
- Replicates DNS zone information by using AD DS replication:
  - Leverages efficient replication topology
  - Uses efficient incremental updates for Active Directory replication processes
- Enables secure dynamic updates
- Delegates zones, domains, and resource records for increased security

## Application partitions in AD DS

The DNS installation process creates two default application partitions: the domainDNSZones application partition and the forestDNSZones application partition. Domain controllers within a domain that have the DNS service installed automatically receive a copy of the domainDNSZones application partition. All domain controllers within the forest—if they have the DNS service installed—receive a copy of the forestDNSZones application partition. However, if you have DNS implemented in your environment, and if you use the existing DNS servers for AD DS, the Active Directory installation will not create the default application partitions.



You can create additional application partitions to store information. When you create an application partition, you must define which of the forest's domain controllers will participate in its replication. To create application partitions and enlist servers to replicate application partitions, use the Dnscmd.exe tool or the Ntdsutil.exe AD DS command-line tool.

When using Active Directory–integrated zones, you can control which domain controllers receive a zone by using AD DS partitions. You can also define which domain controllers within your AD DS forest receive a copy of a given application partition. This helps reduce replication traffic by allowing AD DS to replicate the zone data only to domain controllers that require the information.

### Specifying the replication scope

You can specify the replication scope when you create an Active Directory–integrated zone, or you can change the scope later. You can replicate to:

- All DNS servers in the Active Directory forest. The forestDNSZones application partition stores this zone. All domain controllers in the forest—if they have DNS installed—receive a copy of the zone. This configuration is recommended for zones that all clients need to be able to access throughout the Active Directory forest. For example, the \_msdcs zone includes information about global catalog servers and domain controllers to which hosts anywhere in the forest might require access. You can store this zone in the forestDNSZones partition if your forest includes multiple domains and locations.
- All DNS servers in the Active Directory domain. The domainDNSZones application partition stores this zone. Only domain controllers in the same domain on which you install the DNS service receive a copy of this zone.
- All domain controllers in the Active Directory domain. The domain partition stores this zone, and all domain controllers in the domain receive a copy of it, even if you do not install the DNS service on them. This might cause unwanted replication traffic.
- All domain controllers that you specify in the replication scope of the specified application directory partition. The domain controllers that receive a copy of the application partition will receive a copy of the zone. You must create the application partition in advance.

## Dynamic updates

A *dynamic update* is an update to DNS in real time. Dynamic updates are important for DNS clients that change locations, because they can dynamically register and update their resource records without manual intervention.

The DHCP client service performs the registration, regardless of whether the client's IP address is obtained from a DHCP server or is fixed. The registration occurs during the following events:

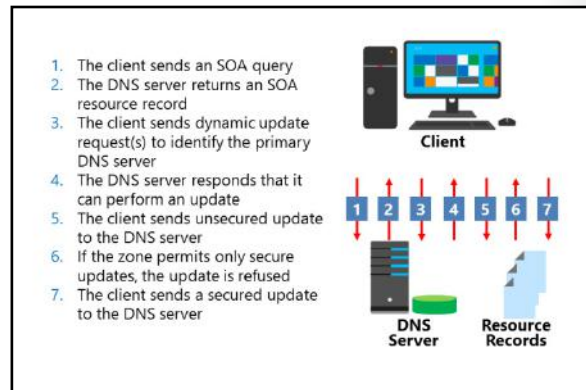
- When the client starts, and the DHCP client service is started.
- When an IP address is configured, added, or changed on any network connection.
- When an administrator executes the Windows PowerShell cmdlet **Register-DNSClient** or runs the **ipconfig /registerdns** at a command prompt.

The process of dynamic updates is as follows:

1. The client identifies a name server and sends an update. If the name server hosts only a secondary zone, the name server refuses the client's update. If the zone is not an Active Directory–integrated zone, the client might have to do this several times.
2. If the zone supports dynamic updates, the client eventually reaches a DNS server that can write to the zone. This DNS server is one of the following:
  - The primary server for a standard, file-based zone.
  - Any domain controller that is a name server for an Active Directory–integrated zone, which is, by default, considered primary because it is writable.
3. If the zone is configured for secure dynamic updates, the DNS server refuses the change. The client then authenticates and resends the update.

In some configurations, you might not want clients to update their records even in a dynamic update zone. In this case, you can configure the DHCP server to register the records on the client's behalf. By default, a client registers that it is a (host/address) record, and the DHCP server registers the PTR (pointer/reverse lookup) record.

By default, Windows operating systems attempt to register their records with their DNS server. You can modify this behavior in the client IP configuration or through Group Policy. Domain controllers also register their SRV records (and their host records) in DNS. SRV records are registered automatically each time the NETLOGON service starts.



## Demonstration: Configuring AD DS–integrated zones

To create an Active Directory–integrated zone, you must install a DNS server on a domain controller. All changes in an Active Directory–integrated zone replicate to the other DNS servers that are on domain controllers through the AD DS multi-master replication model.

In this demonstration, you will learn how to:

- Promote a server as a domain controller.
- Create an Active Directory–integrated zone.
- Create a record.
- Verify replication to a second DNS server.

### Demonstration Steps

#### Promote a server as a domain controller

1. Install the AD DS server role on **TOR-SVR1**.
2. Start the **Active Directory Domain Services Configuration Wizard**.
3. Provide **Pa\$\$w0rd** as the recovery password and then accept all other default selections.
4. After the server restarts, sign in as **Adatum\Administrator** with the password of **Pa\$\$w0rd**.

#### Create an Active Directory–integrated zone

1. On **LON-DC1**, open the **DNS Manager** console.
2. Start the **New Zone Wizard**.
3. Create a new Active Directory–integrated forward lookup zone named **TreyResearch.net** that allows only secure dynamic updates.
4. Review the records in the **TreyResearch.net** zone.

#### Create a record

- Create a **New Host** record in the **TreyResearch.net** zone named **www**, and then have it point to **172.16.0.100**.

#### Verify replication to a second DNS server

- Verify that new record is replicating to the **TOR SVR1** DNS server.

## Lab B: Integrating DNS with AD DS

### Scenario

After making additional improvements to the WAN connection between London and Sydney locations, you have been asked to enable **SYD-SVR1** to update and replicate records for the Adatum.com domain.

### Objectives

After completing this lab, you should be able to integrate DNS with AD DS.

### Lab Setup

Estimated Time: **20 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-EU-RTR**, and **20741A-SYD-SVR1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

You should have the virtual machines **20741A-LON DC1**, **20741A-EU-RTR**, **20741A-INET**, **20741A-LON SVR1**, and **20741A-SYD-SVR1** from the previous lab still running.

## Exercise 1: Integrating DNS with AD DS

### Scenario

You need to deploy another Active Directory-integrated DNS server in Adatum.com. To do this, you will promote **SYD-SVR1** to a domain controller, and integrate DNS with the AD DS database for Adatum.com.

The main tasks for this exercise are as follows:

1. View resource records for the Sydney location.
2. Install AD DS on **SYD-SVR1**.
3. Review resource records on **SYD-SVR1**.

#### ► Task 1: View resource records for the Sydney location

1. In **DNS Manager** on **SYD-SVR1**, note that the Adatum.com forward lookup zone does not exist under this server.
2. Delete the **Adatum.com Conditional Forwarder** entry.
3. Open **DNS Manager** on **LON-DC1** and note the resource records in the **Adatum.com** zone. You will compare these records to the set of records on **SYD-SVR1** when it is promoted to a domain controller.

#### ► Task 2: Install AD DS on SYD-SVR1

1. Install the AD DS server role on **SYD-SVR1**.
2. After the server role is installed, start the **Active Directory Domain Services Configuration Wizard**.
3. Ensure that the **DNS Server** service and **Global Catalog** are installed. Use **Pa\$\$w0rd** for the **Directory Services Restore Mode Password**, and use the default values for all other selections. Allow the server to restart as indicated.
4. After **SYD-SVR1** restarts, sign in as **Adatum\administrator** with the password **Pa\$\$w0rd**.
5. Open the **Network and Sharing Center**, open the Ethernet adapter properties, and then open the **Internet Protocol Version 4 (TCP/IP4)** properties.



6. Change the **Preferred DNS server** to **172.16.19.20**, and the **Alternate DNS server** to **172.16.0.10**.
7. Close all open windows.

► **Task 3: Review resource records on SYD-SVR1**

1. On **SYD-SVR1**, open **Server Manager**, open the **DNS Manager** console and go to the **Adatum.com** forward lookup zone's properties. Examine the **Start of Authority** tab, and then confirm that the primary server listed is **SYD-SVR1.adatum.com**.
2. Review the resource records in the **Adatum.com** domain, and then confirm that they are the same as the resource records observed on **LON-DC1**.
3. Create a **New Host (A or AAAA)...** record named **SYD-CL1** with the IP address **172.16.19.150**.
4. Switch to the **DNS** console on **LON-DC1**, refresh the **Adatum.com** zone, and then confirm that the **SYD-CL1** resource record appears.
5. If the record does not appear, open the **Active Directory Sites and Services** console, force replication from **SYD-SVR1** to **LON-DC1**, and then check the resource record again. It should appear.
6. Close all open windows.

**Results:** After completing this exercise, you should have integrated DNS with AD DS successfully.

► **Task 4: Prepare for the next lab**

- After you finish this lab, leave the virtual machines running for the next lab.

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

## Lesson 5

# Configuring advanced DNS settings

DNS implementations often require complex infrastructure layouts and functionality that ensures the security and proper resolution of DNS queries. This lesson will introduce you to several advanced configuration options for DNS in Windows Server 2016. You will also learn to troubleshoot and monitor DNS servers and name resolution.

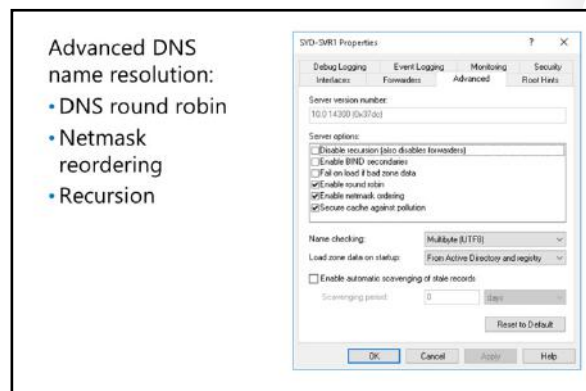
### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to configure advanced DNS name resolution.
- Describe how to configure root hints.
- Describe the GlobalNames zone.
- Describe how to configure a GlobalNames zone.
- Describe split DNS.
- Explain how to implement split DNS.
- Describe DNS policies.
- Describe how to configure DNS policies.
- Describe how to implement DNS security.
- Explain how to implement DNS Security Extensions (DNSSEC).
- Describe how to configure DNSSEC.
- Describe DNS on Nano server.

### Configuring advanced DNS name resolution

When devices communicate with each other by using TCP/IP, they begin the process by creating packets of data that will go out of the network adapter to other devices over the configured media of copper wires, fiber optic cables or radio signals. These packets must contain the specific IP address of the device for which the message is intended. To find that address, devices use DNS name resolution queries based on the FQDN of the device. The FQDN contains the zone name, or, if the client resolver does not have the zone name, appends its own to the name resolution packet.



## DNS round robin

A DNS zone can contain many records and different types of records. These records represent IP addresses of a given host name, alias names, service locator, mail exchanger, and other specialized records. Computers can have more than one IP address on separate network adapters, or several IP addresses can be bound to the same adapter. In this case, the computer's host name will resolve not to one IP address, but two or more, depending on how many IP addresses it has. Each of these addresses should have a host resource record in the DNS forward lookup zone so that they can be resolved.

*DNS round robin* functionality determines which IP addresses to return for a given name. This function returns a list of all the IP addresses for a given name, and then alternates IP addresses within the list for every DNS query from a unique source. If a DNS responded with a different IP each time to the same requester, the benefits of caching would be undermined, and it would be inefficient. For example, if you have a number of web servers that all have the same content and you want to load balance the HTTP GET commands sent to them, you need to create an (A) resource record for each web server with the same name. For example, you could create the following:

```
www.contoso.com 60 IN A 172.16.0.11
www.contoso.com 60 IN A 172.16.0.120
www.contoso.com 60 IN A 172.16.0.133
```

When clients send name resolutions to the DNS server for `www.contoso.com`, the requests will be returned as follows:

First request:

```
172.16.0.11
172.16.0.120
172.16.0.133
```

Second request:

```
172.16.0.120
172.16.0.133
172.16.0.11
```

Third request:

```
172.16.0.133
172.16.0.11
172.16.0.120
```

The requests continue to rotate through the list for all three addresses. Theoretically, every web server will receive one third of all requests, and that would load balance the three servers. You should be aware that using DNS round robin to load balance requests cannot provide any fault tolerance. If one of the three servers goes down, then approximately one third of the clients are sent to an IP address that will not respond. Once it times out, these clients can then go to the next address on the list.

Using DNS round robin also returns lists of domain controllers for client authentication. When a user attempts to sign in to a domain, the Local Security Authority Subsystem Service sends a name resolution request for the service locator records to the preferred DNS server found in the TCP/IP properties of the client. The DNS server searches through the service locator records and returns all of the domain controllers' IP addresses found for that zone. This list uses a DNS round robin function similar to the `www.contoso.com` address shown above. This is because it returns all of the multiple IP addresses for the domain controllers in that domain, and each subsequent request for the same list returns in a different order.

## Netmask reordering

A very similar option to DNS round robin is netmask reordering. A DNS client receives results that are most relevant to its location. If one of the name resolutions to a DNS query is in the same physical subnet as the client, it gets that resolution instead of a resolution from a different subnet. Here is an example:

You have a client with an IP address of 172.16.0.150. The client queries its DNS server for the IP address of www.Contoso.com. The www.Contoso.com name has two host resource records, 172.16.0.44 and 10.45.7.44. Because 172.16.0.44 is in the same Class B subnet as the client, the DNS server returns 172.16.0.44. The client is able to get to the web server on the same physical subnet instead of having to route to some other subnet, which results in faster response than using the external address.

## Recursion

When a DNS server receives an iterative query, it might answer with the IP address for the domain name, if it is known, or with a referral to the DNS servers that are responsible for the domain being queried.

When a DNS server communicates with a root hints server, it only uses an iterative query. If you select the **Do Not Use Recursion For This Domain** option in the **DNS Server Properties** window, the server will not be able to perform queries on the root hints. You might set this option if you want to restrict all name resolutions to a particular network for security purposes.

If you configure a server to use a forwarder, it will attempt to send a recursive query to its forwarding server. If the forwarding server does not answer this query, the server will respond that the host could not be found.

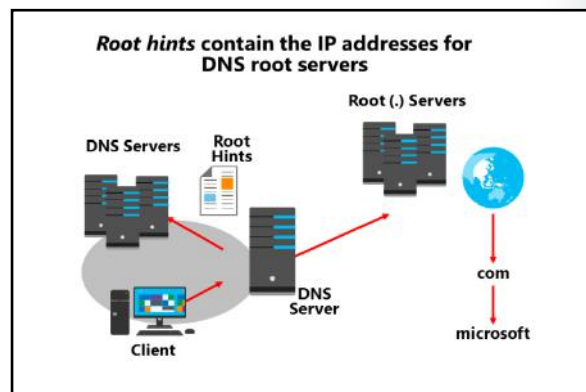
It is important to understand that recursion on a DNS server and recursive queries are not the same thing. Recursion on a server means that the server will use its root hints and try to resolve a DNS query.

## Configuring root hints

*Root hints* are a list of the 13 FQDNs on the Internet that your DNS server uses if it cannot resolve a DNS query by using its own zone data, a DNS forwarder, or its own cache. The root hints list the highest servers in the DNS hierarchy, and can provide the necessary information for a DNS server to perform an iterative query to the next-lowest layer of the DNS namespace.

Root servers are installed automatically when you install the DNS role. They are copied from the **cache.dns** file that is included in the DNS role setup files. You also can add root hints to a DNS server to support lookups for noncontiguous domains within a forest.

When a DNS server communicates with a root hint server, it uses only an iterative query. To configure a server to use only recursive queries to a forwarder, configure the forwarder on the DNS server properties. If you want to disable all iterative queries, deselect the **Use root hints if no forwarders are available** option on the **Forwarders** tab. If you configure the server to use only a forwarder, and you disable root hints, it attempts to send a recursive query to its forwarding server; if the forwarding server does not answer this query, the first server responds that the host could not be found.



It is important to understand that recursion on a DNS server and recursive queries are not the same thing. Recursion on a DNS server means that the server uses its root hints to try to resolve a DNS query, whereas a recursive query is a query that is made to a DNS server in which the requester asks the server to assume the responsibility for providing a complete answer to the query.

IPv6 root hints, as published by Internet Assigned Numbers Authority (IANA), have been added to Windows Server 2016 DNS. Internet name queries can now use IPv6 root servers to perform name resolutions.

## What is the GlobalNames zone?

The DNS Server service in Windows Server 2016 provides the GlobalNames zone, which you can use to contain single-label names that are unique across an entire forest. This eliminates the need to use the NetBIOS-based WINS to provide support for single-label names. GlobalNames zones provide single-label name resolution for large enterprise networks that do not deploy WINS and that have multiple DNS domain environments. You create GlobalNames zones manually, and they do not support dynamic record registration.

When clients try to resolve short names, they append their DNS domain name automatically. Depending on the configuration, they also try to find the name in upper-level domain name, or work through their name suffix list. Therefore, short names are resolved in the same domain.

You use a GlobalNames zone to maintain a list of DNS search suffixes for resolving names among multiple DNS domain environments. For example, if an organization supports two DNS domains, such as Adatum.com and contoso.com, users in the Adatum.com DNS domain need to use an FQDN, such as data.contoso.com, to locate the servers in contoso.com. Otherwise, the domain administrator needs to add a DNS search suffix for contoso.com on all the devices in the Adatum.com domain. If the clients search for the server name **data**, the search would fail.

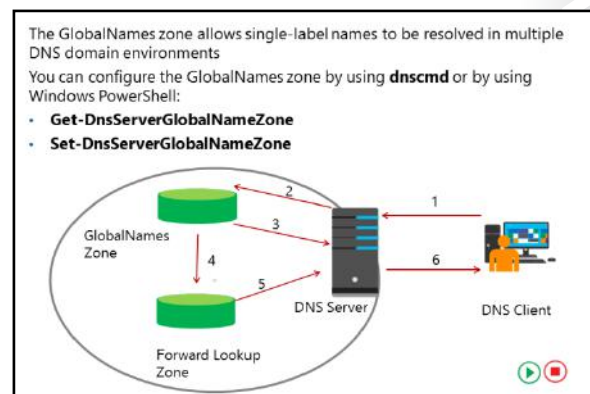
Global names are based on alias (CNAME) resource records in a special forward lookup zone that uses single names to point to FQDNs. For example, GlobalNames zones would enable clients in both the Adatum.com domain and the contoso.com domain to use a single label name, such as **data**, to locate a server whose FQDN is data.contoso.com without having to use the FQDN.

### Creating a GlobalNames zone

To create a GlobalNames zone, perform the following steps:

1. Use **dnscmd** to enable GlobalNames zones support.
2. Create a new forward lookup zone named **GlobalNames** (not case sensitive). Do not allow dynamic updates for this zone.
3. Manually create **CNAME** records that point to records that already exist in the other zones that are hosted on your DNS servers.

For example, you could create a CNAME record in the GlobalNames zone named **Data** that points to Data.contoso.com. This enables clients from any DNS domain in the organization to find this server by the single-label name of Data.



You can also use the Windows PowerShell cmdlets **Get-DnsServerGlobalNameZone** and **Set-DnsServerGlobalNameZone** to configure GlobalNames zones.

## Demonstration: Configuring the GlobalNames zone

In this demonstration, you will learn how to create a GlobalNames zone.

### Demonstration Steps

1. On **LON-DC1**, create an Active Directory–integrated forward lookup zone named **Fabrikam.com**, by running the following command:

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

2. Run the following command to enable support for GlobalName zones:

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

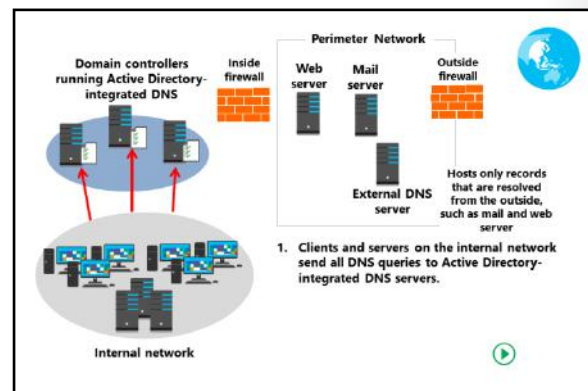
3. Create an Active Directory–integrated forward lookup zone named **GlobalNames** by running the following command:

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

4. Open the **DNS Manager** console, and add a new host record to the Fabrikam.com domain named **App1** with the IP address **172.16.0.200**.
5. In the **GlobalNames** zone, create a new alias named **App1** by using the FQDN of **App1.Fabrikam.com**.
6. Close the **DNS Manager** console, and close the **Windows PowerShell** window.

## Understanding split DNS

In Windows operating systems, DNS has two major functions: to resolve IP addresses to names (and vice versa), and to facilitate domain-level communications and authentication for AD DS. The ability to store SRV records allows domain-member clients to find domain controllers for domain authentication and security while load balancing access to the various domain controllers by using DNS round-robin functionality. However, Internet-level untrusted users from outside the firewall should never be able to access the SRV records and other sensitive AD DS information from the internal DNS servers. That data must remain separate and inaccessible from outside the firewall. At the same time, DNS records of servers and services hosting Internet level resources, such as web, mail, and proxy servers, must remain accessible.




*Split DNS*, also known as split-brain DNS, uses the same DNS domain name for both Internet and internal domain-member resources. However, the DNS server role is assigned to separate servers: one or more servers for the Internet, and the other server(s) for the AD DS domain. Deploying DNS this way requires extra steps to ensure that sensitive information found on the AD DS domain side is separated from the Internet side, and to ensure that only the DNS server deployed on the Internet side, that is, outside the inner firewall, can be accessed by queries from outside the firewall.

Because DNS is such a vital function for AD DS, the DNS server role is usually included with domain controllers when they are deployed. This role can be integrated into AD DS so that DNS records are stored as Active Directory objects and attributes. The DNS zone type in this instance is referred to as Active Directory integrated. Active Directory-integrated zones replace DNS zone transfers with AD DS replication and can ensure secure dynamic updates of client records to the zone. In a domain, using Active Directory-integrated DNS is considered a best practice.

With split DNS, internal clients are only configured with the IP addresses of the Active Directory-integrated DNS servers, which are domain controllers. All client DNS dynamic updates are written to the servers. All DNS queries from internal clients go only to these DNS servers. If any name resolutions are needed beyond the internal domain, such as for Internet web servers, the Active Directory-integrated DNS servers forward these requests to the Internet-facing DNS server. The Internet-facing DNS servers are normally deployed in the perimeter network between the firewalls. Although they have the same domain name as the Active Directory-integrated DNS servers, the Internet-facing DNS servers do not store the same data. All records in the Internet-facing DNS server zone are created manually. Normally, the Internet-facing DNS server zone only contains records for itself and other servers that are located in the perimeter network and need to be accessed from the Internet.

When a query to the Internet-facing DNS server comes in from the Internet requesting a resolution on any domain-level resource, such as an SRV record, the Internet-facing DNS server rejects the query because it does not have any of the SRV records—these are only stored in the domain Active Directory-integrated DNS servers. Because it considers itself authoritative for the zone, the Internet-facing DNS server does not make an iterative query to the Active Directory-integrated DNS servers.

To further enhance security, you can set a firewall rule on the inside firewall, that is, the firewall between the internal and perimeter networks, to reject all DNS (UDP port 53) queries from the perimeter to the internal network, while still allowing DNS replies.

 **Note:** When you use DirectAccess for portable clients, be aware that when the client is deployed outside of the internal network, it uses the Name Resolution Policy Table (NRPT) for continued access to internal resources. This sends DNS name queries for internal resources to the Active Directory-integrated DNS servers. With split DNS and DirectAccess clients, you need to add the FQDN of any Internet-level web servers kept in the perimeter network to the NRPT as a firewall exception rule.

## Implementing split DNS

Using the same namespace internally and externally simplifies resource access from the perspective of users, but it also increases management complexity. You should not make internal DNS records available externally, but some synchronization of records for external resources typically is required. For example, both your internal and external namespaces might use the name *Contoso.com*.

Using unique namespaces for the internal and public namespaces provides a clear delineation between internal and external DNS, and avoids the need to synchronize records between the namespaces. However, in some cases, having multiple namespaces might lead to user confusion. For example, you might choose the external namespace of *Contoso.com* and the internal namespace of *Contoso.local*. Note that when you implement a unique namespace configuration, you no longer are tied to using registered domain names.

Using a subdomain of the public namespace for AD DS avoids the need to synchronize records between the internal and external DNS servers. Because the namespaces are linked, users typically find this structure easy to understand. For example, if your public namespace is *Contoso.com*, you might choose to implement your internal namespace as the subdomain *AD*, or as *AD.Contoso.com*.

- **Same namespace:**
  - Internal records should not be available externally
  - Records might need to be synchronized between internal and external DNS
- **Unique namespace:**
  - Record synchronization is not required
  - Existing DNS infrastructure is unaffected
  - Clearly delineates between internal and external DNS
- **Subdomain:**
  - Record synchronization is not required
  - Contiguous namespace is easy to understand

### Considering split DNS

Having a matching internal and external DNS namespace can pose certain problems. However, split DNS can provide a solution to these problems. Split DNS is a configuration in which your domain has two root-server zones that contain domain-name registration information. Your internal network hosts are directed to one zone, whereas external hosts are directed to another for name resolution. For example, in a nonsplit DNS configuration for the domain *contoso.com*, you might have a DNS zone that looks like the example in the following table.

Host	Record type	IP address
www	A	131.107.1.200
Relay	A	131.107.1.201
Webserver1	A	192.168.1.200
Exchange1	A	192.168.0.201

When a client computer on the Internet wants to access the SMTP relay by using the published name of *relay.contoso.com*, it queries the DNS server that returns the result 131.107.1.201. The client then establishes a connection over SMTP to that IP address.

However, the client computers on the organization's intranet also use the published name of *relay.contoso.com*. The DNS server returns the same result: a public IP address of 131.107.1.201. The client now attempts to establish a connection to the returned IP address by using the external interface of the publishing computer. Depending on the client configuration, this might or might not be successful.

By configuring two zones for the same domain name—one on each of the two DNS servers—you can avoid this problem.



The internal zone for Adatum.com would contain the information in the following table.

Host	Record type	IP address
www	CNAME	Webserver1.contoso.com
Relay	CNAME	Exchange1.contoso.com
Webserver1	A	192.168.1.200
Exchange1	A	192.168.0.201

The external zone for Adatum.com would contain the information in the following table.

Host	Record type	IP address
www	A	131.107.1.200
Relay	A	131.107.1.201
	MX	Relay.contoso.com

Now client computers in the internal and external networks can resolve the name relay.contoso.com to the appropriate internal or external IP address.

## DNS policies

DNS Policy is a new feature for DNS in Windows Server 2016. You use DNS policies to manipulate how a DNS server handles queries based on different factors. As an example, you might create a DNS policy to respond to queries asking for the IP address of a web server to respond with a different IP address based on the closest datacenter to the client. This differs from netmask reordering because the client will not have the same local subnet address of the web server, but the particular web server is closer than others, from the perspective of the client.

- DNS policy scenarios:
  - Application high availability
  - Traffic management
  - Split brain DNS
  - Filtering
  - Forensics
- DNS policy objects:
  - Client subnet
  - Recursion scope
  - Zone scope
- Use Windows PowerShell to create and manage DNS policies

### Scenarios for using DNS policies

You can create several DNS policies depending on your needs. There are various factors that might benefit from creating a DNS policy, based on the following scenarios:

- Application high availability. Clients are redirected to the healthiest endpoint for an application, where healthiest is determined by high availability factors in a failover cluster.
- Traffic management. Clients are redirected to the closest datacenter or server location.
- Split-brain DNS. Clients receive a response based on whether they are internal or external, and the DNS records are split into different zone scopes.
- Filtering. DNS queries are blocked if they are from a list of malicious IP addresses or FQDNs.
- Forensics. Malicious DNS clients are redirected to a sinkhole instead of the computer they are trying to reach.



**Note:** DNS sinkholes, sometimes referred to as black hole DNS, are used to spoof DNS servers to prevent resolving host names of specified Uniform Resource Locators (URLs). You can configure the DNS forwarder to return a false IP address to a specific URL. You can use a DNS sinkhole to prevent access to malicious URLs at the enterprise level. The malicious URLs are blocked by adding a false resource record in DNS, thereby creating a second level of protection.



**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>

- Time-of-day based redirection. Clients are redirected to datacenters based on the time of the day.

### DNS policy objects

To use the above scenarios to create policies, you must identify groups of records in a zone, groups of clients on a network, or other elements. The elements are identified by the following new DNS objects:

- Client subnet. This represents the IPv4 or IPv6 subnet from which queries are sent to a DNS server. You create subnets to later define policies that you apply based on the subnet that generates the requests. For example, you might have a split-brain DNS scenario, where the name resolution request for *www.contoso.com* can be answered with an internal IP address to internal clients, and a different IP address to external clients.
- Recursion scope. This represents unique instances of a group of settings that control DNS server recursion. A recursion scope holds a list of forwarders and specifies whether or not recursion is used. A DNS server can have multiple recursion scopes. You can use DNS server recursion policies to choose a recursion scope for a given set of queries. If the DNS server is not authoritative for certain queries, DNS server recursion policies let you control how to resolve those queries. In this case, you can specify which forwarders to use and whether to use recursion.
- Zone scopes. DNS zones can have multiple zone scopes, and each zone scope can contain its own set of DNS resource records. The same resource record can be present across multiple scopes, with different IP addresses depending on the scope. Additionally, zone transfers can be done at the zone-scope level. This will allow resource records from a zone scope in a primary zone to be transferred to the same zone scope in a secondary zone.

### Create and manage DNS policies

You create DNS policies based on level and type. You can use query-resolution policies to define how client name resolution queries get handled, and zone-transfer policies to define zone transfers. You can apply both policy types at the server or zone level.

You can create multiple query resolution policies of the same level, as long as they have a different value for the processing order. Recursion policies are a special kind of server-level policies. They control how a DNS server performs query recursion, if at all. Recursion policies only apply when query processing reaches the recursion path. You can choose a value of **DENY** or **IGNORE** for recursion for a given set of queries. Otherwise, you can choose a set of forwarders for a set of queries.

You use Windows PowerShell version 5.0 or higher to create and manage DNS policies. The following example shows how to create traffic management policies to direct the client name resolution requests from a certain subnet to an Asian datacenter, and from another subnet to an Australian datacenter:

```
Add-DnsServerClientSubnet -Name "AsiaSubnet" -IPv4Subnet "172.21.33.0/24"
Add-DnsServerClientSubnet -Name "AustraliaSubnet" -IPv4Subnet "172.17.44.0/24"
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "AsiaZoneScope"
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "AustraliaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.17.97.97" -ZoneScope "AustraliaZoneScope"
Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.21.21.21" -ZoneScope "AsiaZoneScope"
Add-DnsServerQueryResolutionPolicy -Name "AsiaPolicy" -Action ALLOW -ClientSubnet
"eq,AsiaSubnet" -ZoneScope "AsiaZoneScope,1" -ZoneName "Contoso.com"
Add-DnsServerQueryResolutionPolicy -Name "AustraliaPolicy" -Action ALLOW -ClientSubnet
"eq,AustraliaSubnet" -ZoneScope "AustraliaZoneScope,1" -ZoneName contoso.com
```



**Note:** For more information, refer to: "Domain Name System (DNS) Server Cmdlets" at <http://aka.ms/M7n1ow>

## Demonstration: Configuring DNS policies

In this demonstration, you will learn how to create a DNS policy that returns a different server address that depends upon the client location.

### Demonstration Steps

#### Create www.adatum.com CNAME record and test resolution

1. On **LON-DC1**, in the **DNS Manager** console, create a **CNAME** resource record named **www.adatum.com** that points to LON-DC1.adatum.com.
2. Switch to **TOR-SVR1**.
3. On **TOR-SVR1**, flush the DNS client cache, and then perform name resolution on www.adatum.com. Verify that the name resolves to an IP address of **172.16.0.10**.
4. Switch to **LON-CL1**.
5. On **LON-CL1**, flush the DNS client cache, and then perform name resolution on www.adatum.com. 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 that has all the below cmdlets you can use to copy and paste the below cmdlets into Windows PowerShell to eliminate excessive typing.

1. Switch to **LON-DC1**.
2. On **LON-DC1** open the **Windows PowerShell** console.

- Run the following cmdlets in Windows PowerShell, and 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
```

- Test the results by performing an **nslookup** command for **www.adatum.com** on **LON-CL1**, and then for **TOR-SVR1**. You should get the respective IP addresses depending on the zone that you created above.

## Implementing DNS security

Because DNS is a critical network service, you must protect it as much as possible. You can choose among several options for protecting the DNS server, including:

- DNS cache locking
- DNS socket pool
- DNSSEC

### DNS cache locking

*Cache locking* is a Windows Server 2016 security feature that you can use to control when

information in the DNS cache can be overwritten. When a recursive DNS server responds to a query, the server caches the results so that it can respond quickly if it receives another query requesting the same information. The period of time the DNS server keeps information in its cache is determined by the TTL value for a resource record. Information in the cache can be overwritten before the TTL expires if updated information about that resource record is received. If a malicious user successfully overwrites information in the cache, then the malicious user might be able to redirect your network traffic to a malicious site. When you use cache locking, the DNS server prohibits cached records from being overwritten for the duration of the TTL value.

You configure cache locking as a percentage value. For example, if the cache locking value is set to 50, the DNS server will not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percentage value is 100. This means that cached entries will not be overwritten for the entire duration of the TTL.

You can configure cache locking by using the **dnscmd** command, as follows:

- Open an elevated command prompt.
- Run the following command:

```
dnscmd /Config /CacheLockingPercent <percent>
```

DNS Security Feature	Description
DNS cache locking	Prevents entries in the cache from being overwritten until a percentage of the TTL has expired.
DNS socket pool	Randomizes the source port for issuing DNS queries. Enabled by default in Windows Server 2012.
DANE	Uses TLSA records that state the CA from which they should expect a certificate
DNSSEC	Enables cryptographically signing DNS records so that client computers can validate responses.

3. Restart the DNS Server service to apply the changes.

Alternatively, you can use the Windows PowerShell **Set-DnsServerCache -LockingPercent** cmdlet to set this value, as shown in this example.

```
Set-DnsServerCache -LockingPercent <value>
```

### DNS socket pool

The DNS socket pool enables a DNS server to use source port randomization when issuing DNS queries. When the DNS service starts, the server chooses a source port from a pool of sockets that are available for issuing queries. Instead of using a predictable source port, the DNS server uses a random port number that it selects from the DNS socket pool. The DNS socket pool makes cache-tampering attacks more difficult because a malicious user must correctly guess both the source port of a DNS query and a random transaction ID to successfully run the attack. The DNS socket pool is enabled by default in Windows Server 2012.

The default size of the DNS socket pool is 2,500. When you configure the DNS socket pool, you can choose a size value from 0 through 10,000. The larger the value, the greater the protection you will have against DNS spoofing attacks. If the DNS server is running Windows Server 2012, you can also configure a DNS socket pool exclusion list.

You can configure the DNS socket pool size by using the **dnscmd** command, as follows:

1. Open an elevated command prompt.
2. Run the following command.

```
dnscmd /Config /SocketPoolSize <value>
```

3. Restart the DNS Server service to apply the changes.

### DANE

The DNS-based authentication of Named Entities (DANE) protocol is a new feature available in the Windows Server 2016 DNS Server role. DANE support is specified in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 6394 and 6698. DANE allows you to use TLSA (Transport Layer Security Authentication) records to provide information to DNS clients that state what Certification Authority (CA) they should expect a certificate from for your domain name. This prevents man-in-the-middle attacks where someone might corrupt the DNS cache to point to their website, and provide a certificate they issued from a different CA.

For example, suppose that your organization hosts a secure website using HTTPS at [www.Fabrikam.com](http://www.Fabrikam.com) by using a certificate from a well-known authority named **CANorth**. Someone might still be able to get a certificate for [www.Fabrikam.com](http://www.Fabrikam.com) from a relatively unknown, different certificate authority named **CAEast**. At that point, an entity hosting the fake [www.Fabrikam.com](http://www.Fabrikam.com) website might be able to corrupt the DNS cache of a client or server to point [www.Fabrikam.com](http://www.Fabrikam.com) over to its fake site. The end user is presented a certificate from CAEast, and might unknowingly acknowledge it and connect to the fake site. With DANE, the client makes a request to the DNS server for [Fabrikam.com](http://Fabrikam.com) asking for the TLSA record, and discovers that the certificate for [www.Fabrikam.com](http://www.Fabrikam.com) was issued by CANorth. If offered a certificate from another CA, the connection is terminated.

### DNSSEC

Domain Name System Security Extensions (DNSSEC) enables a DNS zone and all records in the zone to be signed cryptographically so that client computers can validate the DNS response. DNS is often subject to various attacks, such as spoofing and cache tampering. DNSSEC helps protect against these threats and provides a more secure DNS infrastructure. DNSSEC will be covered in detail in a subsequent topic and demonstration.

You can also configure any Active Directory–integrated zone for secure dynamic update, and then use the ACL to identify which users and groups have authority to modify the zone and records in the zone. Dynamic updates were covered in Lesson 4, "Configuring DNS integration with AD DS."

## Implementing DNSSEC

Intercepting and tampering with an organization's DNS query response is a common attack method. If malicious users can alter responses from DNS servers, or send spoofed responses to point client computers to their own servers, they can gain access to sensitive information. Any service that relies on DNS for the initial connection—such as e-commerce web servers and email servers—are vulnerable. DNSSEC protects clients that are making DNS queries from accepting false DNS responses.

When a DNS server that is hosting a digitally signed zone receives a query, the server returns the digital signatures along with the requested records. A resolver or another server can obtain the public key of the public/private key pair from a trust anchor, and then validate that the responses are authentic and have not been tampered with. To do this, the resolver or server must be configured with a trust anchor for either the signed zone or a parent of the signed zone.

### DNSSEC functions as follows:

- If a zone has been digitally signed, a query response will contain digital signatures
- DNSSEC uses trust anchors, which are special zones that store public keys associated with digital signatures
- Resolvers use trust anchors to retrieve public keys and build trust chains
- DNSSEC requires trust anchors to be configured on all DNS servers participating in DNSSEC
- DNSSEC uses the NRPT, which contains rules that control the requesting client computer behavior for sending queries and handling responses

### Trust anchors

A *trust anchor* is an authoritative entity that is represented by a public key. The TrustAnchors zone stores preconfigured public keys that are associated with a specific zone. In DNS, the trust anchor is the DNSKEY or DS resource record. Client computers use these records to build trust chains. You must configure a trust anchor from the zone on every domain DNS server to validate responses from that signed zone. If the DNS server is a domain controller, Active Directory–integrated zones can distribute the trust anchors.

### NRPT

NRPT contains rules that control the DNS client behavior for sending DNS queries and processing the responses from those queries. For example, a DNSSEC rule prompts the client computer to check for validation of the response for a particular DNS domain suffix. As a best practice, Group Policy is the preferred method of configuring the NRPT. If no NRPT is present, the client computer accepts responses without validating them.

### Deploying DNSSEC

To deploy DNSSEC, follow these steps:

1. Install Windows Server 2016 and assign the DNS Server role to the server.
2. Sign the DNS zone by using the **DNSSEC Configuration Wizard**, which is located in the **DNS Manager** console.
3. Configure trust anchor distribution points.
4. Configure the NRPT on the client computers.

## Assigning the DNS Server role

To assign the DNS Server role, in the **Server Manager Dashboard**, use the **Add Roles and Features Wizard**. You can also add this role when you add the AD DS role. Then, configure the primary zones on the DNS server. After a zone is signed, any new DNS servers in Windows Server 2016 automatically receive the DNSSEC parameters.

## Signing the zone

The following signing options are available:

- **Configure the zone signing parameters.** This option guides you through the steps and enables you to set all values for the key signing key (KSK) and the zone signing key (ZSK).
- **Sign the zone with parameters of an existing zone.** This option enables you to keep the same values and options as another signed zone.
- **Use recommended settings.** This option signs the zone by using the default values.



**Note:** You also can unsign zones by using the DNSSEC management user interface to remove zone signatures.

## Configuring trust anchor distribution points

If the zone is Active Directory integrated, and if all domain controllers are running Windows Server 2016, you can select to distribute the trust anchors to all the servers in the forest. Make this selection with caution, because **Add Roles and Features Wizard** turns on DNSSEC validation. If you enable DNS trust anchors without performing thorough testing, you could cause DNS outages. If trust anchors are required on computers that are not domain members—for example, a DNS server in the perimeter network (also known as *screened subnet*)—you should enable automated key rollover.



**Note:** A *key rollover* is the act of replacing one key pair with another at the end of a key's effective period.

## Configuring NRPT on client computers

The DNS client computer performs DNSSEC validation only on domain names where the NRPT has configured the DNS client computer to do so. A client computer that is running the Windows 7 or later operating system is DNSSEC aware, but it does not perform validation. Instead, it relies on the security-aware DNS server to perform validation on its behalf.

## The DNSSEC Zone Signing Wizard

Windows Server 2016 includes the **DNSSEC Zone Signing Wizard** to simplify the configuration and signing process, and to enable online signing. The wizard allows you to choose the zone signing parameters. If you choose to configure the zone signing settings rather than use parameters from an existing zone or use default values, you can use the wizard to configure settings such as the following:

- KSK options
- ZSK options
- Trust anchor distribution options
- Signing and polling parameters

### ***New resource records***

DNS response validation is achieved by associating a private/public key pair (as generated by the administrator) with a DNS zone, and then defining additional DNS resource records to sign and publish keys. Resource records distribute the public key, while the private key remains on the server. When the client requests validation, DNSSEC adds data to the response that enables the client to authenticate the response.

The following table describes the additional resource records DNSSEC.

Resource record	Purpose
DNSKEY	This record publishes the public key for the zone. It checks the authority of a response against the private key held by the DNS server. These keys require periodic replacement through key rollovers. Windows Server 2016 supports automated key rollovers. Every zone has multiple DNSKEYs that are then broken down to the ZSK and KSK level.
DS (Delegation Signer)	This record is a delegation record that contains the hash of the public key of a child zone. This record is signed by the parent zone's private key. If a child zone of a signed parent is also signed, the DS records from the child must be manually added to the parent so that a chain of trust can be created.
RRSIG (Resource Record Signature)	This record holds a signature for a set of DNS records. It is used to check the authority of a response.
NSEC (Next Secure)	When the DNS response has no data to provide to the client, this record authenticates that the host does not exist.
NSEC3	This record is a hashed version of the NSEC record, which prevents attacks by enumerating the zone.

### ***Other new enhancements***

Other DNSSEC enhancements include:

- Support for DNS dynamic updates in DNSSEC signed zones.
- Automated trust anchor distribution through AD DS.
- Windows PowerShell-based command-line interface for management and scripting.

## **Demonstration: Configuring DNSSEC**

In this demonstration, you will learn how to use the Zone Signing Wizard in the DNS Manager console to configure DNSSEC.

### **Demonstration Steps**

1. On **LON-DC1**, open the **DNS Manager** console.
2. Use the **DNSSEC Zone Signing Wizard** to sign the **Adatum.com** zone.
3. Select the **Customize zone signing parameters** option.
4. Ensure that DNS server **LON-DC1** is the Key Master.



5. Add the **Key Signing Key** by accepting default values for the new key.
6. Add the **Zone Signing Key** by accepting the default values for the new key.
7. Choose to use **NSCE3** with default values.
8. Select the **Enable the distribution of trust anchors for this zone** option.
9. Accept the default values for **signing** and **polling**.
10. Verify that the **DNSKEY** resource records were created in the **Trust Points** zone.
11. Use the **Group Policy Management Console (GPMC)** to configure NRPT. Create a rule that enables DNSSEC for the Adatum.com suffix, and that requires DNS client computers to verify that the name and address data is validated.

## DNS on Nano Server

Nano Server is a new installation option for Windows Server 2016 that is similar to Windows Server in Server Core mode. Run as a virtual machine, the Nano Server uses considerably less hardware resources, including memory, CPU processing, and disk space than a computer running Windows Server Core. However, although it has a significantly smaller hardware footprint, it has no local sign-in capability and supports only 64-bit apps, tools, and agents. Setup is significantly faster, and after installation, the operating system requires far fewer updates. Nano Server is ideal for use as a DNS server. You can install the DNS server role when creating the Nano Server.

To use Nano Server as a DNS Server:

- Install the NanoServer Package
- Create a VHD with the **Microsoft-NanoServer-DNS-Package**
- Import the VHD into Hyper-V as a virtual machine
- Configure networking settings and enable the remote management firewall ports
- Connect remotely to the server running Nano Server by using Windows PowerShell 5.0 on a Windows client or a server
- Run the command **Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role**
- Manage DNS remotely by using the Windows PowerShell 5.0 DNS commands

For Windows Server 2016, Nano Server is distributed on the installation DVD or .iso file, in the **\NanoServer** folder; this folder contains a **.wim** image and a subfolder called **Packages**. You use these package files to add server roles and features to the VHD image, and then boot to that image. You can also find and install these packages with the **NanoServerPackage** provider of the **PackageManagement** PowerShell module.

You do so by running Windows PowerShell as an administrator, and then change directory to the folder where you've placed the Nano Server scripts and then import the **NanoServerImageGenerator** script with the following command:

```
Import-Module NanoServerImageGenerator.psm1 -Verbose
```

You then create a VHD that sets a computer name and includes the Hyper-V guest drivers by running the following command (it will prompt you for an administrator password for the new VHD):

```
New-NanoServerImage -MediaPath <path to root of media> -BasePath .\Base -TargetPath
.\NanoServerVM\NanoServerVM.vhd -ComputerName <computer name> -GuestDrivers -packages
Microsoft-NanoServer-DNS-Package
```

After it installs, you import the VHD into Hyper-V host server as a virtual machine. You can then start the virtual machine and sign in. However, you can perform only the most fundamental management tasks interactively on Nano Server. After you have signed in, the Nano Server Recovery Console displays. This identifies:

- The computer name.
- The workgroup or domain name.
- The installed operating system.
- Local data, the local time, and the time zone.
- The current network configuration.

After you have configured the networking settings and enabled the appropriate remote management firewall ports for inbound communications, you can manage the Nano Server remotely by using Server Manager, Windows PowerShell, or any other management tool by using the **Connect to** option to select the Nano Server.

After this is accomplished, you can use Windows PowerShell remotely to connect to the Nano Server. Before doing so, add the Nano Server to the Trusted Host List. Assuming the Nano Server's IP address is 10.0.1.12, then in Windows PowerShell, run the following command:

```
Set-Item WSMan:\localhost\Client\TrustedHosts "172.16.0.22"
```

Then make the remote connection in PowerShell by running the following commands:

```
$ip = "172.16.0.22"  
$user = "$ip\Administrator"  
Enter-PSSession -ComputerName $ip -Credential $user
```

From the Windows PowerShell session, run the following to install the DNS Server role:

```
Enable-WindowsOptionalFeature -Online -FeatureName DNS-Server-Full-Role
```

After the DNS Server role is installed successfully, you can use the normal Windows PowerShell DNS commands to further configure the DNS Server role on the Nano Server.

## Lab C: Configuring advanced DNS settings

### Scenario

You want to make DNS zone management easier. You want to configure DNS policies in Windows Server 2016, so that users in different geographical areas can connect to a different web server. You must then test and troubleshoot the DNS configuration you have created.

### Objectives

After completing this lab, you will be able to:

- Configure DNS policies.
- Validate the DNS implementation.
- Troubleshoot DNS.

### Lab Setup

Estimated Time: **40 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-INET**, **20741A-EU-RTR**, **20741A-SYD-SVR1**, **20741A-TOR-SVR1**, and **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

You should have the virtual machines **20741A-LON-DC1**, **20741A-EU-RTR**, **20741A-INET**, **20741A-LON-SVR1**, and **20741A-SYD-SVR1** from the previous lab still running.

Start **20741A-TOR-SVR1** and **20741A-LON-CL1**. Sign in to all virtual machines as **Adatum\Administrator** with the password of **Pa\$\$w0rd**.

## Exercise 1: Configuring DNS policies

### Scenario

If you configure the DNS policies correctly, when clients in the Toronto location query for the IP address of **www.adatum.com**, they should receive different name-resolution answers than clients in London location who are mapping to **www.adatum.com**.

The main tasks for this exercise are as follows:

1. Verify DNS name resolution before configuring DNS policies.
2. Configure DNS policies.
3. Check DNS name resolution after configuring DNS policies.

#### ► Task 1: Verify DNS name resolution before configuring DNS policies

1. On **LON-DC1**, in the **DNS Manager** console, create a **CNAME** resource record named **www.adatum.com** that points to **LON-DC1.adatum.com**
2. Switch to **TOR-SVR1**.
3. On **TOR-SVR1**, flush the DNS client cache, and then perform name resolution on **www.adatum.com**. Verify that the name resolves to an IP address of **172.16.0.10**.
4. Switch to **LON-CL1**.

- On **LON-CL1**, flush the DNS client cache, and then perform name resolution on `www.adatum.com`. Verify that the name resolves to an IP address **172.16.0.10**.

### ► Task 2: Configure DNS policies

- On **LON-DC1** in the **Windows PowerShell** console, import the **DnsServer** module.



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

- Run the following cmdlets in Windows PowerShell, pressing 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
```

### ► Task 3: Check DNS name resolution after configuring DNS policies

- Test the results of the previous task by executing the **ipconfig /flushdns** and the **nslookup** command for `www.adatum.com` on **LON-CL1** and then on **TOR-SVR1**. You should get the respective IP addresses depending on the zones that you created previously.

**Results:** After completing this exercise, you should have configured DNS policies, and then tested that the policies work successfully.

## Exercise 2: Validating the DNS implementation

### Scenario

**LON-CL1** is a laptop device, and its end user will be traveling to the Sydney office with it for a few months. You will change its network adapter properties to enable this, and then test to ensure that it works with **SYD-SVR1** as its primary domain controller and DNS server. You will use **Nslookup** and the Windows PowerShell cmdlets to validate the DNS configuration.

The main tasks for this exercise are as follows:

- Connect the client to the appropriate virtual LAN.
- Use DNS tools to confirm proper client configuration.
- Test DNS name resolution to external and internal hosts.

► **Task 1: Connect the client to the appropriate virtual LAN**

1. On the student host computer, in the **20741A-LON-CL1 <hostname> - Virtual Machine Connection** settings, change the network adapter **Virtual switch** from **London\_Network** to **PAC-WAN**.
2. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Open the **Windows PowerShell** console, and then type the following cmdlet, and then press Enter:

```
Get-DnsClientServerAddress
```

4. Note that the DNS server address assigned to London\_Network IPv4 is **172.16.0.10**. This is **LON-DC1**.
5. Use **Network and Sharing Center** to view the properties of the London\_Network.
6. Reconfigure Internet Protocol Version 4 (TCP/IPv4) with the following settings:
  - o IP address: **172.16.19.50**
  - o Default gateway: **172.16.19.1**
  - o Preferred DNS server: **172.16.19.20**.

► **Task 2: Use DNS tools to confirm proper client configuration**

1. On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlet, and press Enter after each line:

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

Note that the DNS Server address assigned to Ethernet IPv4 is **172.16.19.20**. This is **SYD-SVR1**.

2. On **SYD-SVR1**, in the **DNS Manager** console, open the **Adatum.com** zone and note the host record for **LON-CL1**. It should be **172.16.19.50**.
3. If not, perform the following:
  - a. On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
Register-DnsClient
```

- b. Switch to **SYD-SVR1**, and then refresh the **Adatum.com** zone. Note the new address **172.16.19.50** for **LON-CL1**.
4. Clear the DNS server cache on **SYD-SVR1**.

► **Task 3: Test DNS name resolution to external and internal hosts**

1. On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlets, and press Enter after each line:

```
Clear-DnsClientCache
Nslookup mail.contoso.com
```

The reply should be **10.10.0.50**.

- On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
nslookup treyresearch.net
```

You should get a reply of **172.16.19.20**.

**Results:** After completing this exercise, you should have validated the implementation of a global DNS infrastructure successfully.

## Exercise 3: Troubleshooting DNS

### Scenario

A user has reported a networking-related problem to the help desk. You must investigate and attempt a resolution.

Incident Record	
Incident Reference Number: 723101	
Date of Call	May 22
Time of Call	09:01
User	Colin Wilcox (Research Department)
Status	OPEN
<b>Incident Details</b> Colin is unable to access any network resources.	
<b>Additional Information</b> Colin is the only one affected in his department. He cannot access the Research data folder on LON-DC1.	
<b>Plan of Action</b>	
<b>Resolution</b>	

The main tasks for this exercise are as follows:

- Review the scenario.
- Simulate the problem.
- Resolve the problem.

► **Task 1: Review the scenario**

- Read the help desk Incident Record 723101 in the Student Handbook Exercise Scenario.

► **Task 2: Simulate the problem**

1. Switch to **LON-CL1**.
2. In **File Explorer**, connect to `\\LON-DC1\Labfiles\Mod04` and then copy the file named **Scenario.vbs** to the local **Documents** folder.
3. Open a **Command Prompt** window as **Administrator**. Run the `Documents\Scenario.vbs` script.
4. Close all open windows.

► **Task 3: Resolve the problem**

1. Attempt to resolve the problem by using your knowledge of the network architecture and the tools available for troubleshooting the network environment.
2. Update the **Resolution** section of the Incident Record.
3. If you are unable to resolve the problem, escalate it by asking your instructor for additional guidance. To repeat or exit the exercise, revert the virtual machine environment.

**Results:** After completing this exercise, you should have resolved the name resolution problems successfully.

► **Task 4: Prepare for the next module**

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

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

## 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.

### Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Clients sometimes cache invalid DNS records.	
DNS Server performs slowly.	

### Review Questions

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

**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?

**Question:** What benefits do you realize by using forwarders?

### Tools

Name of tool	Used for	Where to find it
DNS Manager console	Manage DNS server role	Administrative Tools
<b>Nslookup</b>	Troubleshoot DNS	Command-line tool
<b>Ipconfig</b>	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: <a href="http://aka.ms/Dbocr6">http://aka.ms/Dbocr6</a>



# Module 5

## Implementing and managing IPAM

### Contents:

Module Overview	5-1
Lesson 1: Overview of IPAM	5-2
Lesson 2: Deploying IPAM	5-7
Lesson 3: Managing IP address spaces by using IPAM	5-16
Lab: Implementing IPAM	5-23
Module Review and Takeaways	5-28

## Module Overview

The complexity of modern networks can make the management of technologies such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) across an enterprise a difficult task. Managing these components and the way they interact is critical to the health and proper functioning of your network. The IP Address Management (IPAM) Server feature helps you to unify the management and visibility of DHCP and DNS across all of the servers in your infrastructure.

This module will introduce you to IPAM functionality, explain how to deploy IPAM, and show you how to manage DNS and DHCP functionality by using IPAM.

### Objectives

After completing this module, you will be able to:

- Describe IPAM functionality and components.
- Deploy IPAM.
- Manage IP address spaces by using IPAM.

## Lesson 1

# Overview of IPAM

IPAM can help you to deploy, manage, and monitor your IP addressing infrastructure. It helps you manage multiple servers that are running the DHCP Server or DNS Server roles. The automatic discovery and agentless operation of IPAM make it easy to deploy, and the integration with Active Directory Domain Services (AD DS), DHCP, DNS, and the Network Policy role service makes it easier to manage your existing infrastructure.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe IPAM.
- Describe IPAM architecture.
- Identify IPAM deployment requirements.
- Describe the considerations for IPAM deployment.
- Describe how to integrate IPAM with System Center Virtual Machine Manager.

### What is IPAM?

Managing the allocation of IP addresses can be a complex task in large networks. IPAM provides a framework for discovering, auditing, and managing the IP address space of your network. It enables you to monitor and administer both DHCP and DNS, and it provides a comprehensive view of where specific IP addresses are allocated.

You can configure IPAM to collect statistics from domain controllers and Network Policy Servers (NPSs). The resultant data is recorded in the Windows Internal Database (WID) or optionally in a Microsoft SQL Server database for Windows Server 2016.

IPAM benefits include:

- IPv4 and IPv6 address space planning and allocation.
- IP address space utilization statistics and trend monitoring.
- Static IP inventory management, lifetime management, and DHCP and DNS record creation and deletion.
- Service and zone monitoring of DNS servers.
- IP address lease and sign-in event tracking.
- Remote administration support by using Remote Server Administration Tools (RSAT).

IPAM consists of four modules that provide the following functionality:

- IPAM discovery
- IP address space management
- Multiserver management and monitoring
- Operational auditing and IP address tracking

IPAM consists of four modules that provide the following functionality:

- **IPAM discovery.** You can configure IPAM to use AD DS for discovering servers that are running Windows Server 2008 and newer and servers that are domain controllers or that have DHCP or DNS installed. You can also add servers manually.
- **IP address space management.** You can use this module to view, monitor, and manage the IP address space. You can dynamically issue or statically assign addresses. You can also track address utilization and detect overlapping DHCP scopes.
- **Multiserver management and monitoring.** You can use this module to manage and monitor multiple DHCP servers. Multiserver management enables tasks to run across multiple servers. For example, you can configure and edit DHCP properties and scopes, and you can track the status of DHCP and scope utilization. You can also monitor multiple DNS servers and monitor the health and status of DNS zones across authoritative DNS servers.
- **Operational auditing and IP address tracking.** You can use the auditing tools to track potential configuration problems. You can collect, manage, and view details of configuration changes from managed DHCP servers. You can also collect address lease tracking from DHCP lease logs and sign-in event information from NPSs and domain controllers.

### What is new in IPAM in Windows Server 2016?

Windows Server 2016 includes several significant new features or improvements to IPAM functionality. This module will explore these features in greater detail later. New features or improvements to IPAM functionality include:

- Enhanced IP address management. Improvements in IPAM capabilities include scenarios such as handling IPv4 /32 and IPv6 /128 subnets and finding free IP address subnets and ranges in an IP address block.
- Enhanced DNS service management. In Windows Server 2012 R2, IPAM could discover DNS zone information and manage the availability of DNS zones. In IPAM for Windows Server 2016, you can now manage DNS resource records, conditional forwarders, and you can perform DNS zone management for domain member Active Directory–integrated and file-backed DNS servers.
- Integrated DNS, DHCP, and IP address management. Improvements in management operations are numerous, including:
  - Visualizing all DNS resource records that pertain to an IP address.
  - Automated inventory of IP addresses based on DNS resource records.
  - IP address lifecycle management for DNS and DHCP operations.
- Multiple AD DS forest support. You can now use IPAM to manage your DNS and DHCP servers across multiple AD DS forests.



**Note:** A two-way trust relationship must exist between the AD DS forest where IPAM is installed and each of the remote AD DS forests.

- Purge utilization data. You can now reduce the IPAM database size by purging older IP address utilization data.
- Windows PowerShell support for role-based access control (RBAC). You can use the Windows PowerShell command-line interface to set access scopes on IPAM objects.



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

## IPAM architecture

IPAM consists of the following main components:

- IPAM server. The IPAM server performs data collection from the managed servers. Additionally, the IPAM server manages the WID or a SQL Server database, and it provides RBAC.
- IPAM client. The IPAM client provides the client computer interface and interacts with the IPAM server, invoking Windows PowerShell cmdlets to perform remote management, DHCP configuration, and DNS monitoring.

IPAM consists of two main components:

- IPAM server
- IPAM client

When deploying IPAM, you can select from three topologies:

- Distributed
- Centralized
- Hybrid

When deploying IPAM, you can select from the following three topologies:

- Distributed. Deploy an IPAM server to each site in your forest. It is common to use the distributed topology when your organization has multiple sites with significant IP addressing infrastructure in place. Servers in each location can help to distribute a workload that might be too large for a single server to handle. You can also use the distributed topology to enable separate locations or business units to administer their own IP addressing management.
- Centralized. Deploy a single IPAM server for your entire forest. A single IPAM server provides centralized control and visibility for IP addressing tasks. You can view your entire IP addressing infrastructure from a single console when you are using the centralized topology.
- Hybrid. In addition to the centralized IPAM server, you also can deploy an IPAM server to each site. The hybrid topology combines the load sharing and shared administration benefits of the distributed topology with the unified management and visibility of the centralized topology. You typically implement the hybrid topology in large organizations that need to distribute the IPAM load, but still want central administration.

## IPAM deployment requirements

To ensure a successful IPAM implementation, your organization's network infrastructure must meet several prerequisites:

- The IPAM server must be a domain member, but it cannot be a domain controller.
- The IPAM server should be a single-purpose server. Do not install other network roles such as DHCP or DNS on the same server. If IPAM installs on a DHCP server, IPAM will not be able to detect other DHCP servers on the network.
- To manage the IPv6 address space, you must enable IPv6 on the IPAM server.
- Sign in to the IPAM server with a domain account and not a local account.
- For IPAM's IP address tracking and auditing feature to work, you must enable logging of account sign-in events on domain controllers and NPSs.

To ensure a successful IPAM implementation, an organization's network infrastructure must meet the following prerequisites:

- The IPAM server must be a domain member
- The IPAM server should be a single-purpose server
- To manage the IPv6 address space, enable IPv6 on the IPAM server
- Sign in to the IPAM server with a domain account
- Belong to the correct IPAM local security group on the IPAM server
- Enable logging of account sign-in events for IPAM's IP address tracking and auditing feature
- Meet software and hardware requirements

The server on which you intend to deploy IPAM must meet the following hardware and software requirements:

- 2.0 gigahertz (GHz) dual-core processor or faster
- Windows Server 2012 operating system or later
- 4 or more gigabytes (GB) of RAM
- 80 GB of free hard disk space

## Considerations for IPAM deployment

When designing an IPAM deployment, consider the following factors:

- By using IPAM, you can manage multiple AD DS forests if the required trusts exist between those forests.
- IPAM servers do not communicate with one another or share database information. If you deploy multiple IPAM servers, you must customize each server's scope of discovery.
- You can define the scope of discovery to a subset of domains in the forest.
- A single IPAM server can support up to:
  - 150 DHCP servers and 500 DNS servers.
  - 6,000 DHCP scopes and 150 DNS zones.
- IPAM stores three years of forensics data—IP address leases, host media access control (MAC) addresses, user sign-in and sign-out information—for 100,000 users in the database.
- IPAM supports WID. Additionally, IPAM on Windows Server 2016 supports SQL Server for storing the IPAM database.

When designing an IPAM deployment, consider the following factors:

- You can manage multiple AD DS forests if the required trusts exist between those forests
- IPAM servers do not communicate with one another
- You can define the scope of discovery to a subset of domains in the forest
- A single IPAM server can support many DHCP servers and DNS zones
- IPAM stores three years of forensics data
- IPAM supports WID or Microsoft SQL Server databases
- IP address utilization trends are provided only for IPv4
- IP address reclamation support is provided only for IPv4
- IPAM does not check for IP address consistency with routers and switches

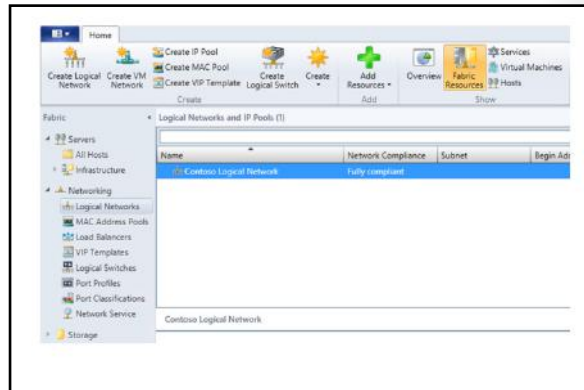


**Note:** If you use a SQL Server database for IPAM, you have the option to use a database on a separate server. However, if you use SQL Server to host your IPAM database, then that must be the only SQL instance running on that SQL Server.

- IP address utilization trends are provided only for IPv4.
- IP address reclamation support is provided only for IPv4.
- IPAM does not check for IP address consistency with routers and switches.

## Integrating IPAM with Virtual Machine Manager


Windows Server 2012 R2 introduced the ability to integrate IPAM with Virtual Machine Manager. You can integrate IPAM with Virtual Machine Manager by performing the following steps:



1. On the IPAM server:
  - a. Configure an account that Virtual Machine Manager uses to communicate with IPAM.
  - b. Grant the account membership to the IPAM ASM Administrator role.
2. In the Virtual Machine Manager console, add and configure the **Microsoft Windows Server IP Address Management** network service in Virtual Machine Manager by performing the following steps:
  - a. In the **Fabric** workspace, add a network service named **IPAM**.
  - b. On the **Manufacturer and Model** page, select **Microsoft and Microsoft Windows Server IP Address Management**.
  - c. Configure the service to run in the context of the user account that you created in step 1.
  - d. Specify the fully qualified domain name (FQDN) of the Internet Message Access Protocol (IMAP) server.
  - e. Verify that the configuration provider is **Microsoft IP Address Management Provider**.

After you have configured the integration of IPAM and Virtual Machine Manager, when using the IPAM network service with Virtual Machine Manager:

- The virtualized IP address space in IPAM automatically updates when you make changes to logical networks in Virtual Machine Manager.
- When you create logical networks in IPAM, they are added to Virtual Machine Manager.

 **Additional Reading:** For more information on how to configure IPAM Virtual Machine Manager integration, refer to: <http://aka.ms/o3vpc>

Verify the correctness of the statement by placing a mark in the column to the right.

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

## Lesson 2

# Deploying IPAM

IPAM has automatic discovery functionality that makes the initial identification of servers that are manageable by IPAM a simple process. However, you must complete several configuration tasks, and you should assess the management considerations before implementing IPAM in your environment. In this lesson, you will learn the process for implementing IPAM and the configuration options that you should consider for implementing and administrating IPAM functionality.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the process of implementing IPAM.
- Install and provision an IPAM server.
- Explain the administration options in IPAM.
- Administer an IPAM server.
- Explain how to configure IPAM options.
- Explain how to manage DNS by using IPAM.
- Manage DNS zones with IPAM.
- Explain how to configure DHCP servers by using IPAM.
- Manage DHCP scopes with IPAM.

### Process of implementing IPAM

Implementing IPAM involves several important steps:

1. Review IPAM functionality and align with implementation goals.
2. Confirm that system and environment requirements are met.
3. Develop a staged deployment plan.
4. Deploy IPAM servers.
5. Deploy IPAM clients.
6. Assign IPAM administration roles.
7. Use IPAM for IP infrastructure management.

Perform the following steps to implement IPAM:

1. Install the IPAM Server feature
2. Provision IPAM servers
3. Configure and run server discovery
4. Choose and manage discovered servers

### Deploying IPAM servers

Deploying IPAM servers begins with the installation of the IPAM Server feature. Several different configuration models exist for IPAM server deployments:

- Distributed
- Centralized
- Hybrid

After deciding the IPAM topology to use, you can deploy IPAM servers by performing the following steps:

1. Install the IPAM Server feature. You can install it by using **Server Manager** or by using the following Windows PowerShell command:

```
Install-WindowsFeature IPAM -IncludeManagementTools
```

2. Provision IPAM servers. After installing the feature, you must provision each IPAM server in order to create the permissions, file shares, and settings on the managed servers. You can perform this manually or by deploying a Group Policy Object (GPO).

Using a GPO offers several advantages over manual provisioning:

- GPO-applied settings are less prone to human configuration error.
  - GPO settings apply automatically to servers when they are assigned a status of **Managed**.
  - Settings are removed easily by disabling or deleting the GPO link.
3. Configure and run server discovery. You must configure the scope of discovery for servers that you are going to manage. Discovery scope is determined by selecting the domain or domains on which the IPAM server will run discovery. You can also manually add a server in the IPAM management console by specifying the FQDN of the server that you want to manage.
  4. Choose and manage discovered servers. After discovery completes and you have manually added any servers that were not discovered, you must choose the servers that you want to manage by editing the server properties in the IPAM console and changing **Manageability Status** to **Managed**. After setting the management permission for a server, you will see a status indicator in the IPAM server inventory displaying **IPAM Access Unblocked**.

### Deploying IPAM clients

You use the IPAM client to configure and manage IPAM servers. In most cases, you install the IPAM client during installation of the IPAM Server feature, and you perform management tasks on the same computer that is running IPAM Server. However, there might be specific instances where you must install the IPAM client on a server or a workstation in your environment to manage an IPAM Server remotely. IPAM installation varies based on the operating system:

- Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. You can install the IPAM client by installing the **Windows Feature** under **Remote Server Administration Tools \Feature Administration Tools\IP Address Management (IPAM) Client**.
- Windows 8, Windows 8.1, and Windows 10. The IPAM client installs automatically when you install RSAT.



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

### Demonstration: Installing and provisioning the IPAM role

In this demonstration, you will learn how to:

- Install IPAM.
- Provision IPAM.



## Demonstration Steps

### Install IPAM

- On **LON-SVR2**, in **Server Manager**, add the IPAM Server feature and all required supporting features.

### Configure IPAM

1. In the **IPAM Overview** pane, connect to and provision the IPAM server.
2. Enter **IPAM** as the GPO name prefix, and then provision IPAM.
3. In the **IPAM Overview** pane, configure server discovery for the Adatum.com forest and then the Adatum domain.
4. In the **IPAM Overview** pane, start the server discovery process.
5. In the **IPAM Overview** pane, add the servers to manage.
6. Verify that IPAM access is currently blocked.
7. Use Windows PowerShell to grant the IPAM server permission to manage **LON-DC1** by using the following command:

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

8. Set the manageability status to **Managed** for both servers.
9. Switch to **LON-DC1**, and then force the update of Group Policy.
10. Switch back to **LON-SVR2**, and then refresh the **IPv4** view.
11. In the **IPAM Overview** pane, retrieve data from the managed server.

## IPAM administration

Configuring administration for IPAM can be a complex task depending on how your IPAM infrastructure is deployed and who is managing the infrastructure. An IPAM server can perform management for multiple domains, or you can limit an IPAM server to specific roles or limit the servers that are managed.

RBAC provides the ability to customize roles, access scopes, and access policies. Thus, you have the ability to define and establish fine-grained control for users and groups, thereby enabling them to perform a specific set of administrative operations on specific objects that IPAM manages. You implement role-based management in IPAM by using:

- You implement role-based management in IPAM by using:
  - Role-based security groups
  - Access scopes
  - Access policies
- IPAM includes several built-in roles
- You can also create and configure custom roles

- Roles. A role is a collection of IPAM operations. You can associate a role with a user or group in Windows by using an access policy. Eight built-in administrator roles are available for convenience, but you can also create customized roles to meet your business requirements. You can create and edit roles from the **Access Control** node in the IPAM management console.

- Access scopes. An access scope determines the objects to which a user has access. You can use access scopes to define administrative domains in IPAM. For example, you might create access scopes based on geographical location. By default, IPAM includes an access scope named *Global*. All other access scopes are subsets of the Global access scope. Users or groups that you assign to the Global access scope have access to all objects in IPAM that their assigned role permits. You can create and edit access scopes from the **Access Control** node in the IPAM management console.
- Access policies. An access policy combines a role with an access scope to assign permissions to a user or group. For example, you might define an access policy for a user with a role named *IP Block Admin* and an access scope named *Global\Asia*. Therefore, this user will have permission to edit and delete IP address blocks that are associated with the *Asia* access scope. This user will not have permission to edit or delete any other IP address blocks in IPAM. You can create and edit access policies from the **Access Control** node in the IPAM management console.

IPAM has several built-in role-based security groups that you can use for managing your IPAM infrastructure, as shown in the following table.

Group name	Description
IPAM DNS Administrator	Members of this group can manage DNS servers and their associated DNS zones and resource records.
IPAM MSM Administrator	Members of this group can manage DHCP servers, scopes, policies, and DNS servers and associated zones and records.
IPAM ASM Administrator	Members of this group can perform IP address space tasks, in addition to common IPAM management tasks.
IP Address Record Administrator	Members of this group can manage IP addresses, including unallocated addresses, and members can create and delete IP address instances.
IPAM Administrator	Members of this group have privileges to view all IPAM data and to perform all IPAM tasks.
IPAM DHCP Administrator	Completely manages DHCP servers.
IPAM DHCP Reservations Administrator	Manages DHCP reservations.
IPAM DHCP Scope Administrator	Manages DHCP scopes.
DNS Record Administrator	Manages DNS resource records.

## Demonstration: Administering IPAM

In this demonstration, you will learn how to:

- Add a custom role group.
- Add a custom scope.
- Add an IPAM access policy.
- Set the access scope.

## Demonstration Steps

### Add a custom role group

1. On **LON-SVR2**, under **ACCESS CONTROL** in the **IPAM navigation** pane, view the available built-in roles.
2. Add a new role named **A Datum DHCP and DNS Management role**.
3. Add the following operations to this role:
  - DHCP server operations
  - DNS zone operations
  - DNS server operations

### Add a custom scope

- Add a new access scope named **London** as a child of **Global**.

### Add an IPAM access policy

- Add a new access policy with the following properties:
  - User Settings: the **IT** group from the **Adatum.com** domain.
  - Role: **A Datum DHCP and DNS Management role**
  - Access scope: **London**

### Set the access scope

1. In the navigation pane, select **DNS and DHCP Servers**.
2. In the **details** pane, for each service listed on **LON-DC1**, right-click the service, and then click **Set Access Scope**.
3. Disable the inherit access scope from the parent, and then set the access scope to **London**.

## Configuring IPAM options

You can configure IPAM to suit your environment and provide the level of manageability that you require. In most cases, you can configure IPAM by using GPOs that deployed during the initial provisioning process. When you provision an IPAM server, it creates three GPOs in any of the domains that you select, and it links those GPOs to the root of the domain in the Group Policy Management Console (GPMC). When you select Group Policy provisioning, you are also asked to provide a prefix for the GPOs so that they can be easily identified in the GPMC. The GPOs created are:

- You can configure IPAM by using the following GPOs:
  - <Prefix>\_DHCP
  - <Prefix>\_DNS
  - <Prefix>\_DC\_NPS
- To finalize the IPAM configuration, run the **Invoke-IpamGpoProvisioning** cmdlet

- <Prefix>\_DHCP. This GPO is used to apply 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 is used to apply 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 is used to apply 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).

After applying the GPO objects and discovering DHCP and DNS servers in your environment, you must use the following command to create the GPOs in the preceding list:

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

In this example, the command creates the GPOs with a prefix of "IPAM" in Adatum.com for the IPAM server LON-SVR2, under the security context of the domain Administrator account.

## How to manage DNS by using IPAM

IPAM enables you to manage DNS servers and zones for all servers that the IPAM server manages. During discovery, IPAM discovers all authoritative DNS servers in the domains that you specify. You can use IPAM to perform the following DNS management tasks:

- View DNS servers and zones. You can view all managed DNS servers, in addition to the forward lookup zones and the reverse lookup zones on those DNS servers. Zone status and health is available for forward lookup zones, but not for reverse lookup zones.
- Create new zones. To create DNS zones, in the navigation pane, click the **DNS and DHCP Servers** node. Right-click the DNS server to which you want to add a zone, and then click **Create DNS zone**.
- Open the DNS console for any server that IPAM manages. You can open the Microsoft Management Console (MMC) for DNS by right-clicking a server on the **DNS and DHCP servers** page, and then selecting **Launch MMC**.

You can perform the following DNS management tasks in IPAM:

- View DNS servers and zones
- Create new zones
- Open the DNS console for any server that IPAM manages
- Create DNS records
- Manage conditional forwarders

- Create DNS records. You can create DNS records for any zone that IPAM manages. To do this, perform the following steps:
  - a. In the **IPAM** navigation pane, select **DNS Zones**. Select the appropriate zone, for example, Adatum.com.
  - b. Right-click the zone, and then click **Add DNS resource record**.
  - c. Verify that the correct DNS zone name and DNS server name display in the list, and then add a new DNS resource record. For example, select **Resource record type A**, and then add the required information: name, FQDN, and IP address.
- Manage conditional forwarders. To add a conditional forwarder, in the navigation pane, click the **DNS and DHCP Servers** node. Right-click the DNS server to which you want to add a zone, and then click **Create DNS conditional forwarder**. To manage a conditional forwarder after you create it, in the navigation pane, under **DNS Zones**, click **Conditional Forwarders**. You can then manage the conditional forwarding settings in the details pane.

## Demonstration: Managing DNS with IPAM

In this demonstration, you will learn how to:

- Add a conditional forwarder.
- Create a DNS zone.
- Add a DNS record.

### Demonstration Steps

#### Add a conditional forwarder

1. 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. Add a new record with the following properties:
  - DNS domain: **TreyResearch.net**
  - FQDN or IP address: **172.16.0.11**

#### Create a DNS zone

- On the **DNS and DHCP Server** tab, create a new DNS zone named **Contoso.com**.

#### Add a DNS record

1. On the **DNS Zones** tab, add a DNS resource record to **Contoso.com** with the following properties:
  - Resource record type: **A**
  - Name: **Contoso1**
  - IP address: **172.32.0.99**
2. On the **DNS and DHCP Servers** tab, select the **Launch MMC** option.
3. In the **DNS Manager** dialog box, verify the presence of the **Contoso.com** zone and the record that you created.
4. Verify that a conditional forwarder exists for **TreyResearch.net**.
5. Close the **DNS Manager** console.

## How to configure DHCP servers by using IPAM

You can configure DHCP servers and DHCP scope information by using the IPAM administration interface. IPAM enables you to configure multiple DHCP servers and to use functionality such as DHCP failover so that the servers work together in your DHCP implementation.

### Configuring DHCP servers

You typically perform DHCP configuration for individual servers from the **DNS and DHCP Servers** page. You can perform several configuration tasks on a DHCP server from within the IPAM administration console:

- View DHCP scope information across all servers.
- Edit DHCP server properties. You can edit server properties such as DHCP audit logging, DNS dynamic update configuration, and MAC address filtering allow and deny lists.
- Edit DHCP server options. You can configure and create DHCP server options based on vendor or user classes.
- Configure DHCP vendor or user classes. You can view and modify user and vendor classes.
- Configure DHCP policy. You can edit DHCP policy properties and conditions.
- Import DHCP policy. You can import DHCP policies by using files that other DHCP servers export.
- Add DHCP MAC address filters. You can add DHCP MAC address filters to allow or deny DHCP address assignments based on MAC address.
- Launch the DHCP MMC. You can open the MMC for the selected server.
- Activate and deactivate DHCP policies. You can control the implementation of DHCP policies.
- Replicate DHCP servers. This option replicates the configuration of failover scopes on a server to failover partner servers.

### Configuring DHCP scopes

You can configure DHCP scope details in IPAM by performing the following tasks:

- Edit DHCP scope properties.
- Duplicate a DHCP scope. Use a DHCP scope as a template for creating a new scope on the same server or another server.
- Create a DHCP reservation.
- Add to a DHCP superscope.
- Configure a DHCP failover.
- Import a DHCP policy.
- Activate and deactivate DHCP scopes.
- Activate and deactivate DHCP policies for the selected scope.
- Replicate a DHCP scope.
- Remove a DHCP failover configuration.

- You can perform all DHCP configuration tasks for a DHCP server in the IPAM administration interface
- You configure DHCP servers and scopes

- Remove a scope from a DHCP superscope.

## Demonstration: Managing DHCP scopes with IPAM

In this demonstration, you will learn how to add a DHCP scope.

### Demonstration Steps

1. 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. Create a new DHCP scope with the following properties:
  - Scope name: **Contoso**
  - Start IP address: **172.32.0.100**
  - End IP address: **172.32.0.200**
  - Activate scope on creation: **No**
  - Option: **006 DNS Servers**
    - Server name: **LON-DC1.Adatum.com**
3. On the **DNS and DHCP Servers** tab, select **Launch MMC**.
4. In the **DHCP console**, verify the presence of scope and the scope options that you created.
5. Close the **DHCP console**.

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

## Lesson 3

# Managing IP address spaces by using IPAM

IP address management is the primary function of IPAM. By using IPAM, you can maintain an accurate inventory of IP addresses that are used in your environment, including those that DHCP servers do not manage. IPAM provides configuration and import functionality for IP address management. It also provides reporting and monitoring capabilities.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to use IPAM for managing IP addressing.
- Explain how to add address spaces to IPAM.
- Explain how to import and update address spaces.
- Explain how to find, allocate, and reclaim IP addresses.
- Explain how to maintain IP address inventory in IPAM.
- Manage IP addressing with IPAM.
- Describe how to implement IPAM monitoring and reporting.

### Using IPAM to manage IP addressing

You can use IPAM to manage, track, audit, and report your organization's IPv4 and IPv6 address spaces. The IPAM IP address space console provides you with IP address utilization statistics and historical trend data so that you can make informed planning decisions for dynamic, static, and virtual address spaces. IPAM periodic tasks automatically discover the address spaces and utilization data as configured on the DHCP servers that IPAM manages. You can also import IP address information from comma-separated value (CSV) files.

- You can view and manage an IP address space by using the following views:
  - IP address blocks
  - IP address ranges
  - IP addresses
  - IP address inventory
  - IP address range groups
- You can monitor the IP address space by using the following views:
  - DNS and DHCP servers
  - DHCP scopes
  - DNS zone monitoring
  - Server groups

IPAM also enables you to detect overlapping IP address ranges that are defined on different DHCP servers, to find free IP addresses within a range, to create DHCP reservations, and to create DNS records.

### Viewing and managing IP addressing

The IPAM administration console provides a number of ways to filter the view of the IP address space. You can customize how you view and manage the IP address space by using any of the following views:

- IP address blocks
- IP address ranges
- IP addresses
- IP address inventory
- IP address range groups



### ***IP address blocks***

IP address blocks are the highest-level entities within an IP address space organization. An *IP address block* is an IP subnet that is marked by a start IP address and an end IP address. You can use IP address blocks to create and allocate IP address ranges to DHCP. You can add, import, edit, and delete IP address blocks. IPAM maps IP address ranges to the appropriate IP address block automatically based on the boundaries of the range.

### ***IP address ranges***

IP address ranges are the next hierarchical level of IP address space entities after IP address blocks. An *IP address range* is an IP subnet that is marked by a start IP address and an end IP address. IP address ranges typically correspond to a DHCP scope, a static IPv4 or IPv6 address range, or to an address pool that is used to assign addresses to hosts.

### ***IP addresses***

IP addresses are the addresses that make up the IP address range. IPAM enables end-to-end lifecycle management of IPv4 and IPv6 addresses, including record syncing with DHCP and DNS servers. IPAM maps an address to the appropriate range automatically based on the starting and ending address of the IP address range.

### ***IP address inventory***

In the **IP Address Inventory** view, you can see a list of all IP addresses in the enterprise along with their device names and types. IP address inventory is a logical group within the IP addresses view. You can use this group to customize the way the address space displays for managing and tracking IP usage.

### ***IP address range groups***

IPAM enables you to organize IP address ranges into logical groups. For example, you might organize IP address ranges geographically or by business division. You define logical groups by selecting the grouping criteria from built-in or user-defined custom fields.

### **Monitoring DHCP and DNS servers**

IPAM enables automated, periodic service monitoring of DHCP and DNS servers across a single forest or across multiple forests. In the IPAM console, monitoring and management of DHCP and DNS servers is organized into the views that the following table lists.

View	Description
DNS and DHCP servers	By default, managed DHCP and DNS servers are arranged by their network interface in /32 subnets for IPv4 and /128 subnets for IPv6. You can select the view to see only DHCP scope properties, only DNS server properties, or both.
DHCP scopes	This view enables scope utilization monitoring. Utilization statistics are automatically collected periodically from a managed DHCP server. You can track important scope properties such as Name, ID, Prefix Length, and Status.
DNS zone monitoring	You enable zone monitoring for forward lookup zones. Zone status is based on events that IPAM collects. The status of each zone is summarized.
Server groups	You can organize managed DHCP and DNS servers into logical groups. For example, you might organize servers by business unit or geography. You define groups by selecting the grouping criteria from the built-in fields or user-defined fields.



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

## Adding address spaces to IPAM

Using IPAM greatly improves the burden of managing IP addressing in large or complex environments. IPAM automatically registers IP address ranges based on the configured scopes on managed DHCP servers. IPAM does not automatically add any IP ranges that are not within DHCP scopes or that reside on non-Microsoft DHCP servers.

To manage these address ranges, you can manually add the address space in IPAM:

- To add a new IP address block, range, or address, in the lower navigation pane, click **IPv4** or **IPv6**, click **Tasks**, and then click **Add IP Address [Range/Block]**.
- To edit an existing address space, right-click the unit of address space (address, range, or block), and then click **Edit IP Address [Range/Block]**.

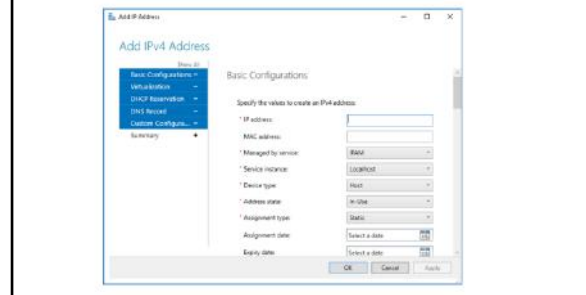
If you select **No** next to **Automatically assign address values when creating a new address block or range**, then you must manually provide the start IP address and end IP address. This allows you to work with an IP address space that does not always start and end on network boundaries.

You cannot specify a **Managed by service** value of MS DHCP for IP address ranges that the IPAM administrative interface manually adds. The MS DHCP value is reserved for DHCP scopes that are discovered on the network. Discovered DHCP scopes add to IP address ranges automatically. Most values for these ranges automatically populate based on discovery data, and you cannot modify them.

## Importing and updating address spaces

You can use IPAM to import and update IP address space information from a CSV file. When importing address space data from a file, the required fields are identical to those that are required when adding IP address data in IPAM by using the IPAM administrative interface. You must include field names on line 1 of the CSV file, followed by corresponding data, with each entry on a separate line. You can use custom field names, but you must define them in the IPAM administrative interface prior to import. You can specify fields in any order, as long as the data values are also in the same order. Data and field names are not case sensitive, and they can be enclosed in quotes and include spaces.

You can add address spaces to IPAM to provide comprehensive management of IP addressing



- You can import the following into IPAM by using CSV files:
  - IP addresses
  - IP address ranges
  - IP address blocks
- The mandatory fields for importing are:
  - IP addresses. IP address, managed by service, service instance, device type, IP address state, and assignment type
  - IP address range. Network, start IP address, end IP address, managed by service, service instance, and assignment type
  - IP address block. Network, start IP address, end IP address, and RIR

For example, you can use the following data to import two IP addresses into the IPAM database, assuming that dhcp1.adatum.com is a valid service instance on the network:

```
IP address,managed by service,service instance,device type,ip address state,assignment
type
172.16.0.25,ms dhcp,dhcp1.adatum.com,host,in-use,static
172.16.0.26,ms dhcp,dhcp1.adatum.com,host,in-use,static
```

For IP address ranges and blocks, the network ID and network prefix length combine in a single field named *Network*. For example, you can use the following data to import an IP address block of 65.52.0.0/14. This example includes optional spaces between the field names and data values:

```
Network, start IP address, end IP address, RIR
65.52.0.0/14, 65.52.0.0, 65.52.255.255, ARIN
```

Because 65.52.0.0/14 is a public IP address space, the regional Internet registry (RIR) field is required. Note that blocks begin on a network ID and end on a broadcast address (.0 and .255), unlike IP address ranges, which start and end on usable IP addresses (.1 and .254).

If a required field is missing or contains unusable data, an error report is created in the current user's **Documents** folder automatically. For example, the following data will generate an error if a **Managed by service** value of MS DHCP is specified. This value is reserved for DHCP scopes on managed DHCP servers. To avoid this error, use a value of IPAM for **Managed by service**. This example includes optional quotes around the field names and data values:

```
"Network", "Start IP address", "End IP address", "Managed by service", "Service instance",
"Assignment Type"
"192.168.100.0/24", "192.168.100.1", "192.168.100.254", "IPAM", "router", "dynamic"
```

The following table lists the mandatory fields for importing.

IP addresses	IP address ranges	IP address blocks
<ul style="list-style-type: none"> <li>• IP address</li> <li>• Managed by service</li> <li>• Service instance</li> <li>• Device type</li> <li>• IP address state</li> <li>• Assignment type</li> </ul>	<ul style="list-style-type: none"> <li>• Network</li> <li>• Start IP address</li> <li>• End IP address</li> <li>• Managed by service</li> <li>• Service instance</li> <li>• Assignment type</li> </ul>	<ul style="list-style-type: none"> <li>• Network</li> <li>• Start IP address</li> <li>• End IP address</li> <li>• RIR</li> </ul>

## Finding, allocating, and reclaiming IP addresses

IPAM enables you to assign IP addresses from managed servers based on availability. When finding, allocating, or reclaiming an IP address, the address is considered to be available if:

- The IP address does not currently exist in the IPAM database.
- The IP address is not reserved on the managed DHCP server that is providing the IP address range.
- The IP address is not excluded on the managed DHCP server that is providing the IP address range.
- The IP address does not respond to a ping request from the IPAM server.
- A DNS pointer (PTR) resource record is not found for the IP address.

You can use IPAM to find, allocate, and reclaim an IP address if:

- The IP address does not exist in IPAM
- The IP address is not reserved in the range
- The IP address is not excluded from the range
- The IP address does not respond to a ping request
- A DNS pointer (PTR) resource is not found for the IP address

### Finding and allocating IP addresses

You can find available IP addresses within an IP address range by right-clicking the IP address range and then clicking **Find and Allocate Available IP Address**. When IPAM searches for available addresses, it follows this process:

1. The search begins with the first address in the range that is unassigned in IPAM.
2. If the address range belongs to a managed DHCP scope, the search automatically ignores IP reservations and exclusions.
3. When a PING and DNS query have completed and no response is received from the PING and DNS query, the address is added to the list.

### Reclaiming IP addresses

When you reclaim IP addresses in IPAM, they delete from the IPAM database. IP address reclamation does not affect DHCP reservations and DNS records.



**Note:** If you also want to delete DHCP reservations and DNS records with the IPAM administrative interface, in the IP addresses view, select one or more IP addresses, right-click, and then click **Delete DHCP Reservation**, **Delete DNS Host Record**, or **Delete DNS PTR Record**.

- To reclaim IP addresses, right-click one or more IP address ranges, and then click **Reclaim IP Addresses**.

## Maintaining IP address inventory in IPAM

You can view IP addresses in the IPAM database by clicking **IP Address Blocks** or by clicking **IP Address Inventory**. If you click **IP Address Blocks**, you must also choose IP addresses that are next to the **current view**. By default, IPv4 addresses display. Select IPv6 in the lower navigation pane to switch to the IPv6 addresses view.

If you click **IP Address Inventory**, only IP addresses display—ranges and blocks do not display. You also must select either IPv4 or IPv6 addresses in the lower navigation pane.

The IP address blocks view organizes IP addresses based on whether they map to a public or private IP address block. The IP address inventory view organizes IP addresses by device type, including custom IP address inventory groups.



## Demonstration: Managing IP addressing with IPAM

In this demonstration, you will learn how to:

- Add an address block in IPAM.
- Create an IP address reservation.

### Demonstration Steps

#### Add an address block in IPAM

1. On **LON-SVR2**, in **Server Manager**, add the following IP address block:
  - 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**
2. Change the **current view** to **IP Address Blocks** to view the newly created block.

#### Create an IP address reservation

1. In **Server Manager**, on the **IP Address Blocks** page, switch the view to **IP Address Ranges**.
2. Edit the IP address range for the **172.16.0.0/16** network.
3. Add a reservation for the **172.16.0.170** IP address.

## Monitoring and reporting in IPAM

You can use the IPAM address space management feature to view, monitor, and manage the IP address space on a network. The address space management feature supports IPv4 public and private addresses, in addition to IPv6 global and unicast addresses.

### Utilization monitoring

IPAM maintains utilization data for:

- IP address ranges
- IP address blocks
- IP range groups

You can configure thresholds for the utilized percentage of the IP address space and then use those thresholds to determine under-utilization or over-utilization.

You can perform utilization trend building and reporting for IPv4 address ranges, blocks, and range groups.

### Monitoring DHCP and DNS servers

Using IPAM, you can monitor DHCP and DNS servers from any physical location in an enterprise. One of the primary benefits of IPAM is its ability to simultaneously manage multiple DHCP servers or DHCP scopes that are spread across one or more DHCP servers.

You can use the IPAM monitoring view to check the status and health of selected sets of Windows Server DNS and DHCP servers from a single IPAM administrative interface. The IPAM monitoring view displays the basic health of servers and recent configuration events that occurred on these servers. You can also use the monitoring view to organize managed servers into logical server groups.

For DHCP servers, you can use the server view to track various server settings, server options, the number of scopes, and the number of active leases that are configured on a server. For DNS servers, you can use this view to track all zones that are configured on the server, along with details about the zone type. You can also use the view to see the total number of zones that are configured on the server and the overall zone health status as derived from the zone status of individual forward lookup zones on the server.

### Managing DNS servers

You can start the **DNS Manager** console for any managed DNS server from a central console in the IPAM server, and you can retrieve server data from the selected set of servers. The DNS zone monitoring view displays all the forward lookup and reverse lookup zones on all the DNS servers that IPAM is currently managing. For the forward lookup zones, IPAM also displays all the servers that are hosting the zone, the aggregate health of the zone across all of these servers, and the zone properties.

### The event catalog

The IPAM event catalog provides a centralized repository for auditing all configuration changes that occur on managed DHCP servers from a single IPAM management console. The IPAM configuration events console gathers all of the configuration events. You can use these configuration event catalogs to view, query, and generate reports about consolidated configuration changes, along with details that are specific to each record.

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

With IPAM, you can:

- Monitor IP address space utilization
- Monitor DNS and DHCP health
- Configure many DHCP properties and values from the IPAM console
- Use the event catalog to view a centralized repository for all configuration changes

# Lab: Implementing IPAM

## Scenario

With the distribution of network services in multiple locations, it is becoming increasingly complex to manage the networking environment at A. Datum Corporation. The IT management at A. Datum has decided to deploy IPAM and use it to manage the IP address configuration centrally in the organization.

## Objectives

After completing this lab, you will be able to:

- Install the IPAM Server feature.
- Provision IPAM to manage servers.
- Manage IP address spaces by using IPAM.

## Lab Setup

Estimated Time: 90 minutes

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, and **20741A-EU-RTR**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-EU-RTR**.
6. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-TOR-SVR1**, and **20741A-SYD-SVR1**.

## Exercise 1: Installing the IPAM Server feature

### Scenario

You will implement IPAM for Adatum.com by using **LON-SVR2** as your IPAM server. Your task is to install the IPAM Server feature on **LON-SVR2**.

The main tasks for this exercise are as follows:

1. Prepare the lab environment.
2. Install the IPAM Server feature on **LON-SVR2**.

### ► Task 1: Prepare the lab environment



**Note:** Running the following scripts will return several warnings regarding Windows updates. You can ignore these warnings.

1. On **LON-SVR1**, open a Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\LON-SVR1_Mod05_Setup.ps1
```

2. On **TOR-SVR1**, open a Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\TOR-SVR1_Mod05_Setup.ps1
```

3. On **SYD-SVR1**, open a Windows PowerShell (Admin) command prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\SYD-SVR1_Mod05_Setup.ps1
```

**SYD-SVR1** will restart when the script completes. After it restarts, sign in as **Adatum\Administrator** with the password of **Pa\$\$w0rd**.

### ► Task 2: Install the IPAM Server feature on LON-SVR2

1. If necessary, sign in to **LON-SVR2** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Start **Server Manager**, and then use the **Add Roles and Features Wizard** to add the IPAM Server feature and all required supporting features.

**Results:** After completing this exercise, you should have successfully installed the IPAM Server feature.

## Exercise 2: Provisioning the IPAM Server

### Scenario

Now, you must configure IPAM discovery for servers in the Adatum.com domain. You will use IPAM to manage the following servers:

- **LON-DC1:** DC, DHCP, DNS
- **LON-SVR1:** DHCP, DNS
- **TOR-SVR1:** DHCP
- **SYD-SVR1:** DC, DNS

The main tasks for this exercise are as follows:

1. Configure the IPAM server for GPO deployment.
2. Perform discovery on Adatum.com.
3. Provision IPAM server to manage DC, DNS, and DHCP servers.



► **Task 1: Configure the IPAM server for GPO deployment**

1. On **LON-SVR2**, in the **Server Manager** navigation pane, click **IPAM**.
2. In the **IPAM Overview** pane, connect to and provision the IPAM server by using Group Policy.
3. Enter **IPAM** as the **GPO name prefix**, and then provision IPAM.

► **Task 2: Perform discovery on Adatum.com**


1. In the **IPAM Overview** pane, configure server discovery for the Adatum domain, and then start the server discovery process.
2. In the **IPAM Overview** pane, click the **Select or add servers to manage and verify IPAM access** link.
3. Verify that IPAM access is currently blocked.

► **Task 3: Provision IPAM server to manage DC, DNS, and DHCP servers**

1. On **LON-SVR2**, use Windows PowerShell (Admin) to grant the IPAM server permission to manage servers in Adatum.com by using the following command:

```
Invoke-IPamGpoProvisioning -Domain Adatum.com -DomainController lon-dc1.adatum.com -GpoPrefixName IPAM IpamServerFqdn LON-SVR2.adatum.com -DelegatedGpoUser Administrator
```

2. Switch to **LON-DC1**, and then make the following changes to the **IPAMUG** group in **Active Directory Administrative Center**:
  - Group scope: **Global**
  - Member Of: Add the **Adatum\Domain Admins** group
3. Restart **LON-SVR2**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
4. Open **Server Manager**, and then on the **IPAM** page, open the **Edit Server** page, and then set the manageability status to **Managed** for all servers.

 **Note:** If a GPO error appears, switch the server back to **Unspecified**, and then restart **LON-DC1**, **LON-SVR1**, **LON-SVR2**, **TOR-SVR1**, and **SYD-SVR1**. Sign back in to all servers as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

5. Switch to **LON-DC1**.
6. Force the update of Group Policy by using **Gpupdate /force**.
7. Switch to **LON-SVR1**.
8. Force the update of Group Policy by using **Gpupdate /force**.
9. Switch to **TOR-SVR1**.
10. Force the update of Group Policy by using **Gpupdate /force**.
11. Switch to **SYD-SVR1**.
12. Force the update of Group Policy by using **Gpupdate /force**.
13. Switch back to **LON-SVR2**, and then refresh the **IPv4** view.



**Note:** It might take up to five minutes for the status to change. If the status does not change, restart **LON-DC1**, **LON-SVR1**, **LON-SVR2**, **TOR\_SVR1**, and **SYD-SVR1**, and then repeat step 13. Ensure that you restart **LON-DC1** before restarting the other virtual machines.

14. In the **IPAM Overview** pane, retrieve data from the managed server.

**Results:** After completing this exercise, you should have successfully provisioned the IPAM server.

## Exercise 3: Managing IP address spaces by using IPAM

### Scenario

Your task is to use IPAM to confirm the status of the current DHCP and DNS environment and to make the following changes:

- Add an IP address block for the Toronto subnet, which is configured through static IP addresses:
  - 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 addresses**
- Create an IP address reservation in the Houston scope for a network printer that is being installed:
  - Server IP: **172.16.20.200**
- Deactivate the DHCP scope for the Portland office.

The main tasks for this exercise are as follows:

1. Add an IP address block.
2. Create an IP address reservation.
3. Deactivate the Portland Wired scope.
4. Prepare for the next module.

#### ► Task 1: Add an IP address block

1. On **LON-SVR2**, in **Server Manager**, add the following IP address block:
  - 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**
2. Change the **current view** to **IP Address Blocks** to view the newly created address block.

► **Task 2: Create an IP address reservation**

1. In **Server Manager**, on the **IP Address Blocks** page, switch the view to **IP Address Ranges**.
2. Edit the IP address range for either of the **172.16.20.0/23** networks.
3. Add a reservation for the **172.16.20.200** IP address.

► **Task 3: Deactivate the Portland Wired scope**

- On the **DHCP Scopes** page, deactivate both Portland Wired scopes:
  - Scope name: **Portland Wired**
  - Scope ID: **172.16.23.0**



**Note:** This scope is duplicated as a result of DHCP failover configuration between **TOR-SVR1** and **LON-SVR1**. The preceding step deactivates the scopes on both servers.

**Results:** After completing this exercise, you should have successfully managed IP address spaces by using IPAM.

► **Task 4: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-EU-RTR**, **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-SYD-SVR1**, and **20741A-TOR-SVR1**.

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

**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?

## Module Review and Takeaways

### Review Questions

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

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

# Module 6

## Remote access in Windows Server 2016

### Contents:

Module Overview	6-1
Lesson 1: Overview of remote access	6-2
Lesson 2: Implementing Web Application Proxy	6-13
Lab: Implementing Web Application Proxy	6-18
Module Review and Takeaways	6-25

## Module Overview

Remote access technologies in Windows Server 2016 enable users to connect securely to data and resources in corporate networks. In Windows Server 2016, four component technologies—virtual private network (VPN), DirectAccess, Routing, and Web Application Proxy—are combined into a single, unified server role called Remote Access.



**Note:** VPN, DirectAccess, and Routing are available in both Windows Server 2012 and Windows Server 2012 R2. However, Web Application Proxy is a feature that was introduced in Windows Server 2012 R2.

In this module, you will learn how to implement remote access technologies in Windows Server 2016. You will also learn about different implementation scenarios for small or medium-sized organizations and enterprise organizations.

### Objectives

After completing this module, you will be able to:

- Install and manage the Remote Access server role in Windows Server 2016.
- Implement Web Application Proxy.

## Lesson 1

# Overview of remote access

You can configure and manage the Remote Access server role in Windows Server 2016 by using the Remote Access Management console. The type of remote access technology that organizations implement depends on their business requirements. Some organizations might deploy several remote access technologies on different servers, and some might deploy them on the same server. For example, organizations that need to enable users to seamlessly access the corporate network or enable administrators to manage servers or workstations on the Internet will deploy DirectAccess. At the same time, they will deploy Web Application Proxy to provide more secure access to internal applications from smartphones, tablets or home computers without having to change the configuration on these devices or be inside the corporate network.

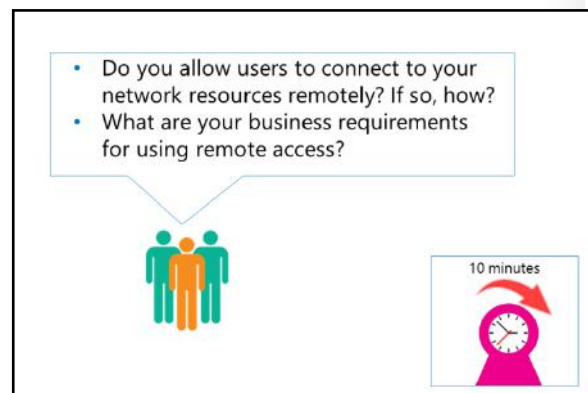
### Lesson Objectives

After completing this lesson, you will be able to:

- Explain when to use remote access.
- Describe the remote access options available in Windows Server 2016.
- Describe how to manage remote access in Windows Server 2016.
- Install and manage the Remote Access server role.
- Explain the role of Network Policy Server.
- Describe network policies and how to evaluate them.
- Configure Network Policy Server policies.
- Describe the considerations for deploying a public key infrastructure (PKI) for remote access in Windows Server 2016.
- Explain how to configure routing and network address translation (NAT).

### Discussion: When to use remote access

Remote access technologies provide various solutions that allow secure access to an organization's infrastructure from different locations. While organizations usually own and protect local area networks (LANs) entirely by themselves, remote connections to servers, shares, and apps must often travel across unprotected and unmanaged networking infrastructure, such as the Internet. Any method of using public networks for the transit of organizational data must include a way to protect the integrity and confidentiality of that data.



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

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

## Remote access options

The Remote Access server role in Windows Server 2016 provides four remote access options: DirectAccess, VPN, Routing, and Web Application Proxy. Each of the options represents a technology that organizations can use to access internal resources from offices in remote site locations or from the Internet. The technology that they use depends on their different business scenarios.

- DirectAccess
- VPN
- Routing
- Web Application Proxy

### DirectAccess

DirectAccess enables remote users to access corporate resources such as email servers, shared folders, and internal websites securely, without connecting to a VPN. DirectAccess also provides increased productivity for a mobile workforce by offering the same connectivity experience both inside and outside the office. With the new unified management experience, you can configure DirectAccess and older VPN connections from a single location. Other enhancements in DirectAccess include simplified deployment and improved performance and scalability.

### VPN

VPN connections enable users who are working offsite (for example, from home, a customer site, or a public wireless access point) to access a server on an organization's private network by using the infrastructure that a public network, such as the Internet, provides. From the user's perspective, the VPN is a point-to-point connection between a computer, the VPN client, and an organization's server. The exact infrastructure of the shared or public network is irrelevant, because it appears as if the data is sent over a dedicated private link.

### Routing

Windows Server 2016 can act as a router or NAT device between two internal networks or between the Internet and the internal network. Routing works with routing tables and supports routing protocols such as Routing Information Protocol (RIP) version 2, Internet Group Management Protocol (IGMP), and Dynamic Host Configuration Protocol (DHCP) Relay Agent.

### Web Application Proxy

Web Application Proxy provides reverse proxy functionality for users who must access their organization's internal web applications from the Internet. Web Application Proxy preauthenticates users by using the following options:

- Active Directory Federation Services (AD FS) technology, where Web Application Proxy acts as an AD FS proxy.
- Pass-through authentication, where authentication is not performed by Web Application Proxy, but is performed by the published application

## Managing remote access in Windows Server 2016

After you install the Remote Access role on a server that is running Windows Server 2016, you can manage the role by using the Microsoft Management Console (MMC), and by using Windows PowerShell. You can use the MMC for your day-to-day tasks of managing remote access, and you can use Windows PowerShell for managing multiple servers and for scripting or automating management tasks.

There are two MMCs for managing the Remote Access server role: the Remote Access Management console, and the Routing and Remote Access console. You can access these consoles from the **Tools** menu in **Server Manager**.

You can manage the Remote Access server role by using:

- Remote Access Management console
- Routing and Remote Access console
- Windows PowerShell commands:
  - **Set-DAServer**
  - **Get-DAServer**
  - **Set-RemoteAccess**
  - **Get-RemoteAccess**

### The Remote Access Management console

The Remote Access Management console allows you to manage DirectAccess, VPN, and Web Application Proxy. When you open this console for the first time, it provides you with a wizard-based setup to configure remote access settings according to your business requirements. After you configure the initial remote access settings, you will be provided with the following options in the console to manage your remote access solution:

- **Configuration.** You can edit the remote access settings by using wizards and by using the graphical representation of the current network configuration in the console.
- **Dashboard.** You can monitor the overall status of servers and clients that are part of your remote access solution.
- **Operations status.** You can access detailed information on the status of the servers that are part of your remote access solution.
- **Remote Client Status.** You can access detailed information on the status of the clients that are connecting to your remote access solution.
- **Reporting.** You can generate historical reports on different parameters, such as remote access usage, access details, connection details, and server load statistics.

### The Routing and Remote Access console

You can use the Routing and Remote Access console to configure a server running Windows Server 2016 as a NAT device, as a router for both IPv4 and IPv6 protocols, and as a VPN server. After you complete the configuration, you can manage the remote access solution by using the following options in the console:

- **Server Status.** You can monitor the status of the Remote Access server, the ports in use, and how long the server has been operational (that is, the server uptime).
- **Remote Access Client, Ports, Remote Access Logging.** You can monitor the client status, port status, and detailed logging information about clients that are connected to the Remote Access server.
- **IPv4.** You can configure the IPv4 settings such as NAT, IPv4 routing with static routes, and the following routing protocols: RIP version 2, IGMP, and the DHCP Relay Agent.
- **IPv6.** You can configure IPv6 settings, such as IPv6 routing with static routes and the DHCP Relay Agent routing protocol.



## Windows PowerShell commands

Windows PowerShell commands in Windows Server 2016 allow you to configure remote access and create scripts for automation of some the configuration and management procedures. Some examples of Windows PowerShell commands for remote access include:

- **Set-DAServer.** Sets the properties specific to the DirectAccess server.
- **Get-DAServer.** Displays the properties of the DirectAccess server.
- **Set-RemoteAccess.** Modifies the configuration that is common to both DirectAccess and VPN, such as Secure Sockets Layer (SSL) certificate, internal interface, and Internet interface.
- **Get-RemoteAccess.** Displays the configuration of DirectAccess and VPN (both remote access VPN and site-to-site VPN).



**Additional Reading:** For more information, refer to: "Remote Access Cmdlets" at <http://aka.ms/Fp4ry6>

## Demonstration: Installing and managing the Remote Access server role

In this demonstration, you will see how to:

- Install the Remote Access server role.
- Manage the Remote Access server role.

### Demonstration Steps

#### Install the Remote Access server role

1. On **LON-SVR1**, open **Server Manager**, click **Manage**, and then start the **Add Roles and Features Wizard**.
2. Complete the wizard as follows:
  - a. On the **Before you begin** page, click **Next**.
  - b. On the **Select installation type** page, click **Next**.
  - c. On the **Select destination server** page, click **Next**.
  - d. On the **Select server roles** page, click **Remote Access**, and then click **Next**.
  - e. On the **Select features** page, click **Next**.
  - f. On the **Remote Access** page, click **Next**.
  - g. 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**. Then click **Next**.
  - h. On the **Confirm installation selections** page, click **Install**.
3. When the installation finishes, click **Close**.

#### Manage the Remote Access server role

1. In the **Server Manager** console, open the **Remote Access Management Console**.
2. In the console, review the options for configuring and managing remote access.
3. From the **Server Manager** console, open the **Routing and Remote Access** console.
4. In the console, review the options for configuring and managing remote access.

## What is Network Policy Server?

Network Policy Server is part of the Network Policy and Access Services server role. It enables you to create and enforce organization-wide network access policies for connection request authentication and connection request authorization. You also can use a Network Policy Server as a RADIUS proxy to forward connection requests to another Network Policy Server or other RADIUS servers that you configure in remote RADIUS server groups.

You can use Network Policy Server to centrally configure and manage network access authentication, authorization, and client health policies with any combination of the following functions:

- RADIUS server.
- RADIUS proxy.

### RADIUS server

Network Policy Server performs centralized connection authentication, authorization, and accounting for wireless, authenticating switch, and dial-up and VPN connections. When using Network Policy Server as a RADIUS server, you configure network access servers, such as wireless access points and VPN servers, as RADIUS clients in Network Policy Server. You also configure network policies that Network Policy Server uses to authorize connection requests, and you can configure RADIUS accounting so that Network Policy Server logs accounting information to log files on the local hard disk or in a Microsoft SQL Server database.

Network Policy Server is Microsoft's implementation of a RADIUS server. Network Policy Server enables the use of a heterogeneous set of wireless, switch, remote access, or VPN equipment. You can use Network Policy Server with the Routing and Remote Access service, which has been available since Windows 2000.

When a Network Policy Server is a member of an AD DS domain, Network Policy Server uses AD DS as its user account database and provides single sign-on (SSO), which means that users utilize the same set of credentials for network access control (authenticating and authorizing access to a network) as they do to access resources within the AD DS domain.

Organizations that maintain network access, such as Internet service providers (ISPs), must manage a variety of network access methods from a single administration point, regardless of the type of network access equipment they use. The RADIUS standard supports this requirement. RADIUS is a client-server protocol that enables network access equipment, used as RADIUS clients, to submit authentication and accounting requests to a RADIUS server.

A RADIUS server has access to user account information, and it can verify network access authentication credentials. If the user's credentials are authentic, and RADIUS authorizes the connection attempt, the RADIUS server then authorizes the user's access based on configured conditions, and it logs the network access connection in an accounting log. Using RADIUS, you can collect and maintain the network access user authentication, authorization, and accounting data in a central location, rather than on each access server.

A Network Policy Server in Windows Server 2016 provides the following functions:

- RADIUS server. Network Policy Server performs centralized connection authentication, authorization, and accounting for wireless, authenticating switch, and dial-up and VPN connections
- RADIUS proxy. You configure connection request policies that indicate which connection requests the Network Policy Server will forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests

## RADIUS proxy

When using Network Policy Server as a RADIUS proxy, you configure connection request policies that indicate which connection requests the Network Policy Server will forward to other RADIUS servers and to which RADIUS servers you want to forward the connection requests. You also can configure Network Policy Server to forward accounting data for logging by one or more computers in a remote RADIUS server group.

With Network Policy Server, your organization also can outsource its remote access infrastructure to a service provider, while retaining control over user authentication, authorization, and accounting.

You can create different Network Policy Server configurations for the following solutions:

- Wireless access.
- Organizational dial-up or VPN remote access.
- Outsourced dial-up or wireless access.
- Internet access.
- Authenticated access to extranet resources for business partners.

## Network Policy Server policies

Network Policy Server supports policies that are designed to manage and control connection request attempts for remote access clients and to determine which Network Policy Server are responsible for managing and controlling connection attempts. The Network Policy Server policies are:

- Connection request policies. These allow you to designate whether the local Network Policy Server processes connection requests locally or if they are forwarded for processing to another RADIUS server.

With connection request policies, you can use Network Policy Server as a RADIUS server or as a RADIUS proxy, based on a variety of factors, including:

- The time of day and day of the week.
- The realm name in the connection request.
- The connection type that you are requesting.
- The RADIUS client's IP address.

When you install Network Policy Server, a default connection request policy is created with the following conditions:

- Authentication is not configured.
- Accounting is not configured to forward accounting information to a remote RADIUS server group.
- Attribute manipulation is not configured with rules that change attributes in forwarded connection requests.

- Network Policy Server supports policies that manage and control connections from remote access clients
- Two types of policies exist:
  - Connection request policies
    - Used when Network Policy Server should act as a RADIUS server or RADIUS proxy
  - Network policies
    - Used to authenticate and authorize the connection attempt
- You set conditions and constraints to control access
- When you first deploy Network Policy Server, remote access is denied. You must configure at least one policy to allow access



- Forwarding Request is turned on, which means that the local Network Policy Server authenticates and authorizes connection requests.
- Advanced attributes are not configured.
- The default connection request policy uses Network Policy Server as a RADIUS server.
- Network policies. A network policy is a set of conditions, constraints, and settings that enable you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Each network policy has four categories of properties:

- Overview. Overview properties allow you to specify whether the policy is enabled, whether the policy grants or denies access, and whether a specific network connection method or type of network access server is required for connection requests. Overview properties also enable you to specify whether to ignore the dial-in properties of user accounts in AD DS. If you select this option, Network Policy Server uses only the network policy's settings to determine whether to authorize the connection.
- Conditions. These properties allow you to specify the conditions that the connection request must have to match the network policy. If the conditions that are configured in the policy match the connection request, Network Policy Server applies the network policy settings to the connection. For example, if you specify the network access server IPv4 address (NAS IPv4 Address) as a condition of the network policy and Network Policy Server receives a connection request from a network access server that has the specified IP address, the condition in the policy matches the connection request.
- Constraints. Constraints are additional parameters of the network policy that are required to match the connection request. If the connection request does not match a constraint, Network Policy Server rejects the request automatically. Unlike the Network Policy Server response to unmatched conditions in the network policy, if a constraint is not matched, Network Policy Server does not evaluate additional network policies, and the connection request is denied.
- Settings. The Settings properties allow you to specify the settings that Network Policy Server applies to the connection request, if all of the policy's network policy conditions are matched and the request is accepted.

When Network Policy Server performs authorization of a connection request, it compares the request with each network policy in the ordered list of policies, starting with the first policy and moving down the list. If Network Policy Server finds a policy in which the conditions match the connection request, Network Policy Server uses the matching policy and the dial-in properties of the user account to perform authorization. If you configure the dial-in properties of the user account to grant or control access through a network policy, and if the connection request is authorized, Network Policy Server applies the settings that you configure in the network policy to the connection:

- If Network Policy Server does not find a network policy that matches the connection request, Network Policy Server rejects the connection unless the dial-in properties on the user account are set to grant access.
- If the dial-in properties of the user account are set to deny access, Network Policy Server rejects the connection request.



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



**Additional Reading:** For more information, refer to: "RADIUS Proxy" at <http://aka.ms/Oy16cb>

## Demonstration: Configuring Network Policy Server policies

In this demonstration, you will see how to configure remote access policies.

### Demonstration Steps

1. On **EU-RTR**, from **Server Manager**, open the **Network Policy Server** console.
2. In the **Network Policy Server** console, in the navigation pane, expand **Policies**, and then right-click **Network Policies**.
3. Create a new network policy with following settings:
  - o Policy name: **Adatum IT VPN**
  - o Type of network access server: **Remote Access Server (VPN-Dial up)**
  - o Windows Groups: **IT**
  - o Specify Access Permission: **Access granted**
  - o Configure Authentication Methods: Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box
  - o Add **Microsoft Secured password (EAP-MSCHAP v2)**.
  - o Add **Microsoft: Smart Card or other certificate**.
  - o Complete the wizard by accepting the default settings on the other pages.
4. Close all open windows.

## Considerations for deploying PKI for remote access

Public key infrastructure (PKI) helps you verify and authenticate the identity of each party involved in an electronic transaction. It also helps establish trust between computers and the corresponding applications that are hosted on application servers. A common example includes the use of PKI technology to secure websites and remote access. Digital certificates are key PKI components that contain electronic credentials, which are then used to authenticate users or computers. Windows Server 2016 supports building a certificate services infrastructure in your organization by using Active Directory Certificate Services (AD CS) components.

- Will you use PKI for encryption of only data and traffic?
- Will you use PKI not just for encryption, but for authenticating users and their computers?
- Will you use self-signed certificates, certificates provided by internal private CAs, or external public CAs?

## Using PKI for remote access

When employees of an organization access internal resources from the Internet, it is critical to protect the communication and data in transit from interception by unauthorized users. Therefore, you should encrypt communications between the organization's internal resources and the employees using the Internet. Furthermore, the users that connect from the Internet as well as their computers should be authenticated. Remote access technologies in Windows Server 2016 use PKI for authenticating users and computers and for encrypting data and communication when users remotely access internal resources.

When planning to use PKI for remote access in your organization, you should consider the following:

- Will you use PKI for encryption of data and traffic only? In this scenario, you install the certificate only on the Remote Access server, from which users are authenticated with their user names and passwords.
- Will you use PKI for authenticating users and their computers in addition to encryption? In this scenario, you use PKI for encryption and for issuing certificates to users and computers. Note that some organizations choose to issue certificates to either users or computers, but not to both.
- Which type of certificates will you use? You can use self-signed certificates, or certificates issued either by a private certification authority (CA) or by a public CA:
  - Self-signed certificates are issued by the server itself. By default, they are trusted only by the issuing server and not by other computers in the organization. You use self-signed certificates in small and medium-sized organizations that use DirectAccess configured with the **Getting Started Wizard**, which provides easy setup and configuration.
  - Certificates issued by a private CA. You use certificates issued by a private CA in organizations that want to manage their own PKI infrastructure and that use PKI for many purposes, such as remote access, client authentication, and server authentication. These organizations realize significant cost benefits when using private CAs, because they do not need to purchase a large number of certificates and instead use the certificates issued by the private CA.
  - Certificates issued by a public CA. You use certificates issued by a public CA in organizations that deploy certificates for applications that need to be trusted by many different operating systems, computers, and devices. In these organizations, you cannot use a private CA, because, by default, only domain computers trust private CA certificates. Public CAs also are used by organizations that do not have a PKI infrastructure deployed, or that need smaller numbers of certificates.

When deploying advanced DirectAccess infrastructure, you should use either a private CA or a public CA. As a best practice, you should not use self-signed certificates. The following table includes the advantages and disadvantages of certificates issued by private CAs or public CAs.

CA type	Advantages	Disadvantages
Private CA	<ul style="list-style-type: none"> <li>• Provides greater control over certificate management</li> <li>• Lower cost when compared to a public CA</li> <li>• Customized templates</li> <li>• Autoenrollment</li> </ul>	<ul style="list-style-type: none"> <li>• By default, not trusted by external clients (web browsers, operating systems)</li> <li>• Requires greater administration</li> </ul>
Public CA	<ul style="list-style-type: none"> <li>• Trusted by many external clients (web browsers, operating systems)</li> <li>• Requires minimal administration</li> </ul>	<ul style="list-style-type: none"> <li>• Higher cost when compared to a private CA</li> <li>• Cost is based per certificate</li> <li>• Certificate procurement is slower</li> </ul>

Some organizations have started using a hybrid approach for their PKI architecture. A hybrid approach uses an external public CA for the root CA and a hierarchy of internal CAs for distribution of certificates. This gives organizations the advantage of having their internally-issued certificates trusted by external clients, while still providing the advantages of an internal CA.

## Configuring Routing and NAT with the remote access role

### Routing

In Windows Server 2016, Routing and Remote Access (RRAS) can function as a software-based router and thereby manage the data that flows between subnets. Its routing capabilities include LAN-to-WAN and NAT.

A router manages outgoing and incoming data packets and, based on the information in its routing table, directs the traffic to the destination or to another router, which then processes the packet and forwards it to the destination network.

The routing table holds the information about the router's own network interfaces, destinations, and sources for network traffic.

RRAS supports the following types of routing:

- Static Routes (IPv4 and IPv6).
- Internet Group Management Protocol (IGMP) (IPv4).
- Router Information Protocol (RIP) (IPv4).
- Network Address Translation (NAT) (IPv4).

### Static Routes

The routing information is static and must be entered manually by an administrator.

### RIP

When using RIP, the routing table is dynamically updated as the router advertises the information about the networks it knows and listens for other router's advertisements. When new information about a network is received it will be inserted into the router's routing table. RIP-enabled routers advertise their routing every 30 seconds.

### IGMP

IGMP is used to route multicast traffic.

If the router is connected directly to the networks for which it manages traffic, no additional configuration is needed, because the router automatically updates its routing table with the required routing information. Consider a scenario in which you have three different networks called Network 1, Network 2, and Network 3, and two routers called Router A and Router B. Router A is connected directly to Network 1 and Network 2, and Router B is connected directly to Network 2 and Network 3. Router A needs information about how to reach Network 3, and Router B needs information about how to reach Network 1. This can be done by enabling the RIP routing protocol on both routers and letting them exchange routing information automatically. Alternatively, an administrator could create a static route on each of the routers.

#### Routing in RRAS:

- RRAS is a software-based router
- Can route LAN-to-LAN, LAN-to-WAN, demand-dial, and NAT traffic
- Supports the following type of routing:
  - Static Routes (IPv4/IPv6)
  - IGMP (IPv4)
  - RIP (IPv4)
  - NAT (IPv4)
- A good option for directing traffic between networks with light-to-medium traffic





**Note:** The routing functionality in RRAS is normally a good option for directing traffic between networks with light-to-medium traffic. If you need to route heavy traffic between network segments, a hardware-based router might be a better fit, because hardware devices usually can handle a higher load and perform better under heavy load.

## NAT

NAT is a component of the RRAS service that enables corporate computers to access resources on the Internet or other public networks. NAT translates private IPv4 addresses in a corporate network into public IPv4 addresses.

### **Why is NAT necessary?**

Computers and devices that connect to the Internet must be configured with public IP addresses. However, the number of public IPv4 addresses is becoming limited, and organizations cannot obtain a public IPv4 address for every corporate computer. Therefore, organizations use private IP addressing for corporate computers. Because private IP addresses are not routable on the Internet, computers configured with private IP addresses cannot access the Internet. By using NAT, organizations need to obtain only one public IPv4 address to access the Internet. NAT then translates the private IPv4 address into a public IPv4 address, which then provides Internet access to corporate computers.

A NAT server has two network adapters. One of these network adapters is configured with a private IPv4 address and connects to the corporate network, whereas the other network adapter is configured with a public IPv4 address and connects to the Internet.

### **How does NAT work?**

To connect a client computer to the Internet by using NAT, you must configure the computer to use the NAT server as a default gateway. When a client computer on the private network requests access to a computer that is located on the Internet, such as a web server, the NAT-enabled server translates the outgoing packets and then sends them to the web server on the Internet. The NAT server also translates the response from the web server on the Internet and returns it to the client on the corporate network.

The NAT server secures the corporate network by hiding the IP addresses of computers on that network. When a computer on the corporate network communicates with a web server located on the Internet, only the external IP address of the NAT server is visible to the Internet web server. Furthermore, you can configure Windows Firewall with Advanced Security on the NAT server to protect your corporate network from Internet security threats.

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

Verify the correctness of the statement by placing a mark in the column to the right.

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



## Lesson 2

# Implementing Web Application Proxy

Many organizations must provide their users access to web applications that are on the corporate network, even though the users are not on the corporate network, but on the Internet. The process of configuring an application so that it is accessible from the Internet is called *publishing*. Windows Server 2012 R2 introduced the Web Application Proxy role service that you can use for publishing applications. Web Application Proxy is deployed as a component of the Remote Access server role in Windows Server 2016 and Windows Server 2012 R2.

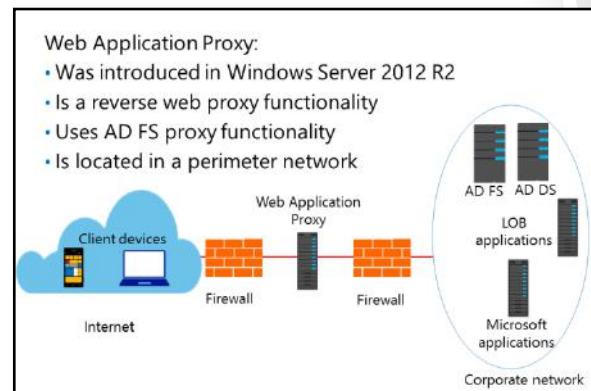
### Lesson Objectives

After completing this lesson, you will be able to:

- Describe Web Application Proxy.
- Identify the authentication options for Web Application Proxy.
- Explain how to publish applications with Web Application Proxy.
- Publish a secure website.

### What is Web Application Proxy?

Web Application Proxy is a Remote Access role service that was introduced in Windows Server 2012 R2. This role service functions as a reverse web proxy, and provides users that are located on the Internet with access to internal corporate web applications or Remote Desktop Gateway servers. Web Application Proxy uses the AD FS technology to preauthenticate Internet users and acts as an AD FS proxy for publishing claims-aware applications. A claims-aware application can use any information about a user such as group membership, email address, department or company to authorize the user.



Before you install Web Application Proxy, you must deploy AD FS as a prerequisite. AD FS provides users with the single sign-on (SSO) functionality, which means that if users enter their credentials for accessing a corporate web application once, they will not be asked to enter their credentials again for subsequent access to the corporate web application.

Placing the Web Application Proxy server in the perimeter network between two firewall devices is a typical configuration. The AD FS server and applications that are published are located on the corporate network, and together with domain controllers and other internal servers, are protected by the second firewall. This scenario provides secure access to corporate applications for users located on the Internet, and at the same time protects the corporate IT infrastructure from security threats on the Internet.

## Authentication options for Web Application Proxy

Web Application Proxy in Windows Server 2016 supports two types of preauthentication:

- AD FS preauthentication. AD FS preauthentication uses AD FS for web applications that use claims-based authentication. When a user initiates a connection to the corporate web application, the first entry point the user connects to is the Web Application Proxy. Next, Web Application Proxy preauthenticates the user in the AD FS server. If the authentication is successful, Web Application Proxy establishes a connection to the web server in the corporate network where the application is hosted.
- Pass-through preauthentication. Pass-through preauthentication does not use AD FS for authentication, nor does Web Application Proxy preauthenticate the user. Instead, the user is connected to the web application through Web Application Proxy, and if the web application is configured for authentication, the user is authenticated by the application.

- User authentication:
  - AD FS preauthentication
  - Pass-through preauthentication
- AD FS benefits:
  - Workplace join
  - SSO
  - Multifactor authentication
  - Multifactor access control

AD FS preauthentication provides the following benefits over pass-through preauthentication:

- Workplace join. Workplace Join was a new feature in AD FS in Windows Server 2012 R2. It allows devices that are not members of the Active Directory domain, such as smartphones, tablets, or non-company laptops, to be added to a workplace. After these non-domain devices are added to the workplace, you can configure them for AD FS preauthentication.
- SSO. SSO allows users that are preauthenticated by AD FS to enter their credentials only once. If users subsequently access other applications that use AD FS for authentication, they will not be prompted again for their credentials.
- Multifactor authentication. Multifactor authentication allows you to configure multiple types of credentials in order to strengthen security. For example, you can configure the system so that users enter their user name and password together with a smart card.
- Multifactor access control. Multifactor access control is used in organizations that want to strengthen their security in publishing web applications by implementing authorization claim rules. The rules are configured so that they issue either a permit or a deny claim that determines whether a user or a group is allowed or denied access to a web application that is using AD FS preauthentication.

## Publishing applications with Web Application Proxy

After the Web Application Proxy server role is installed, you must configure it by using the **Web Application Proxy Configuration Wizard** from the **Remote Access Management** console. When the Web Application Proxy Configuration Wizard completes, it creates the **Web Application Proxy** console, which you can use for further management and configuration of Web Application Proxy.

The Web Application Proxy Configuration Wizard requires that you enter the following information during the initial configuration process:

### Configuring Web Application Proxy settings:

- AD FS server name
- AD FS administrator credentials
- AD FS certificate

- AD FS name. To locate this name, open the **AD FS Management** console, and, under **Edit Federation Service Properties**, find the value in the **Federation Service name** box.
- Credentials of local administrator account for AD FS.
- AD FS Proxy Certificate. This is a certificate that Web Application Proxy will use for AD FS proxy functionality.

After completing the Web Application Proxy Configuration Wizard, you can publish either your web application or your Remote Desktop Gateway (RDG) by using the Web Application Proxy console.


When you publish your web application you must provide the following information:

- Type of preauthentication (for example, pass-through).
- The application that will be published.
- The external URL of the application (for example, <https://lon-svr1.adatum.com>).
- A certificate whose subject name covers the external URL (for example, [lon-svr1.adatum.com](https://lon-svr1.adatum.com)).
- URL of the backend server (note that this value is automatically entered when you enter the external URL).

If you want to publish RDG, you will have to decide whether to use pre-authentication or pass-through authentication. If you want to use Multifactor Authentication (MFA) together with RDG, you must use pre-authentication when publishing RDG. If you do not need MFA you can use pass-through authentication which will provide a single point of connection into your systems.

When you publish your RDG you must provide the following information:

- Type of preauthentication (for example, pass-through).
- The application that will be published.
- The external URL of the RDG (for example, <https://rdgw.adatum.com>).
- A certificate whose subject name covers the external URL (for example, [rdgw.adatum.com](https://rdgw.adatum.com)).
- URL of the backend server (note that this value is automatically entered when you enter the external URL).

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

## Demonstration: Publishing a secure website

In this demonstration, you will learn how to:

- Install the Web Application Proxy role service.
- Configure access to an internal website.
- Verify access to the internal website from the client computer.

### 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** field, type **http://lon-svr1.adatum.com**, and then press Enter. Notice that a Network Error message displays.
6. Open the **Remote Desktop Connection** app, and try to connect to **LON-DC1**. Notice that you cannot connect to **LON-DC1**, because the computer cannot be found on the network.
7. Close all open windows.



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

#### Install the Web Application Proxy role service

1. Switch to **EU-RTR**.
2. Open **Server Manager**, and then on the **Dashboard** page, click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, on the **Select server roles** page, expand **Remote Access**, and then click **Web Application Proxy**.
4. Click **Next**, and then click **Install**.

#### Obtain a certificate for the ADFS WAP farm

- Open the **MMC**, add the **Certificates - Computer account** snap-in, and then request a new certificate with the following settings:
  - Subject Name: **Common Name adfswap.adatum.com**
  - Alternative name: **DNS adfswap.adatum.com, lon-svr1.adatum.com, rdgw.adatum.com**

#### Configure Web Application Proxy

1. From **Server Manager**, open the **Remote Access Management** console.
2. In the navigation pane, click **Web Application Proxy**, and then run the **Web Application Proxy Configuration Wizard**.
3. In the **Web Application Proxy Configuration Wizard**, for **Federation service name**, type **adfswap.adatum.com**.
4. In the **User name** box, type **Administrator** and, in the **Password** box, type **Pa\$\$w0rd**.

5. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the **Web Application Proxy** server, click **adfswap.adatum.com**.
6. On the **Results** page, verify that the configuration was successful, and then close the wizard.



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

### Publish an internal website

1. On the Web Application Proxy server, in the **Remote Access Management** console, in the navigation pane, start the **Publish New Application Wizard**.
2. On the **Preauthentication** page, click **Pass-through**.
3. In the **Name** box, type **Adatum LOB Web App (LON-SVR1)**.
4. In the **External URL** box, type **https://lon-svr1.adatum.com**.
5. In the **External certificate** list, click **adfswap.adatum.com**.
6. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed.



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

### Configure internal website authentication

1. Switch to **LON-SVR1**, open **Server Manager**, and in the **Tools** menu, click **Internet Information Services (IIS) Manager**.
2. Expand **LON-SVR1 (ADATUM\administrator)**, expand **Sites**, and then click **Default Web site**.
3. In the **Default Web Site Home** pane, double-click **Authentication**. In the **Authentication** pane, right-click **Windows Authentication**, and then click **Enable**.
4. In the **Authentication** pane, right-click **Anonymous Authentication**, and then click **Disable**.
5. Close the **Internet Information Services (IIS) Manager** console.

### Verify access to internal web site

1. Switch to **LON-CL1**, and on the taskbar, click the **Microsoft Edge** icon. Open the **https://lon-svr1.adatum.com** web address.
2. When prompted, type **adatum\logan** for the username and **Pa\$\$w0rd** for the password, and then click **OK**.
3. Verify that the default **IIS 9.0** webpage for **LON-SVR1** opens.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
The Web Application Proxy role requires AD FS.	

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

## Lab: Implementing Web Application Proxy

### Scenario

The remote access deployment is working well at A. Datum Corporation, but IT management also wants to enable access to some internal applications for users from partner companies. These users should not have access to any internal resources except for the specified applications. You must implement and test Web Application Proxy for these users. Furthermore, administrators at A. Datum should be able to remotely manage servers in the internal network in the most secure manner possible.

### Objectives

After completing this lab, you will be able to:

- Implement Web Application Proxy.
- Validate the Web Application Proxy deployment.

### Lab Setup

Estimated Time: 70 minutes

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-EU-RTR**, and **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Virtual machine: **20741A-INET1**

User name: **Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, on the **Start** screen, click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-EU-RTR**, and **20741A-LON-CL1**.
6. In Hyper-V Manager, click **20741A-INET1**, and in the **Actions** pane, click **Start**.
7. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
8. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**

## Exercise 1: Implementing Web Application Proxy

### Scenario

You need to implement Web Application Proxy to enable external users to access applications at A. Datum. You will use the initial deployment as a proof of concept while the developers at A. Datum modify the internal applications to use claims-based authentication. You also need to enable the administrators at A. Datum to be able to securely connect to any server in the internal network by using Remote Desktop. You will install and configure a Remote Desktop Gateway server in the internal network and publish it through a Web Application Proxy server.

The main tasks for this exercise are as follows:

1. Prepare environment.
2. Remove the client computer from a domain.
3. Install the Web Application Proxy role service.
4. Configure access to an internal website.
5. Configure access to Remote Desktop Gateway.

#### ► Task 1: Prepare environment

##### Disable routing and remote access on EU-RTR

1. Switch to **EU-RTR**.
2. Open **Server Manager**, and then from the **Tools** menu, open **Routing and Remote Access**.
3. In the **Routing and Remote Access** console, disable **Routing and Remote Access**.



**Note:** Routing and Remote Access is preconfigured on the virtual machine for the purpose of other labs in this course. The Web Application Proxy configuration in this lab will not work properly if you leave Routing and Remote Access enabled on the virtual machine.

#### ► Task 2: Remove the client computer from a domain

1. Switch to **LON-CL1**.
2. Open **Control Panel**.
3. In **Control Panel**, remove **LON-CL1** from the **adatum.com** domain, and then add **LON-CL1** to a workgroup named **WORKGROUP**.

##### Import Root CA certificate on client

1. When the **LON-CL1** computer restarts, sign in with the user name **Admin** and the password **Pa\$\$w0rd**.
2. When prompted by **Networks**, click **Yes**.
3. Click **File Explorer** and open **\\172.16.0.10\C\$**.
4. Install the **AdatumRootCA** certificate on **LON-CL1** to **Local Machine** by selecting the **Place all certificates in the Trusted Root Certification Authorities** option.
5. Open a command prompt, type **mmc**, and then add the **Certificate -Local Computer** snap-in.
6. In the **Certificates** console, in the navigation pane, navigate to **Trusted Root Certification Authorities\Certificates**, and then verify that the **AdatumCA** certificate exists.



**Note:** You perform the above steps to import the AdatumCA certificate into Trusted Root Certification Authorities of **LON-CL1**, and then to verify that the AdatumCA certificate is imported into Trusted Root Certification Authorities of **LON-CL1**. This enables the client to trust the certificates issued by the Adatum Certification Authority.

### 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** field, type **http://lon-svr1.adatum.com**, and then press Enter. Notice that a Network Error message displays.
6. Open the **Remote Desktop Connection** app, and try to connect to **LON-DC1**. Notice that you cannot connect to **LON-DC1**, because the computer cannot be found on the network.
7. Close all open windows.



**Note:** You are unable to open the internal web site running on **LON-SVR1** and connect to **LON-DC1** using Remote Desktop because the client cannot access the internal network.

### ► Task 3: Install the Web Application Proxy role service

#### Install the Web Application Proxy role service

1. Switch to **EU-RTR**.
2. Open **Server Manager**, and then, on the **Dashboard** page, click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, on the **Select server roles** page, expand **Remote Access**, and then click **Web Application Proxy**.
4. Click **Next**, and then complete the install.

### ► Task 4: Configure access to an internal website

#### Obtain a certificate for the ADFS WAP farm


- Open the **MMC**, add the **Certificates - Computer account** snap-in, and then request a new certificate with the following settings:
  - Subject Name: **Common Name adfswap.adatum.com**
  - Alternative name: **DNS adfswap.adatum.com, lon-svr1.adatum.com, rdgw.adatum.com**

#### Configure Web Application Proxy

1. From **Server Manager**, open the **Remote Access Management** console.
2. In the navigation pane, click **Web Application Proxy**, and then run the **Web Application Proxy Configuration Wizard**.
3. In the **Web Application Proxy Configuration Wizard**, for **Federation service name**, type **adfswap.adatum.com**.
4. In the **User name** and **Password** boxes, type **Administrator** and **Pa\$\$w0rd**.



5. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, click **adfsweb.adatum.com**.
6. On the **Results** page, verify that the configuration was successful, and then close the wizard.

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

### **Publish an internal website**

1. On the Web Application Proxy server, in the **Remote Access Management** console, in the navigation pane, start the **Publish New Application Wizard**.
2. On the **Preauthentication** page, click **Pass-through**.
3. In the **Name** box, type **Adatum LOB Web App (LON-SVR1)**.
4. In the **External URL** box, type **https://lon-svr1.adatum.com**.
5. In the **External certificate** list, click **adfsweb.adatum.com**.
6. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed.

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

7. On the **Confirmation** page, review the settings, and then click **Publish**.
8. On the **Results** page, ensure that the application published successfully, and then click **Close**.

### **Configure internal website authentication**

1. Switch to **LON-SVR1**.
2. From **Server Manager**, open the **Internet Information Services (IIS) Manager** console.
3. In the **Internet Information Services (IIS) Manager** console, navigate to **Default Web Site**.
4. Configure **Authentication** for the **Default Web Site** with following settings:
  - o Windows Authentication: **Enabled**
  - o Anonymous Authentication: **Disabled**
5. Close the **Internet Information Services (IIS) Manager** console.

### **► Task 5: Configure access to Remote Desktop Gateway**

#### **Install Remote Desktop Gateway**

1. Switch to **LON-SVR2**.
2. Open **Server Manager**, and then, on the **Dashboard** page, click **Add roles and features**.
3. Click **Next** three times.
4. On the **Select Server roles** page, click **Remote Desktop Services**, and then click **Next** three times.
5. On the **Select role services** page, click **Remote Desktop Gateway**, and then click **Next** four times.
6. On the **Confirm installation selections** page, click **Install** and then click **Close**.

## Obtain a certificate for Remote Desktop Gateway server

1. Open the **MMC**, add the **Certificates - Computer account** snap-in, and then request a new certificate with the following setting:
  - o Subject Name: **Common Name rdgw.adatum.com**

## Configure Remote Desktop Gateway server

1. Open **Remote Desktop Gateway Manager** and then, in the **RD Gateway Manager**, click **LON-SVR2 (Local)**.
2. Click the **View or modify certificate properties link**, and then click the **SSL Certificate** tab in the **LON-SVR2 Properties** dialog box. Then click **Import Certificate**.
3. In the **Import Certificate** dialog box, click the **rdgw.adatum.com** certificate, and then click **Import**. Verify that information about the certificate is now listed on the **SSL Certificate** tab.
4. Click the **SSL Bridging** tab, and then click **Use SSL Bridging**. Then click **OK** and, when prompted by RD Gateway, click **Yes**.
5. In the **RD Gateway Manager**, expand **LON-SVR2 (Local)**, right-click **Policies**, and then click **Create New Authorization Policies**.
6. On the **Create Authorization Policies for RD Gateway** page, click **Next**.



**Note:** An RD CAP allows you to select the users that can connect to a remote computer using the RD Gateway server.

7. On the **Create an RD CAP** page, type **Adatum Admins**, and then click **Next**.
8. On the **Select Requirements** page, in the **User group membership (required)** section, click **Add Group**.
9. Type **Domain admins**, click **Check Names** and then click **OK**. On the **Select Requirements** page, click **Next**.
10. On the **Enable or Disable Device Redirection** page, click **Disable device redirection for the following client device types**, and then click **Next**.
11. On the **Set Session Timeout** page, click **Enable idle timeout**, and then, in the value field, type **15**. Then click **Next**.
12. On the **RD CAP Settings Summary** page, verify your selections, and then click **Next**.



**Note:** An RD RAP allows you to select the network resources that users can connect to remotely using the RD Gateway server.

13. On the **Create an RD RAP** page, type **Adatum admins – allow access to all computers**, and then click **Next**.
14. On the **Select User Groups** page, verify that **ADATUM\Domain Admins** displays under **User group membership (required)**, and then click **Next**.
15. On the **Select Network Resources** page, click **Allow users to connect to any network resource (computer)**, and then click **Next**.
16. On the **Select Allowed Ports**, click **Next**.

17. On the **RD RAP Settings Summary** page, verify your selection, and then click **Finish**.
18. On the **Confirm Creation of Authorization Policies**, click **Close**.

### **Publish the Remote Desktop Gateway Server**

1. Switch to **EU-RTR**.
2. On the Web Application Proxy server, in the **Remote Access Management** console, in the navigation pane, start the **Publish New Application Wizard**.
3. On the **Preauthentication** page, click **Pass-through**.
4. In the **Name** box, type **Adatum LOB Web App (LON-SVR1)**.
5. In the **External URL** box, type **https://rdgw.adatum.com**.
6. In the **External certificate** list, click **adfsweb.adatum.com**.
7. In the **Backend server URL** box, ensure that **https://rdgw.adatum.com** is listed.



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

8. On the **Confirmation** page, review the settings, and then click **Publish**.
9. On the **Results** page, ensure that the application published successfully, and then click **Close**.

**Results:** After completing this exercise, you should have successfully implemented Web Application Proxy.

## **Exercise 2: Validating the Web Application Proxy deployment**

### **Scenario**

Now that you have deployed the Web Application Proxy role service, you need to verify that external users can access the internal application through the proxy.

The main tasks for this exercise are as follows:


1. Verify access to the internal website from the client computer.
2. Verify access to the internal Remote Desktop Gateway Server and remote desktop access to **LON-DC1**.
3. Prepare for the next module.

#### **► Task 1: Verify access to the internal website from the client computer**


1. Switch to **LON-CL1**, open Microsoft Edge, and then type the following address:  
**https://lon-svr1.adatum.com**
2. When you receive a prompt, in the **Microsoft Edge** dialog box, type **adatum\logan** for the username and **Pa\$\$w0rd** for the password, and then click **OK**.
3. Verify that the default IIS 9.0 webpage for **LON-SVR1** opens.

### ► Task 2: Verify access to the internal Remote Desktop Gateway Server and remote desktop access to LON-DC1


1. Open the **Remote Desktop Connection** app, click **Show Options**, and then click the **Advanced** tab.
2. In the drop-down box, under **If server authentication fails**, click **Connect and don't warn me**.

 **Note:** In real life, you would leave this setting at **Warn me**. However, because the certificate revocation list distribution point (CDP) is not reachable to **LON-CL1** in this lab, you change it.

3. Click **Settings**, click **Use these RD Gateway server settings**, and for the server name, type **rdgw.adatum.com**. Click **Use my RD Gateway credentials for the remote computer**. Click **OK**.

 **Note:** If you have not chosen the **Use my RD Gateway credentials for the remote computer** setting, you would have to validate twice—once for the Remote Desktop Gateway server and once for the server you are connecting to.

4. Click the **General** tab. In the **Computer** field, type **LON-DC1**, and then click **Connect**.
5. In the **Windows Security** dialog box, type **adatum\administrator** for the username and **Pa\$\$w0rd** for the password, and then click **OK**.
6. Verify that you can connect to **LON-DC1** using Remote Desktop.

 **Note:** It will take approximately 20 seconds to connect to **LON-DC1**.

**Results:** After completing this exercise, you will have verified that external users are able to access the internal application through the Web Application Proxy.

### ► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741-LON-SVR1**, **20741A-LON-SVR2**, **20741A-EU-RTR**, **20741A-INET1**, and **20741A-LON-CL1**.

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

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

## 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?

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

**Question:** What type of applications can you publish by using Web Application Proxy in Windows Server 2016?

### Tools

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

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 7

## Implementing DirectAccess

### Contents:

Module Overview	7-1
<b>Lesson 1:</b> Overview of DirectAccess	7-2
<b>Lesson 2:</b> Implementing DirectAccess by using the Getting Started Wizard	7-13
<b>Lab A:</b> Implementing DirectAccess by using the Getting Started Wizard	7-20
<b>Lesson 3:</b> Implementing and managing an advanced DirectAccess infrastructure	7-27
<b>Lab B:</b> Deploying an advanced DirectAccess solution	7-44
Module Review and Takeaways	7-55

## Module Overview

Remote access technologies in Windows Server 2016 enable users to connect securely to data and resources in corporate networks. In Windows Server 2016, four component technologies—virtual private network (VPN), DirectAccess, Routing, and Web Application Proxy—are integrated into a single, unified server role called Remote Access.

In this module, you will learn how to implement DirectAccess in Windows Server 2016. You also will learn about different implementation scenarios for small or medium-sized organizations and enterprise organizations.

### Objectives

After completing this module, you will be able to:

- Explain what is DirectAccess and how it works.
- Implement DirectAccess in Windows Server 2016 by using the Getting Started Wizard.
- Implement and manage an advanced DirectAccess infrastructure in Windows Server 2016.

## Lesson 1

# Overview of DirectAccess

You can configure and manage the Remote Access server role in Windows Server 2016 by using a single wizard. The type of remote access technology that organizations will implement depends on the organization's business requirements. Some organizations might deploy several remote access technologies on different servers, and some might deploy them on the same server. For example, organizations that need administrators to manage servers from the Internet might deploy DirectAccess, and at the same time they might deploy Web Application Proxy if they need to publish internal applications to the Internet.

DirectAccess enables remote users to securely access corporate resources such as email servers, shared folders, or internal websites, without connecting to a VPN. DirectAccess also provides increased productivity for a mobile workforce by offering the same connectivity experience both inside and outside the office. With the new unified management experience, you can configure DirectAccess and older VPN connections from one location. Other enhancements in DirectAccess include simplified deployment, and improved performance and scalability.

### Lesson Objectives

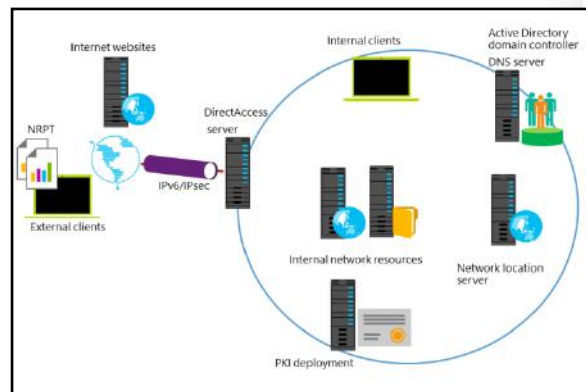
After completing this lesson, you will be able to:

- Describe the DirectAccess components in Windows Server 2016.
- Describe the DirectAccess server deployment options.
- Describe the DirectAccess Tunneling Protocol options in Windows Server 2016.
- Describe how to manage DirectAccess in Windows Server 2016.
- Explain how DirectAccess work for internal clients.
- Explain how DirectAccess work for external clients.
- Explain how to install the Remote Access server role in Windows Server 2016.

### DirectAccess components

To deploy and configure DirectAccess, your organization must support the following infrastructure components:

- DirectAccess server
- DirectAccess clients
- Network location server
- Internal resources
- An Active Directory domain
- Group Policy
- Public key infrastructure (PKI) (optional for the internal network)
- Domain Name System (DNS) server
- Network Access Protection (NAP) enforcement server (deprecated)





## DirectAccess server

The DirectAccess server can be any computer running Windows Server 2016 that you join to a domain, that accepts connections from DirectAccess clients, and that establishes communication with intranet resources. This server provides authentication services for DirectAccess clients and acts as an Internet Protocol security (IPsec) tunnel mode endpoint for external traffic. The Remote Access server role allows centralized administration, configuration, and monitoring for both DirectAccess and VPN connectivity.

The wizard-based setup simplifies DirectAccess management for small and medium-sized organizations. The wizard does so by removing the need for full PKI deployment. In Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012, the Getting Started Wizard detects the actual implementation state of the DirectAccess server, and selects the best deployment automatically. When DirectAccess clients communicate with the DirectAccess server, they use IPv6 exclusively. If you are implementing DirectAccess and using the Getting Started Wizard no IPv6 configuration or planning are not required as the underlying complexity of configuring the various IPv6 transition technologies are not shown to the administrator.

## DirectAccess clients

A DirectAccess client can be any domain-joined computer that is running an Enterprise edition of the Windows 10, Windows 8.1, Windows 8.0, or Windows 7 operating system.



**Note:** With off-premise provisioning, you can join the client computer to a domain without connecting the client computer to your internal premises.

The DirectAccess client computer connects to the DirectAccess server by using IPv6 and IPsec. If a native IPv6 network is not available, the client establishes an IPv6-over-IPv4 tunnel by using 6to4 or Teredo. Note that the user does not have to be logged on to the computer for this step to complete.

If a firewall or proxy server prevents the client computer using 6to4 or Teredo from connecting to the DirectAccess server, the client computer automatically attempts to connect by using the IP-HTTPS protocol, which uses a Secure Sockets Layer (SSL) connection to the DirectAccess server.

## Network location server

A DirectAccess client uses the network location server to determine its location. If the client computer can securely connect to the network location server by using HTTPS, then the client computer assumes it is on the intranet, and the DirectAccess policies are not enforced. If the network location server is not contactable, the client assumes it is on the Internet. The network location server installs on the DirectAccess server with the web-server role.



**Note:** You can distribute the URL for the network location server by using a Group Policy Object (GPO).

## Internal resources

You can configure any IPv6-capable application that is running on internal servers or client computers to be available for DirectAccess clients. For older applications and servers that do not have IPv6 support, such as non-Microsoft operating systems, Windows Server 2016 includes native support for protocol translation (NAT64) and a name resolution (DNS64) gateway to convert IPv6 communication from the DirectAccess client to IPv4 for the internal servers.

## Active Directory domain

You must deploy at least one Active Directory domain that is running at a minimum, Windows Server 2003 domain-functional level. DirectAccess provides integrated multiple-domain support, which allows client computers from different domains to access resources that might be located in different trusted domains.

## Group Policy

You should use Group Policy for the centralized administration and deployment of DirectAccess settings. The Getting Started Wizard creates a set of GPOs and settings for DirectAccess clients, the DirectAccess server, and selected servers.

## PKI

For simplified configuration and management, PKI deployment is optional. DirectAccess enables client authentication requests to be sent over a HTTPS-based Kerberos proxy service that is running on the DirectAccess server. This eliminates the need for establishing a second IPsec tunnel between clients and domain controllers. The Kerberos proxy will send Kerberos requests to domain controllers on behalf of the client.

However, for a full DirectAccess configuration, two-factor authentication, and force tunneling, you must implement certificates for authentication for every client that will participate in DirectAccess communication. Furthermore, PKI is required for Direct Access client computers that are running Windows 7.

## Name Resolution Policy Table (NRPT)

The NRPT is the mechanism used by the DirectAccess clients to determine which DNS server they should use to resolve the names of resources they are accessing. For internal resources, the clients will use the internal DNS servers and for resources on the Internet, they will use their locally configured DNS server.

## DNS server

When using ISATAP, you must use at least Windows Server 2008 R2, Windows Server 2008 with the Q958194 hotfix, Windows Server 2008 Service Pack 2 (SP2) or newer, or a non-Microsoft DNS server that supports DNS message exchanges over the ISATAP.

## NAP servers

NAP was deprecated in Windows Server 2012 R2 and has been removed from Windows Server 2016.



**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 server deployment options

Organizations might choose different DirectAccess server deployment options depending on their business requirements. Deployment options might vary from using the Getting Started Wizard for a simple deployment to using advanced configuration options for a more complex deployment.

### Prerequisites for deploying the DirectAccess server role

The server on which you plan to install the DirectAccess server role should meet the following prerequisites:

- Domain member. The DirectAccess server must be a domain member. You cannot deploy the DirectAccess server role on workgroup server computers.
- Network adapters. The DirectAccess server must have at least one network adapter connected to the domain network.
- Network topology. You should deploy the DirectAccess server in one of following network topologies:
  - Edge. You use this topology in organizations where firewall software is deployed on an edge computer that is running Windows Server 2016. The edge computer must have two network adapters: one network adapter that connects to the internal network and the other network adapter that connects to the Internet.
  - Behind the firewall with two network adapters. You use this topology in organizations that use an edge device as a firewall solution. In this scenario, the DirectAccess server is located in a perimeter network, behind the edge device. The DirectAccess server must have two network adapters: one network adapter that connects to the internal network and the other network adapter that connects to the perimeter network.
  - Behind the firewall with one network adapter. You use this topology in organizations that use an edge device as a firewall solution where the DirectAccess server has one network adapter connected to the internal network.
- You must enable Windows Firewall for all profiles. You should not disable Windows firewall on the DirectAccess server and the Direct Access clients, because turning off the Windows Firewall will disable DirectAccess connectivity.
- The DirectAccess server cannot be a domain controller. Deploying the DirectAccess server role on a domain controller is not supported.

- DirectAccess server Deployment options:
    - Simple deployment by using the Getting Started Wizard
    - Complex deployment by using advance configuration options
  - DirectAccess server advance deployment options:
    - Deploy multiple endpoints
    - Multiple domain support
    - Deploy a server behind a NAT device
    - Support for OTP and virtual smart cards
    - Support for NIC Teaming
    - Off-premise provisioning

### DirectAccess server advanced deployment options

DirectAccess server advanced deployment options in Windows Server 2016 include:

- Deploying multiple endpoints. When you implement DirectAccess on multiple servers in different network locations, the DirectAccess client computer selects the closest endpoint automatically if it is running Windows 10, Windows 8.1, or Windows 8. For DirectAccess client computers running Windows 7, you must specify the endpoint manually. This also works for Distributed File System (DFS) shares that are redirected to an appropriate Active Directory site.
- Multiple domain support. Organizations that have complex multiple domain infrastructure can deploy DirectAccess servers in multiple domains. In this scenario, DirectAccess client computers can connect to DirectAccess servers located in different domains.

- Deploy a DirectAccess server behind a network address translation (NAT) device. You can deploy a DirectAccess server behind a NAT device, with support for a single or multiple interfaces, which removes the prerequisite for a public address. In this configuration, only IP-HTTPS is deployed, which establishes a secure IP tunnel by using a secure HTTP connection.
- Support for one-time passwords (OTPs) and virtual smart cards. Direct Access supports OTP authentication, where users are authenticated by providing a combination of user name, password, and an OTP. This feature requires a PKI deployment. In addition, DirectAccess can use the Trusted Platform Module (TPM)-based virtual smart card, which uses the TPM of a client computer to act as a virtual smart card for two-factor authentication.
- Offload network adapters with support for Network Adapter Teaming (NIC Teaming). NIC Teaming in Windows Server 2016 is fully supported without requiring non-Microsoft drivers. This is because DirectAccess servers support NIC Teaming. This capability allows DirectAccess client computers to benefit from bandwidth aggregation on network adapters, and failover capability if one of the network adapters is not working.
- Off-premise provisioning. With the new Djoin.exe tool, you can provision a non-domain computer with an Active Directory binary large object (BLOB) so that the computer can join a domain without being connected to the internal network. After the computer is joined to the domain, it can access the intranet resources by using DirectAccess.

## DirectAccess tunneling protocol options

DirectAccess uses IPv6 and IPsec when clients connect to internal resources. However, many organizations do not have native IPv6 infrastructure. Therefore, DirectAccess uses transitioning tunneling technologies to connect IPv6 clients to IPv4 internal resources by communicating through IPv4-based computers and devices that are located on the Internet.


DirectAccess tunneling protocols include:


- ISATAP. ISATAP enables DirectAccess clients to connect to the DirectAccess server over the IPv4 networks for intranet communication. By using ISATAP, an IPv4 network emulates a logical IPv6 subnet to other ISATAP hosts, where ISATAP hosts automatically tunnel to each other for IPv6 connectivity. Windows Server 2008 and newer and Windows 7 and newer can act as ISATAP hosts. ISATAP does not need changes on IPv4 routers because IPv6 packets are tunneled within an IPv4 header. In order to use ISATAP, you have to configure DNS servers to answer ISATAP queries, and you must enable IPv6 on network hosts.
- 6to4. 6to4 enables DirectAccess clients to connect to the DirectAccess server over the IPv4-based Internet. You can use 6to4 when clients have a public IP address. IPv6 packets are encapsulated in an IPv4 header, and then are sent over the 6to4 tunnel adapter to the DirectAccess server. You can configure the 6to4 tunnel adapter for DirectAccess clients and the DirectAccess server by using a GPO. 6to4 cannot work if clients are located behind an IPv4 NAT device.


DirectAccess tunneling protocols include:

- ISATAP. Tunnels IPv6 traffic over IPv4 networks for intranet communication
- 6to4. Used by DirectAccess clients with a public IP address
- Teredo. Used by DirectAccess clients with a private IP address behind a NAT device
- IP-HTTPS. Used by DirectAccess clients if they are not able to use ISATAP, 6to4, or Teredo

- **Teredo.** Teredo enables DirectAccess clients to connect to the DirectAccess server across the IPv4 Internet, when clients are located behind an IPv4 NAT device. Before deploying Teredo, you should configure the firewall to allow outbound traffic on User Datagram Protocol (UDP) port 3544. Clients that have a private IPv4 address use Teredo to encapsulate IPv6 packets in an IPv4 header, and then send them over the IPv4-based Internet. You can configure Teredo for DirectAccess clients and the DirectAccess server by using a GPO.
- **IP-HTTPS.** IP-HTTPS enables DirectAccess clients to connect to the DirectAccess server over the IPv4-based Internet. IP-HTTPS is used by clients that are unable to connect to the DirectAccess server by using ISATAP, 6to4, or Teredo. You can configure IP-HTTPS for DirectAccess clients and the DirectAccess server by using Group Policy.

 **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

After you install the Remote Access server role on a server that is running Windows Server 2016, you can manage the role by using the Microsoft Management Console (MMC), and by using Windows PowerShell. You can use the MMC for your day-to-day tasks of managing remote access, and you can use Windows PowerShell for managing multiple servers and for scripting or automating management tasks.

There are two MMCs for managing the Remote Access server role: the Remote Access Management console, and the Routing and Remote Access console. You can access these consoles from the **Tools** menu in Server Manager.

Manage the Remote Access server role by using:

- Remote Access Management console
- Routing and Remote Access console
- Windows PowerShell:
  - **Set-DAServer**
  - **Get-DAServer**
  - **Set-RemoteAccess**
  - **Get-RemoteAccess**

### The Remote Access Management console

The Remote Access Management console allows you to manage DirectAccess, VPN, and Web Application Proxy. When you open this console for the first time, it provides you with a wizard-based setup to configure remote access settings according to your business requirements. After you configure the initial remote access settings, you will be able to configure and manage your remote access solution in these areas:

- **Configuration.** You can edit the remote access settings by using wizards and by using the graphical representation of the current network configuration in the console.
- **Dashboard.** You can monitor the overall status of servers and clients that are part of your remote access solution.

- **Operations Status.** You can access detailed information on the status of the servers that are part of your remote access solution.
- **Remote Client Status.** You can access detailed information on the status of the clients that are connecting to your remote access solution.
- **Reporting.** You can generate historical reports on different parameters, such as remote access usage, access details, connection details, and server load statistics.

### The Routing and Remote Access console

You can use the Routing and Remote Access console to configure a server running Windows Server 2016 as all of the following:

- A NAT device
- As a router for both IPv4 and IPv6 protocols
- As a VPN server

After you complete the configuration, you will be able to configure and manage your remote access solution in these areas in the console:

- **Server Status.** You can monitor the status of the Remote Access server, the ports in use, and how long the server has been operational (that is the *server uptime*).
- **Remote Access Client, Ports, Remote Access Logging.** You can monitor the client status, port status, and detailed logging information about clients that are connected to the Remote Access server.
- **IPv4.** You can configure the IPv4 settings such as NAT, IPv4 routing with static routes, and the following routing protocols: Routing Information Protocol version 2, Internet Group Management Protocol (IGMP), and the Dynamic Host Configuration Protocol (DHCP) Relay Agent.
- **IPv6.** You can configure IPv6 settings, such as IPv6 routing with static routes and the DHCP Relay Agent routing protocol.

### Windows PowerShell commands

Windows PowerShell commands in Windows Server 2016 allow you to configure remote access and create scripts for automation of some the configuration and management procedures. Some examples of Windows PowerShell commands for remote access include:

- **Set-DAServer.** This command sets the properties specific to the DirectAccess server.
- **Get-DAServer.** This command to display the properties of the DirectAccess server.
- **Set-RemoteAccess.** This command modifies the configuration that is common to both DirectAccess and VPN, such as SSL certificate, internal interface, and Internet interface.
- **Get-RemoteAccess.** This command displays the configuration of DirectAccess and VPN (both Remote Access VPN and site-to-site VPN).

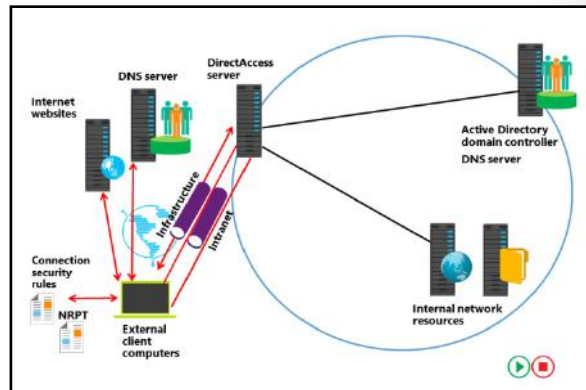


**Additional Reading:** For a complete list of remote access cmdlets in Windows PowerShell, refer to: "Remote Access Cmdlets" at <http://aka.ms/Ar09tz>



## How DirectAccess works for external clients

When a DirectAccess client cannot reach the URL address specified for the network location server, the DirectAccess client assumes that it is not connected to the intranet and that it is located on the Internet. When the client computer cannot communicate with the network location server, it starts to use NRPT and connection security rules. The NRPT has DirectAccess-based rules for name resolution, and connection security rules define DirectAccess IPsec tunnels for communication with intranet resources.



Internet-connected DirectAccess clients use the following process to connect to intranet resources.

1. The DirectAccess client attempts to access the network location server.
2. The client attempts to locate a domain controller.
3. The client first attempts to access intranet resources, and then attempts to access Internet resources.

### DirectAccess client attempts to access the network location server

The DirectAccess clients attempt to access the network location server as follows:

1. The client tries to resolve the FQDN of the network location server URL. Because the FQDN of the network location server URL corresponds to an exemption rule in the NRPT, the DirectAccess client does not send the DNS query to a locally configured DNS server (an Internet-based DNS server). An external Internet-based DNS server would not be able to resolve the name.
2. The DirectAccess client processes the name resolution request as defined in the DirectAccess exemption rules in the NRPT.
3. Because the network location server is not found on the same network where the DirectAccess client is currently located, the DirectAccess client applies a public or private firewall network profile to the attached network.
4. The Connection Security tunnel rules for DirectAccess, which are scoped for the public and private profiles, provide the public or private firewall network profile.

The DirectAccess client uses a combination of NRPT rules and connection security rules to locate and access intranet resources across the Internet through the DirectAccess server.

### DirectAccess client attempts to locate a domain controller

After starting up and determining its network location, the DirectAccess client attempts to locate and sign in to a domain controller. This process creates either an IPsec tunnel or an infrastructure tunnel to the DirectAccess server by using the IPsec tunnel mode and encapsulating security payload (ESP). The process is as follows:

1. The DNS name for the domain controller matches the intranet server namespace rule in the NRPT, which specifies the IPv6 address of the intranet DNS server. The DNS client service constructs the DNS name query that is addressed to the IPv6 address of the intranet DNS server, and forwards it to the DirectAccess client's TCP/IP stack for sending.
2. Before sending the packet, the TCP/IP stack determines whether there are Windows Firewall outgoing rules or connection security rules for the packet.



3. Because the destination IPv6 address in the DNS name query matches a connection security rule that corresponds with the infrastructure tunnel, the DirectAccess client uses Authenticated IP (AuthIP) and IPsec to negotiate and authenticate an encrypted IPsec tunnel to the DirectAccess server. The DirectAccess client (both the computer and the user) authenticates itself with its installed computer certificate and its NTLM credentials, respectively.



**Note:** AuthIP enhances authentication in IPsec by adding support for user-based authentication with Kerberos version 5 (v5) or SSL certificates. AuthIP also supports efficient protocol negotiation and usage of multiple sets of credentials for authentication.



**Note:** DirectAccess client computers that are running Windows 7 must have computer certificates issued. However, client computers running Windows 10, Windows 8.1, or Windows 8 support AuthIP, and do not require computer certificates to connect to the DirectAccess server.

4. The DirectAccess client sends the DNS name query through the IPsec infrastructure tunnel to the DirectAccess server.
5. The DirectAccess server forwards the DNS name query to the intranet DNS server. The DNS name query response is sent back to the DirectAccess server and back through the IPsec infrastructure tunnel to the DirectAccess client.

When the user on the DirectAccess client signs in, the domain sign-in traffic goes through the IPsec infrastructure tunnel.

### **DirectAccess client attempts to access intranet resources**

The first time that the DirectAccess client sends traffic to an intranet location that is not on the list of destinations for the infrastructure tunnel (such as an email server), the following process occurs:

1. The application or process that attempts to communicate constructs a message or payload, and transfers it to the TCP/IP stack for sending.
2. Before sending the packet, the TCP/IP stack determines whether there are Windows Firewall outgoing rules or connection security rules for the packet.
3. Because the destination IPv6 address matches the connection security rule that corresponds with the intranet tunnel (which specifies the IPv6 address space of the entire intranet), the DirectAccess client uses AuthIP and IPsec to negotiate and authenticate an additional IPsec tunnel to the DirectAccess server. The DirectAccess client authenticates itself with its installed computer certificate and with the user account's Kerberos credentials.
4. The DirectAccess client sends the packet through the intranet tunnel to the DirectAccess server.
5. The DirectAccess server forwards the packet to the intranet resources. The response is sent back to the DirectAccess server and back through the intranet tunnel to the DirectAccess client.

Any subsequent intranet access traffic that does not match an intranet destination in the infrastructure tunnel connection security rule must go through the intranet tunnel.

### **DirectAccess client attempts to access internet resources**

When the user or a process on the DirectAccess client attempts to access an Internet resource (such as an Internet web server), the following process occurs:

1. The DNS client service passes the DNS name for the Internet resource through the NRPT. There are no matches, so the DNS client service constructs the DNS name query that is addressed to the IP address of an interface-configured Internet DNS server, and transfers it to the TCP/IP stack for sending.

2. Before sending the packet, the TCP/IP stack determines whether there are Windows Firewall outgoing rules or connection security rules for the packet.
3. Because the destination IP address in the DNS name query does not match the connection security rules for the tunnels to the DirectAccess server, the DirectAccess client sends the DNS name query normally.
4. The Internet DNS server responds with the IP address of the Internet resource.
5. The user application or process constructs the first packet to send to the Internet resource. Before sending the packet, the TCP/IP stack determines whether there are Windows Firewall outgoing rules or connection security rules for the packet.
6. Because the destination IP address in the DNS name query does not match the connection security rules for the tunnels to the DirectAccess server, the DirectAccess client sends the packet normally.

Any subsequent Internet resource traffic that does not match a destination in either the infrastructure intranet tunnel or the connection security rules is sent and received normally.

The process of accessing the domain controller and intranet resources is very similar to the connection process, because both of these processes use NRPT to locate the appropriate DNS server to resolve the name queries. However, the main difference is in the IPsec tunnel that is established between the client and DirectAccess server. When accessing the domain controller, all the DNS queries are sent through the IPsec infrastructure tunnel, and when accessing intranet resources, a second IPsec tunnel is established to access intranet resources.

## Demonstration: Installing the Remote Access server role

In this demonstration, you will learn how to install the Remote Access server role.

### Demonstration Steps

#### Install the Remote Access server role

1. On **LON-SVR1**, switch to the **Server Manager** console, click **Manage**, and then start the **Add Roles and Features Wizard**.
2. Complete the wizard by using the following steps:
  - a. On the **Before You Begin** page, click **Next**.
  - b. On the **Select installation type** page, click **Next**.
  - c. On the **Select destination server** page, click **Next**.
  - d. On the **Select server roles**, click **Remote Access**, and then click **Next**.
  - e. On the **Select features** page, click **Next**.
  - f. On the **Remote Access** page, click **Next**.
  - g. On the **Select role services** page, click **DirectAccess and VPN (RAS)**.
  - h. In the **Add Roles and Features Wizard** dialog box, click **Add Features**.
  - i. On the **Select role services** page, click **Next**.
  - j. On the **Confirm installation selection** page, click **Install**.
3. When installation completes, click **Close**.

## Lesson 2

# Implementing DirectAccess by using the Getting Started Wizard

The DirectAccess feature in Windows Server 2016 provides users with remote access to intranet resources without first establishing a user-initiated VPN connection. The DirectAccess feature also ensures connectivity to the application infrastructure for both internal and remote users.

Unlike traditional VPNs that require user intervention to initiate a connection to an intranet, DirectAccess enables any application that supports IPv6 on the client computer to have complete access to intranet resources. DirectAccess also enables you to specify resources and client-side applications that are restricted for remote access.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe how to run the Getting Started Wizard.
- Describe the configuration changes that the Getting Started Wizard makes so that DirectAccess clients can connect to the intranet.
- Identify the Getting Started Wizard settings.
- Describe the limitations of deploying DirectAccess by using the Getting Started Wizard.

### Demonstration: Running the Getting Started Wizard

In this demonstration, you will learn how to configure DirectAccess by running the Getting Started Wizard.

#### Demonstration Steps

##### Create a security group for DirectAccess client computers

1. On **LON-DC1**, open the **Active Directory Users and Computers** console, and create an organizational unit named **Special Accounts**.
2. Inside that organizational unit, create a **Global Security** group named **DirectAccessClients**.
3. Add **LON-CL1** to the **DirectAccessClients** security group.
4. Close the **Active Directory Users and Computers** console.

##### Configure DirectAccess by running the Getting Started Wizard

1. Switch to **EU-RTR**.
2. On **EU-RTR**, in the **Server Manager** console, click **Remote Access Management**.
3. In the **Remote Access Management** console, under **Configuration**, click **DirectAccess and VPN**.
4. Complete the **Run the Getting Started Wizard** by using the following settings:
  - a. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
  - b. Verify that **Edge** is selected, and then in the **Type the public name or IPv4 address used by clients to connect to Remote Access server** text box, type **131.107.0.10**.
  - c. On the **Remote Access Review** page, click the **here** link.

- d. Change **remote clients** to **DirectAccess Clients**.
  - e. Clear the **Enable DirectAccess for mobile computers only** check box.
  - f. For **Helpdesk email address**, type **DAHelp@adatum.com**.
  - g. For **DirectAccess connection name**, type **A. Datum DirectAccess**.
5. Close the **Applying Getting Started Wizard Settings** dialog box.

## Getting Started Wizard configuration changes

The Getting Started Wizard makes multiple configuration changes so that DirectAccess clients can connect to the intranet. These changes include:

- GPO settings. Two GPOs, DirectAccess Server Settings and DirectAccess Client Settings, are created in order to define which computers will be DirectAccess servers and which computers will be DirectAccess clients:
  - DirectAccess Server Settings GPO. This GPO defines the settings that will apply to the DirectAccess servers. These settings include:
    - Global Settings. These settings define the IPsec Internet Control Message Protocol (ICMP) that will be allowed through the local firewall on the DirectAccess server.
    - Inbound Rules. These rules define inbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls. Inbound rules also allow traffic to the DNS64 server that is deployed on the Remote Access server.
    - Connection Security Settings. These settings define the IPv6 address prefixes and the Kerberos authentication settings.
  - The DirectAccess Client Settings GPO. This GPO defines the settings that will apply to the DirectAccess clients. These settings include:
    - Public Key Policies/Trusted Root Certification Authorities. This setting configures DirectAccess client computers to trust the self-signed certificates that the DirectAccess server issues.
    - Global Settings. These settings define the IPsec ICMP protocol that will be allowed through the local firewall on the DirectAccess clients.
    - Outbound Rules. These rules define the outbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
    - Connection Security Settings. These settings define the IPv6 address prefixes and the Kerberos authentication settings.
- DNS server settings. In the **DNS Manager** console, under **Forward Lookup Zones**, the **Getting Started Wizard** creates A and AAAA records for the following hosts: directaccess-corpConnectivityHost, DirectAccess-NLS, and directaccess-WebProbeHost.

Changes made by the Getting Started Wizard include:


- GPO settings:
  - DirectAccess Server Settings GPO
  - DirectAccess Client Settings GPO
  - It is not supported to manually edit the GPOs
- DNS server settings
- Remote clients
- Remote access server
- Infrastructure servers

- Remote clients. In the Getting Started Wizard, you can configure the following DirectAccess settings for client computers:
  - **Select groups.** You use this setting to select which groups of client computers will be configured for DirectAccess. By default, the Domain Computers group will be configured for DirectAccess. However, you can edit this setting and replace the Domain Computers group with a custom security group.
  - **Enable DirectAccess for mobile computers only.** If this setting is enabled, a WMI filter will be created and configured for the DirectAccess Client GPO. This means that DirectAccess will only be enabled for mobile computers. If you disable this setting the DirectAccess Client GPO will apply to all computers in the specified security groups.
  - **Network Connectivity Assistant.** Network Connectivity Assistant runs on every client computer and provides DirectAccess connectivity information, diagnostics, and remediation support.
  - **Resources that validate connectivity to internal network.** DirectAccess client computers need information that will help them decide whether they are located on the intranet or Internet. Therefore, they will contact resources that you provide in this Getting Started Wizard. You can provide a URL that the HTTP request will access, or a FQDN that will be contacted by a **ping** command. By default, this setting is not configured.
  - **Helpdesk email address.** By default, the helpdesk email address is not configured. The user uses the email address to send in DirectAccess log files in case of a problem. If you do not specify an email address, the **Collect Logs** button will not be available to users. We highly recommend that you always specify a helpdesk email address.
  - **DirectAccess connection name.** The default name is **Workplace Connection**.
  - **Allow DirectAccess clients to use local name resolution.** When this setting is enabled, the end user can select to use the computers' own configured DNS server for name resolution and bypass the NRPT. This setting is disabled by default.
- Remote access server. In the Getting Started Wizard, you define the network topology where the DirectAccess server is located:
  - On an edge of the internal corporate network, where the edge server has two network adapters.
  - On a server located behind an edge device, where the server has two network adapters.
  - On a server located behind an edge device, where the server has one network adapter.

In the wizard one of the preceding settings will be selected already. In addition, the public name or IPv4 address where DirectAccess clients connect from the Internet will also be in the wizard already.

You also can define the network adapter to which the DirectAccess clients connect, in addition to the certificates that the IP-HTTPS connections use.

- Infrastructure servers. In the Getting Started Wizard, you define infrastructure servers. DirectAccess clients connect to these servers before they connect to internal corporate resources. By default, two entries are configured: the domain name suffix, and DirectAccess-NLS name followed by the domain name suffix. For example, if the domain name is contoso.com, then following entries are configured: contoso.com and DirectAccess-NLS.contoso.com.

 **Note:** Changes to the DirectAccess configuration can be made by using either Windows PowerShell commands, or the **Remote Access Management** console. Manually editing the two GPOs created by DirectAccess setup is not supported.



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

## Demonstration: Identifying the Getting Started Wizard settings

In this demonstration, you will learn how to identify the changes that are made in DirectAccess by the Getting Started Wizard

### Demonstration Steps

#### Review the configuration changes in the Remote Access Management console

1. On **EU-RTR**, switch to the **Remote Access Management** console.
2. In the **Remote Access Setup** window, under the image of the client computer labeled **Step 1 Remote Clients**, click **Edit** to display the **DirectAccess Client Setup** window.
3. Record the default settings of the following items in the menu on the left, and then close the window without saving any changes:
  - o **Deployment Scenario**
  - o **Select Groups**
  - o **Network Connectivity Assistant**
4. In the **Remote Access Setup** window, under the image of the client computer labeled **Step 2 Remote Access Servers**, click **Edit** to display the **Remote Access Server Setup** window.
5. Record the default settings of the following items in the menu on the left, and then close the window without saving any changes:
  - o **Network Topology**
  - o **Network Adapters**
  - o **Authentication**
6. In the **Remote Access Setup** window, under the image of the client computer labeled as **Step 3 Infrastructure Servers**, click **Edit** to display the **Infrastructure Server Setup** window.
7. Review the default settings of the following items in the menu on the left, and then close the window without saving any changes:
  - o **Network Location Server**
  - o **DNS**
  - o **DNS Suffix Search List**
  - o **Management**
8. In the **Remote Access Setup** window, under the image of the client computer labeled as **Step 4 Application Servers**, click **Edit** to display the **DirectAccess Application Server Setup** window.
9. Review the default settings for all items, and then close the window without saving any changes.
10. Close all open windows.

## Review the infrastructure changes in the Group Policy Management Console

1. On **EU-RTR**, in **Server Manager**, open the **Group Policy Management** Console.
2. In the **Group Policy Management Console**, notice that two new GPOs are created:
  - o **DirectAccess Client Settings**
  - o **DirectAccess Server Settings**
3. Review the **DirectAccess Server Settings GPO** settings.
4. In the details pane, under **Computer Configuration (Enabled)**, review the **Windows Firewall with Advanced Security** settings. Notice that there are three groups of firewall settings configured for DirectAccess clients:
  - o **Global Settings**
  - o **Inbound Rules**
  - o **Connection Security Settings**
5. In the **Global Settings** firewall settings, review the **IPsec ICMP** exception setting.
6. In the **Inbound Rules** firewall settings, review the following rule configurations:
  - o **Core Networking – IP-HTTPS (TCP-In)**. This rule allows the inbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
  - o **Domain Name Server (UDP-In)** and **Domain Name Server (TCP-In)**. These rules allow traffic to the DNS64 server that is deployed on the Remote Access server. Notice the IPv6 address in the rules. This is the address of the London\_Network adapter on EU-RTR.
7. In the **Connection Security Settings** row, review the following rule configuration:
  - o **DirectAccess Policy-DaServerToCorpSimplified**. Review the IPv6 address prefixes and compare them with the IPv6 address prefixes that you recorded in step 6 of the previous section in this demonstration. Notice that they are the same prefixes that you configured with the Getting Started Wizard.
8. Under **Connection Security Settings**, review the **First Authentication**, **Second Authentication**, **Key Exchange (Main Mode)**, and **Data Protection (Quick Mode)** configurations.
9. In the navigation pane, select the **DirectAccess Client Settings** GPO, and then click the **Settings** tab.
10. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, review the **Public Key Policies/Trusted Root Certification Authorities** configuration.
11. Notice that the GPO is configuring the DirectAccess client computers to trust the self-signed certificates 131.107.0.10 and DirectAccess-NLS.Adatum.com that are issued by **EU-RTR**.
12. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, review the **Windows Firewall with Advanced Security** settings.
13. Notice that there are three groups of firewall settings configured for the DirectAccess clients:
  - o **Global Settings**
  - o **Outbound Rules**
  - o **Connection Security Settings**
14. In the **Global Settings** row, review the **IPsec ICMP** exception setting.

15. In the **Outbound Rules** row, review the following setting:
  - **Core Networking – IP-HTTPS (TCP-Out)**. This rule allows the outbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
16. In the **Connection Security Settings** row, review the three rules, and then compare the IPv6 address prefixes with the IPv6 address prefixes that you recorded in step 6 of the previous section in this demonstration. Notice that they are the same prefixes that you configured with the **Getting Started Wizard**.
17. Under the **Connection Security Settings** row, in the **First Authentication** row, review the **Kerberos authentication** setting.
18. Repeat step 17 for rows **Second Authentication, Key Exchange (Main Mode)**, and **Data Protection (Quick Mode)**.
19. Close the **Group Policy Management Console**.
20. On **LON-DC1**, in **Server Manager**, open the **DNS Manager** console.
21. In the **DNS Manager** console, in the **Adatum.com forward lookup** zone, notice the A and AAAA records for the following hosts:
  - **directaccess-corpConnectivityHost**
  - **DirectAccess-NLS**
  - **directaccess-WebProbeHost**.

These records are created by the **Getting Started Wizard**.

## Limitations of deploying DirectAccess by using the Getting Started Wizard

The Getting Started Wizard is simpler to implement, but it is not suitable for large deployments that need to support multiple site access, that require a highly available infrastructure, or that require support for computers running Windows 7 in a DirectAccess scenario.

### Self-signed certificates

The Getting Started Wizard creates a self-signed certificate to enable SSL connections to the DirectAccess and network location servers. For DirectAccess to function, you need to ensure that the CRL distribution point for both certificates is available externally. In addition, you cannot use the self-signed certificate in multiple site deployments or with two-factor authentication.

- **Certificates:**
  - Creates self-signed certificates that cannot be used in multisite deployments or with two-factor authentication
  - Needs you to ensure that the CRL distribution point for both certificates is available externally
- **Network location server design:**
  - Deploys the network location server on the same server as the DirectAccess server
- **Windows client operating system support:**
  - The Getting Started Wizard configuration is applicable for clients running: Windows 10, Windows 8.1 or Windows 8 or Windows Server 2016, Windows Server 2012 R2, or Windows Server 2016
  - Windows 7 clients require a client certificate for IPsec authentication



**Note:** The certificate revocation list contains all revoked certificates and reasons for revocation.



Because of these limitations, most organizations either configure a public certificate for the DirectAccess server and the network location server, or provide certificates generated by an internal CA. Organizations that have implemented an internal CA can use the web server certificate template to issue certificates to the DirectAccess server and the network location server. The organizations also must ensure that CRL distribution points are accessible from the Internet.

### Network location server design

The network location server is a critical part of a DirectAccess deployment. The Getting Started Wizard deploys the network location server on the same server as the DirectAccess server. If DirectAccess client computers on the intranet cannot successfully locate and access the secure Web page on the network location server, they might not be able to access intranet resources. When DirectAccess clients obtain a physical connection to the intranet or experience a network status change on the intranet (such as an address change when roaming between subnets), they attempt an HTTPS connection to the network location server URL. If the client can establish an HTTPS connection to network location server and check the revocation status for the Web server's certificate, the client determines that it is on the intranet. As a result, the NRPT will be disabled on the client, and Windows Firewall will be configured to use the Domain profile with no IPsec tunnels.

You need to deploy the network location server on a highly available, high-capacity intranet Web server. Larger companies will consider implementing the network location server either on a Network Load Balancing (NLB) cluster, or by using external hardware balancer.

### Support for Windows 7

The Getting Started Wizard configures the Remote Access server role to act as a Kerberos proxy to perform IPsec authentication without requiring certificates. Client authentication requests are sent to a Kerberos proxy service running on the DirectAccess server. The Kerberos proxy then sends Kerberos requests to domain controllers on behalf of the client. This configuration is only applicable for clients running the following operating systems: Windows 10, Windows 8.1 or Windows 8 client operating system or the Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012. If Windows 7 clients need to be supported for DirectAccess, you must deploy a PKI to issue computer certificates for backward compatibility.

### Check Your Knowledge

Question	
How many GPOs does the Getting Started Wizard create?	
Select the correct answer.	
<input type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5

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

# Lab A: Implementing DirectAccess by using the Getting Started Wizard

## Scenario

Many users at A. Datum Corporation work from outside the organization. This includes mobile users and people who work from home. These users currently connect to the internal network by using a non-Microsoft VPN solution. The security department is concerned about the security of the external connections and wants to ensure that the connections are as secure as possible. The support team wants to minimize the number of support calls related to remote access, and would like to have more options for managing remote computers.

IT management at A. Datum is considering deploying DirectAccess as the remote access solution for the organization. As an initial proof of concept deployment, management has requested that you configure a simple DirectAccess environment that client computers running Windows 10 can use.

## Objectives

After completing this lab, you should be able to:

- Verify that the infrastructure is ready for the DirectAccess deployment.
- Run the Getting Started Wizard.
- Validate the DirectAccess deployment.

## Lab Setup

Estimated Time: **45 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Virtual machine: **20741A-INET1**

User name: **Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, on the **Start** screen, click **Hyper-V Manager**.
2. In Microsoft Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-EU-RTR**, and **20741A-LON-CL1**.
6. In Hyper-V Manager, click **20741A-INET1**, and in the **Actions** pane, click **Start**.
7. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.

8. Sign in using the following credentials:
  - o User name: **Administrator**
  - o Password: **Pa\$\$w0rd**



**Note:** You may not be able to connect to the internal file share or the internal Web site since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

## Exercise 1: Verifying readiness for a DirectAccess deployment

### Scenario

Before you deploy DirectAccess, you need to ensure that the infrastructure is ready for the deployment.

The main tasks for this exercise are as follows:

1. Document the network configuration.
2. Verify the server readiness for DirectAccess.

### ► Task 1: Document the network configuration

#### Verify the IP address on LON-DC1

1. Switch to **LON-DC1**.
2. Open **Control Panel**.
3. Open the **Ethernet Properties** dialog box.
4. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.
5. Document the current IP address, subnet mask, default gateway, and DNS configuration.

#### Verify the network configuration on EU-RTR

1. Switch to **EU-RTR**.
2. Open **Server Manager**, and then from the **Tools** menu, open **Routing and Remote Access**.
3. In the **Routing and Remote Access** console, disable the **Microsoft Routing and Remote Access Service (RRAS)**.



**Note:** Routing and Remote Access is preconfigured on the virtual machine for the purpose of other labs in this course. The DirectAccess configuration in this lab will not work properly if you leave Routing and Remote Access enabled on the virtual machine.

4. Right-click **Start**, and then click **Network Connections**.
5. In the **Network Connections** window, verify that the following four network adapters display: **London\_Network**, **NA\_WAN**, **PAC\_WAN**, and **Internet**.
6. In the **Network Connections** window, disable and then enable the **London\_Network** adapter.
7. Repeat step 6 for the following network connections: **Internet**, **NA\_WAN**, and **PAC\_WAN**.
8. Verify that the **London\_Network** adapter is connected to the domain network **Adatum.com**.
9. Open the **London\_Network Properties** dialog box.
10. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.

11. Verify that the IP address corresponds with the subnet used in the domain network. (The IP address should be **172.16.0.1**.) and then cancel the **Properties** dialog boxes.
12. Open the **Internet Properties** dialog box.
13. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.
14. Verify that IP address corresponds with the subnet used to simulate internet connectivity. (The IP address should be **131.107.0.10**.)
15. Click **Cancel** twice, and then close the **Network Connections** window.



**Note:** If you notice that the Internet network adapter is connected to Adatum.com, disable RRAS. This is because for DirectAccess, you will need at least one adapter to be on the external network.

### Verify the network configuration on LON-CL1

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **Network Connections**.
3. Verify that the **London\_Network** adapter is connected to domain network **Adatum.com**.
4. Open the **London\_Network Properties** dialog box.
5. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration.

### Verify the network configuration on LON-SVR1

1. Switch to **LON-SVR1**.
2. Right-click **Start**, and then click **Network Connections**.
3. Verify that the **Ethernet** adapter is connected to the domain network **Adatum.com**.
4. Open the **Ethernet Properties** dialog box.
5. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration.

### Verify the network configuration on INET1

1. Switch to **INET1**.
2. Open Control Panel.
3. Under **Network and Internet**, click **View network status and tasks**.
4. Verify that the **Ethernet** adapter is connected to **Public network**.
5. Open the **Ethernet Properties** dialog box.
6. Open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.
7. Document the current IP address, subnet mask, default gateway, and DNS configuration.



**Note:** The **INET1** server will have the IP address of 131.107.0.100, which simulates the Internet DNS server.

► **Task 2: Verify the server readiness for DirectAccess**

1. On **LON-DC1**, from **Server Manager**, open the **Active Directory Users and Computers** console, and create an organizational unit named **Special Accounts**.
2. Inside that organizational unit, create a Global Security group named **DirectAccessClients**.
3. Add **LON-CL1** to the **DirectAccessClients** security group.
4. Close the **Active Directory Users and Computers** console.

**Results:** After completing this exercise, you should have successfully verified the readiness for DirectAccess deployment.

## Exercise 2: Configuring DirectAccess

### Scenario

You have verified that the infrastructure is ready for the DirectAccess deployment. A colleague has already installed the Remote Access role on EU-RTR. You now need to configure DirectAccess on the DirectAccess server by using the Getting Started Wizard.

The main task for this exercise is as follows:

1. Configure DirectAccess by using the Getting Started Wizard.

► **Task 1: Configure DirectAccess by using the Getting Started Wizard**

1. Switch to **EU-RTR**.
2. On **EU-RTR**, in the **Server Manager** console, click **Remote Access Management**.
3. In the **Remote Access Management** console, under **Configuration**, click **DirectAccess and VPN**.
4. Complete the **Run the Getting Started Wizard** with the following settings:
  - a. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
  - b. Verify that **Edge** is selected, and in the **Type the public name or IPv4 address used by clients to connect to Remote Access server** text box, type **131.107.0.10** and click **Next**.
  - c. On the **Remote Access Review** page, click the **here** link.
  - d. Change **remote clients** to **DirectAccess Clients**.
  - e. Clear the **Enable DirectAccess for mobile computers only** check box.
  - f. In the **Helpdesk email address** text box, type **DAHelp@adatum.com**.
  - g. In the **DirectAccess connection name** text box, type **A. Datum DirectAccess**.
5. Close the **Applying Getting Started Wizard Settings** dialog box.

**Results:** After completing this exercise, you should have successfully configured DirectAccess by using the **Getting Started Wizard**.

## Exercise 3: Validating the DirectAccess deployment

### Scenario

Now that you have configured DirectAccess, you need to verify that DirectAccess is working. You will start by verifying the changes made by the Getting Started Wizard, and then you will verify that client computers can access the internal network by using DirectAccess.

The main tasks for this exercise are as follows:

1. Verify the GPO deployment.
2. Test DirectAccess connectivity from an internal and external client.

#### ► Task 1: Verify the GPO deployment

1. Switch to **LON-CL1**.
2. Restart **LON-CL1**.



**Note:** You must restart the **LON-CL1** machine because you added the machine account to the DirectAccess Clients security while the machine was running. In order to update the machine's security token, it must be restarted.

3. When **LON-CL1** restarts, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.
4. At the command prompt, type **gpresult /R** to verify that the **DirectAccess Client Settings GPO** is applied to the **Computer Settings**.



**Note:** If the DirectAccess Client Settings GPO is not applied, restart **LON-CL1**, and then repeat steps 2 and 3 on **LON-CL1**.

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

```
netsh name show effectivepolicy
```

Verify that following message displays: **DNS Effective Name Resolution Policy Table Settings Note: DirectAccess settings are inactive when this computer is inside a corporate network.**

6. Close all open windows.

#### ► Task 2: Test DirectAccess connectivity from an internal and external client



**Note:** You may not be able to connect to the internal file share or the internal Web site since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

### Verify connectivity to internal network resources

1. Switch to **LON-CL1**.
2. On **LON-CL1**, from the taskbar, open Microsoft Internet Explorer.
3. In the Internet Explorer Address bar, type **http://lon-svr1.adatum.com**, and then press Enter.
4. Verify that the default IIS 9.0 webpage for **LON-SVR1** displays.
5. Leave the **Internet Explorer** window open.

6. On the **Start** screen, type `\\LON-SVR1\Corpdata`, and then press Enter. Note that you are able to access the folder content.
7. Close all open windows.
8. Open a command prompt, and then type `ipconfig`.



**Note:** Notice that you have information about the Ethernet adapter and Tunnel adapter isatap. This is because the **LON-CL1** is connected directly to the internal network and is not using DirectAccess.

### Verify connectivity to internal resources from an external client

1. Simulate moving **LON-CL1** out of the corporate network and to the Internet by disabling the London\_Network network adapter and enabling the Internet network adapter, which is configured with following values:
  - o IP address: **131.107.0.20**
  - o Subnet mask: **255.255.255.0**
  - o Preferred DNS server: **131.107.0.100**
2. Close all open windows.
3. On **LON-CL1**, from the taskbar, open **Internet Explorer**.
4. In the Internet Explorer Address bar, type `http://lon-svr1.adatum.com`, and then press Enter.
5. Verify that the default IIS 9.0 webpage for **LON-SVR1** displays.
6. Right-click **Start**, click **Run**, type `\\LON-SVR1\Corpdata`, and then press Enter. Note that you are able to access the folder content.
7. Open a command prompt and type `ipconfig`. Notice that you now have information about the Tunnel adapter iphttpsinterface. You should see three IPv6 addresses with two of them starting with **2002**. This is because the **LON-CL1** client is connected to the internal network using DirectAccess.

### Verify connectivity to the DirectAccess server

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

```
Netsh name show effectivepolicy
```

2. Verify that **DNS Effective Name Resolution Policy Table Settings** displays two entries: **Adatum.com**, and **DirectAccess-NLS.Adatum.com**.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-DAClientExperienceConfiguration
```

4. Notice the DirectAccess client settings.

### Verify client connectivity on the DirectAccess server

1. Switch to **EU-RTR**.
2. In the **Remote Access Management** console tree, click **Remote Client Status**. Notice that the **Client** is connected via **IPHttps**.

3. In the **Connection Details** pane, in the bottom-right corner of the screen, note the use of Kerberos for the **Machine** and the **User**.
4. Close all open windows.



**Note:** Do not revert the virtual machines after completing this lab. You will use them for subsequent labs.

**Results:** After completing this exercise, you should have successfully validated the DirectAccess deployment.

**Question:** Why did you create the DirectAccessClients group?

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



## Lesson 3

# Implementing and managing an advanced DirectAccess infrastructure

The Getting Started Wizard in the Remote Access Management console provides an easy method for organizations to configure DirectAccess connectivity for remote clients. However, as you learned in the previous lesson, there are limitations to deploying DirectAccess by using the Getting Started Wizard. Therefore, some organizations choose to deploy DirectAccess by configuring advanced features such as PKI, configuring advanced DNS settings, and configuring advanced settings for network location servers and management servers.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe advanced DirectAccess options.
- Explain how to integrate a PKI with DirectAccess.
- Describe Load balancing and high availability options.
- Describe how to support multiple locations.
- Explain how to implement certificates for DirectAccess clients.
- Describe the considerations for planning internal network configuration.
- Explain how to configure advanced DNS settings.
- Describe how to implement network location servers.
- Describe how to implement management servers.
- Describe how to modify the DirectAccess infrastructure.
- Explain how to monitor DirectAccess connectivity.
- Explain how to troubleshoot DirectAccess connectivity.

### Overview of the advanced DirectAccess options

You can configure advanced DirectAccess options by using the Remote Access Management console, or by using Windows PowerShell. When you install the Remote Access server role, two wizards become available in the Remote Access Management console for initial DirectAccess deployment:

- The Getting Started Wizard. Use this wizard to deploy DirectAccess quickly.
- The Remote Access Setup Wizard. Use this wizard to configure advanced options for DirectAccess.

Advanced DirectAccess configuration options include:

- Scalable and customized PKI infrastructure
- Customized network configuration options
- Scalable and highly-available server deployment
- Customized monitoring and troubleshooting

By using the Remote Access Management console, you can do the following advanced DirectAccess configurations:

- Scalable and customized PKI infrastructure. A DirectAccess deployment can benefit from a custom PKI solution, whether used with a public or private CA. You can configure the PKI components according to the organization's business requirements, for example to provide support for computers running Windows 7.
- Customized network configurations options. Organizations can benefit from deploying DirectAccess to meet specific network topology and design, including complex scenarios such as multiple site and multiple domain deployments. You can configure the DirectAccess clients so that they can connect to the corporate network by using multiple Internet connections in different geographical locations as DirectAccess entry points. Customized network configuration options include advanced DNS configurations and firewall settings.
- Scalable and highly available server deployment. While configuring advanced DirectAccess options, you can use a variety of solutions for better scalability of the servers. This will help your organization achieve their business goal of better remote access performance. Additionally, in cases where DirectAccess is a business critical solution, you can deploy multiple servers that are highly available so that no single point of failure exists and users can establish DirectAccess connectivity regardless of any potential issue. You also can configure management servers that will perform management tasks such as deploying Windows updates on DirectAccess clients and servers.
- Customized monitoring and troubleshooting. Advanced DirectAccess options include customized monitoring and troubleshooting options that will help you diagnose and resolve any potential DirectAccess issues quickly.

## Load balancing and high availability options

In order to provide your clients with a continuous smooth access to DirectAccess servers even if one of the server stops responding due to hardware failure, power outage or other unplanned problems, you must provide some form of load balancing and fault tolerance.

With DirectAccess, you can use the following high-availability solution:

- You can use Network Load Balancing (NLB), which is built into Windows Server 2016.
- You can use a third party solution such as Citrix NetScaler, F5, and others.

- DirectAccess can be made highly-available using:
  - Network Load Balancing (NLB)
  - Third party solution such as Citrix NetScaler, F5 and others
- If DirectAccess server is running in a Hyper-V virtual machine, MAC spoofing must be enabled
- All DirectAccess servers in a load balancing cluster must have the same configuration
- You should consider making the Network Location Server highly-available as well

To load-balance DirectAccess servers in the same location, you will install the Remote Access Role on two or more servers and then configure DirectAccess on one of them. You will then add the other servers as load balanced DirectAccess servers. The network configuration and number of NIC must be the same on all the DirectAccess you want to add to the NLB cluster. If your first DirectAccess server has two network cards, the other DirectAccess servers must also have two network cards connected to the same networks.


You perform the following steps to configure high-availability for DirectAccess servers:

1. Configure the first DirectAccess server according to your requirements.
2. Install the Remote Access role on the additional servers.

3. Add the Network Load Balancing feature on all DirectAccess Servers.
4. Run the Enable Load Balancing wizard in the Remote Access console on the first server.
5. In the Enable Load Balancing wizard, select the load balancing method, which could be either NLB or an external load balancer (3. party).
6. Add the additional DirectAccess servers when running the Enable Load Balancing wizard.

If your DirectAccess servers is running as Hyper-V virtual machines, you must enable MAC address spoofing on the vNIC in order for NLB to function properly. This is done by opening the settings for the virtual machine and under **Advanced Features** for the **Network Adapter**, selecting **Enable MAC address spoofing**.

As mentioned, it is also supported to use 3. party load balancers with DirectAccess but it requires the direct configuration of IPv6 address and additional configuration.

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

The Network Location Server (NLS) is as important as the DirectAccess server itself. The DirectAccess clients use the NLS to determine whether they are outside or inside the company network. If a DirectAccess client can connect to the NLS, then it must be inside. If it is not able to connect to the NLS, then it must be outside.

If the NLS goes offline for whatever reason, DirectAccess clients outside the company network will not be affected, but DirectAccess clients inside your company network will believe that they are outside and attempt to make a connection to the DirectAccess server. If the DirectAccess server cannot be reached from inside the company network none of the clients inside the company network will be able to connect to any network resources before the NLS is online again.

Because of this, you should make sure that your Network Location Server (NLB) is highly available. This can be done by installing two or more web servers and then making them highly-available using Network Load Balancing.

 **Note:** DirectAccess only support one Network Location Server URL per deployment.

## Supporting multiple locations

When you deploy DirectAccess in your organization you can choose between a single-site or multisite deployment. With a multisite deployment, you install two or more DirectAccess servers and place them in multiple geographic locations as opposed to a single-site deployment where you install your DirectAccess server in a single geographic location.

A multisite deployment has the following advantages:

- Your DirectAccess clients connect to the closest DirectAccess thus reducing latency

- With a multisite deployment, two or more DirectAccess servers are placed in multiple locations.
- A multisite deployment gives the following benefits:
  - Your DirectAccess clients connects to the closest and fastest DirectAccess server
  - If a DirectAccess server in one site goes offline, clients can connect to DirectAccess server in another site
- A multisite deployment requires:
  - A PKI
  - A single DirectAccess server with advanced settings already deployed
  - Internal network must be IPv6 enabled
  - Windows 7 clients must be manually assigned to a site

- Your DirectAccess clients connect to the fastest responding DirectAccess server
- In case one of your DirectAccess servers goes offline, clients can connect to a Direct Access server in another site

You can either assign clients to connect to a specific DirectAccess server or you can let your users select one at connection time. You can also have the user's computer, if it is running Windows 8 or newer, selecting the closest or fastest DirectAccess server. Windows 7 clients however, can only be assigned to a single DirectAccess and are not able to choose which DirectAccess server to use.


The requirements for a multisite deployment are:


- Public Key infrastructure.
- A single DirectAccess server with advanced settings has already been deployed.
- The internal network must be IPv6 enabled.
- Windows 7 clients are not location aware and will always connect to a specific location.

Compared with a single-site deployment which only uses two Group Policy objects, a multisite deployment requires a separate Group Policy object for DirectAccess server (entry point) and a separate Group Policy object for client domain. If you are also supporting Windows 7 clients, they would need a separate Group Policy object for each entry point as well.

You configure a multisite deployment from the Remote Access Management console by running the Enable Multisite wizard. Even though the Enable Multi wizard will configure the required Group Policy objects you must create the required security groups yourself. These security groups are used by Group Policy to only apply the DirectAccess client settings to members of a particular security group.

Windows 10, Windows 8.1, and Windows 8 clients can all be member of the same security group but because Windows 7 cannot select the entry point (DirectAccess server) to connect to by themselves, you will have to decide which entry point they should connect to. This means that you will essentially need a security group for each entry point (DirectAccess server) in your multisite deployment, and the group membership will determine the location that the Windows 7 computer connects to.

 **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

While planning for DirectAccess implementation, organizations can choose to use a private or public certification authority (CA). If an organization has already deployed an internal PKI infrastructure that is used for different purposes (such as user or server authentication), the organization can further customize the current PKI infrastructure to deploy DirectAccess.

Configuring PKI for DirectAccess includes the following high-level steps:

1. Add and configure the Active Directory Certificate Services server role (if not already present). At least one server with the Enterprise CA role should be present in the corporate network. The CA server receives certificate requests, issues certificates for network location server and DirectAccess clients and servers, and manages the CRL.

Configuring PKI for DirectAccess includes the following steps:

1. Add and configure the CA server role (if not already present)
2. Create the certificate template
3. Create a CRL distribution point and publish the CRL list
4. Distribute the computer certificates



**Note:** Implementing and configuring a PKI is no trivial task and should not be taken lightly. Furthermore, you must ensure that all your DirectAccess servers and clients trusts the Certification authority that have issued the certificates. The Certificate Revocation List Distribution Point (CDP) must be accessible to all machines using the certificates in order to verify the revocation status and it must be configured before you begin to issue certificates. Because the location of the CDP is embedded into the certificate. Making the CDP accessible to remote machines is often overlooked when implementing a PKI.



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

2. Create the certificate template. DirectAccess requires that you create a new certificate template based on the web certificate template on the CA server, which will be used for issuing a certificate to the network location server. The security settings on the default Web server certificate doesn't allow you to enroll the certificate using the Certificates snap-in.
3. The network location server will use its web certificate to authenticate itself to DirectAccess client computers and to encrypt traffic between itself and DirectAccess client computers.
4. Create a CRL distribution point and publish the CRL list. When connecting to the network location server, DirectAccess client computers check if the certificate being presented to them by the network location server is revoked. Therefore, you have to configure your CA server with a CRL distribution point where the CRL will be published. This distribution point also will be accessible to the DirectAccess client computers from both the internal network and the Internet.
5. Distribute the computer certificates. DirectAccess uses IPsec for encrypting the traffic between DirectAccess client computers and DirectAccess servers. IPsec requires that the CA server issue computer certificates to both DirectAccess client computers and DirectAccess servers. The most efficient way for distributing computer certificates is by using Group Policy. Computer certificates are a prerequisite only for the DirectAccess clients that are running Windows 7 to connect to the DirectAccess server.

The following certificates are required to support an advanced implementation of DirectAccess:

- A certificate with an intended purpose of Client and Server authentication. It must be deployed to each client computer.
- A certificate with an intended purpose of Client and Server authentication. This is used by the DirectAccess server and is for the IPsec authentication. This can be a wildcard certificate, so all your DirectAccess servers can use the same certificate.
- A certificate with an intended purpose of Web server or server authentication used for the IP-HTTPS connection. This can be a wildcard certificate.
- A certificate with an intended purpose of Web server or server authentication used for the Network Location Server (NLS). This cannot be a wildcard certificate.

## Implementing client certificates for DirectAccess

Organizations that have an environment with computers running Windows 7 also can use DirectAccess. For a computer running Windows 7 to use DirectAccess, a certificate with an intended purpose of Client and Server authentication must be issued to the computer.

The most efficient way for issuing certificates to client computers is by using Group Policy. The following are the high-level steps for configuring a GPO to issue certificates:

1. Create a GPO and link the GPO to the organizational unit where DirectAccess client computers are located.
2. Edit the GPO that you created in the previous step. To do this, navigate to **Computer Configuration \Policies\Windows Settings\Security Settings\Public Key Policies**, and then at **Automatic Certificate Request Settings**, configure **Automatic Certificate Request** to issue the Computer certificate.
3. Apply the GPO settings to the DirectAccess client computers by performing one of following actions:
  - At each DirectAccess client computer, run the **gpupdate /force** command.

Or

  - Restart the DirectAccess client computer.
4. Verify that the GPO has been applied. To do this:
  - Open an **MMC** on a client computer, with Certificates for the Local Computer snap-in added.
  - In the **Certificates** console, verify that a certificate with the DirectAccess client computer name displays, with **Intended Purposes of Client Authentication and Server Authentication**.

- Computer certificate for IPsec authentication is required for DirectAccess clients running Windows 7
- Steps for deploying certificates for client computers:
  1. Create a GPO and link it to the organizational unit that contains the DirectAccess clients
  2. Configure the GPO for automatic certificate request for the computer account
  3. Apply the GPO
  4. Verify that the certificates are issued
- DirectAccess can be configured to use OTP
- Typically requires 3rd party software or hardware to supply the password

### One Time Password (OTP)

When using OTP, a unique password is generated for each connection that is made by the Direct Access Client. This password is created by special software and is usually valid only for a short period of time.

When the DirectAccess client is turned on and it connects to the Internet, the user is prompted for the OTP. If the user provides the correct password, the DirectAccess client connects to the DirectAccess server.

You must do the following for enabling the use of OTP with DirectAccess:

1. Create and configure a certificate template for the OTP certificate.
2. Create and configure a certificate template for the OTP request signing certificate.
3. If you are using OTP with Windows 7 clients, you must download and install the DirectAccess Connectivity Assistant (DCA) 2.0.
4. Configure your DirectAccess server as a Remote Authentication Dial-in User (RADIUS) client.
5. Enable OTP on the DirectAccess server by using the Remote Access Management console.



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

## Internal network configuration options

Depending on your organization's business requirements, you can configure multiple network topologies when deploying an advanced DirectAccess infrastructure.

When planning for internal network configurations, you should take into account the following considerations:

- Plan for the DirectAccess server location. You can install the DirectAccess server in different network configurations:
  - Edge. In this configuration, you install the DirectAccess server role service on a computer that acts as an edge server. An edge server also acts as a firewall. The edge server has two network adapters, where one network adapter is connected to the Internet and the other network adapter is connected to the internal network.
  - Behind an edge device (with two network adapters). In this configuration, you install the DirectAccess role service on a computer that is located in a perimeter network, behind an edge device. The DirectAccess server has two network adapters, where one network adapter is connected to the perimeter network and the other network adapter is connected to the internal network.
  - Behind an edge device (with one network adapter). This configuration assumes that the DirectAccess role service is installed on a computer located in the internal network.
- Plan the IP address assignment. You should plan your IP addressing based on whether your organization has deployed native IPv6 addressing, both IPv6 and IPv4 addressing, or IPv4-only addressing. In a scenario where both Internet and intranet IP addressing is IPv4, you must configure the external network adapter of the DirectAccess server with two consecutive public IPv4 addresses. This configuration is required by the Teredo tunneling protocol because the DirectAccess server will act as a Teredo server. If you do not configure two consecutive public IPv4 address for the Teredo protocol, the DirectAccess client computers will connect by using IP-HTTPS.

Planning for internal network configuration includes:

- Plan for DirectAccess server location (Edge, perimeter network, and internal network)
- Plan the IP address assignment
- Plan the firewall configuration
- Plan for AD DS
- Plan for client deployment



**Note:** The DirectAccess client computers will first try to connect by using 6to4. If the connection is not successful, the DirectAccess clients will try connecting by using Teredo. If they are not able to connect with Teredo, they will try to connect by using IP-HTTPS.

- Plan the firewall configuration. The DirectAccess server requires a number of ports to be open on the corporate firewall so that the DirectAccess client computers can connect from Internet to the internal network. Firewall ports needed for DirectAccess on IPv4 network include:
  - Teredo traffic. UDP destination port 3544 inbound and UDP source port 3544 outbound.
  - 6to4 traffic. IP Protocol 41 inbound and outbound.
  - IP-HTTPS. Transmission Control Protocol (TCP) destination port 443 and TCP source port 443 outbound.
  - For scenarios where DirectAccess and the network location server are installed on the same server with a single adapter, TCP port 62000 on the server should be open.
- Plan for Active Directory Domain Services (AD DS). DirectAccess requires at least one domain controller installed on a server running Windows Server 2008 or newer Windows Server operating system. The computer where the DirectAccess role service is installed must be a domain member. The DirectAccess client computers also have to be domain members. DirectAccess clients can establish a connection from the Internet with any domain in the same forest as the DirectAccess server, and with any domain that has a two-way trust with the DirectAccess server forest.
- Plan for client deployment. Prior to deploying clients, you should configure the following:
  - Create a security group for DirectAccess client computers and configure the group membership.
  - Configure DirectAccess to either be available for all computers in the domain, or just for mobile computers.
  - Configure the Network Connectivity Assistant.



**Additional Reading:** For more information, refer to: "Step 2: Plan DirectAccess Deployments" at <http://aka.ms/Ttfwyn>

## Configuring advanced DNS settings

Detailed planning for a DNS server is important for proper configuration of DirectAccess. This is because many DirectAccess technology components use the DNS service. DirectAccess supports a DNS server on Windows Server 2008 and newer Windows Server operating systems.

You use DNS in DirectAccess for the following tasks:

- Resolving the network location server name. DirectAccess clients attempt to resolve the network location server name in DNS, and then contact the network location server to determine if they are on the internal network.

- DirectAccess uses DNS for resolving:
  - Network location server
  - IP-HTTPS
  - CRL distribution point
  - ISATAP
  - Connectivity verifiers
- You can configure the NRPT by using Group Policy with the following settings:
  - DNS suffixes
  - CRL distribution point
  - Split-brain DNS



- Resolving the IP-HTTPS server name. The DirectAccess client computers should use public DNS servers to resolve the IP-HTTPS name.
- Checking CRL revocation. DirectAccess client computers attempt to resolve the CRL distribution point name in DNS.
- Answering ISATAP queries. You should configure DNS servers to answer ISATAP queries. By default, the DNS server service blocks name resolution for the name ISATAP through the DNS Global Query Block List.
- Connectivity verifiers. To verify connectivity to the internal network, DirectAccess creates a default web probe that DirectAccess client computers use. For this, you should register the following names manually in DNS:
  - `directaccess-webprobehost`. This name should resolve to the internal IPv4 address of the DirectAccess server, or to the IPv6 address in an IPv6-only environment.
  - `directaccess-corpconnectivityhost`. This name should resolve to the localhost (loopback) address. The following host (A and AAAA) resource records should be created: A host (A) resource record with the value 127.0.0.1, and an IPv6 host (AAAA) resource record with the value constructed out of a NAT64 prefix with the last 32 bits as 127.0.0.1. You can retrieve the NAT64 prefix by running the **`get-netnattransitionconfiguration`** cmdlet.



**Note:** Connectivity verifier DNS records configure automatically when you run the Getting Started Wizard.

To separate Internet traffic from intranet traffic in DirectAccess, Windows Server 2016 and Windows 10 include Name Resolution Policy Table (NRPT), a feature that allows DNS servers to be defined per DNS namespace, rather than per interface.

The NRPT stores a list of rules. Each rule defines a DNS namespace and configuration settings that describe the DNS client's behavior for that namespace.

When a DirectAccess client is on the Internet, each name query request is compared against the namespace rules stored in the NRPT. If a match is found, the request is processed according to the settings in the NRPT rule. If a name query request does not match a namespace listed in the NRPT, the request is sent to the DNS servers that are configured in the TCP/IP settings for the specified network interface.

DNS settings on the network interface are configured depending upon the client location:

- For a remote client computer, the DNS servers are typically the Internet DNS servers configured through the Internet service provider (ISP).
- For a DirectAccess client on the intranet, the DNS servers are typically the intranet DNS servers configured through DHCP.

Single-label names, for example, `http://internal`, typically have configured DNS search suffixes appended to the name before they are checked against the NRPT.

If no DNS search suffixes are configured, and if the single-label name does not match any other single-label name entry in the NRPT, the request is sent to the DNS servers specified in the client's TCP/IP settings.

Namespaces such as internal.adatum.com are entered into the NRPT, followed by the DNS servers to which requests matching that namespace should be directed. If an IP address is entered for the DNS server, all DNS requests are sent directly to the DNS server over the DirectAccess connection. The NRPT allows DirectAccess clients to use intranet DNS servers for name resolution of internal resources, and Internet DNS for name resolution of other resources. Dedicated DNS servers are not required for name resolution. DirectAccess is designed to prevent the exposure of your intranet namespace to the Internet.



**Note:** You must treat some names differently with regards to name resolution; you should not resolve these names by using intranet DNS servers. To ensure that these names are resolved with the DNS servers specified in the client's TCP/IP settings, you must add them as NRPT exemptions.

You control the NRPT through Group Policy. When a computer is configured to use NRPT, the name resolution mechanism uses the following locations in this order:

1. The local name cache
2. The hosts file
3. NRPT

The name resolution mechanism subsequently sends the query to the DNS servers specified in the TCP/IP settings.

You might also need to create exemption rules in NRPT in the following scenarios:

- If your organization uses multiple domain names in the internal namespace, you must add more DNS suffixes in NRPT.
- If the FQDNs of your CRL distribution points are based on the intranet namespace, you must create exemption rules for the FQDNs of the CRL distribution points.
- In a scenario where the organization's domain name is the same on both the Internet and on the intranet (known as *split-brain DNS configuration*), you have to create exemption rules for the Internet clients to decide whether they want to resolve the Internet FQDN or intranet FQDN.

## Implementing network location servers

The network location server hosts the network location server website, which can be located on a DirectAccess server or on another server in your organization. If the network location server website is located on the DirectAccess server, the website is created automatically when you deploy DirectAccess. If the network location server website is located on another computer running a Windows Server operating system, you must install Internet Information Services (IIS) on that computer manually, and then configure the network location server website.

- You can locate the network location server on:
  - A DirectAccess server
  - Another server with IIS installed
- Requirements for network location server configuration include:
  - Configure a network location server website certificate
  - Ensure that DirectAccess clients trust the CA
  - Ensure that the the network location server website server certificate is checked against a CRL
  - The network location server should be accessible by internal clients
  - The network location server should not be accessible by Internet clients
  - The network location server should be highly available

The network location server must meet the following requirements:

- You must configure an HTTPS server certificate for the network location server website.
- The DirectAccess client computers must trust the CA that issues the HTTPS certificate for the network location server website.
- You must check the network location server website server certificate against a CRL.
- The DirectAccess client computers on the internal network must be able to resolve the name of the network location server.
- The network location server should not be accessible to DirectAccess client computers on the Internet.
- If DirectAccess is business critical for the organization, you should configure the network location server with high availability for computers located on the internal network.

## Implementing management servers

Management servers in a DirectAccess infrastructure are the servers that provide different management tasks, such as Windows Update and antivirus updates. Management servers also perform software or hardware inventory assessments. In a DirectAccess infrastructure, domain controllers are also considered management servers.

DirectAccess clients can discover the following management servers automatically:

- Domain controllers. DirectAccess servers perform automatic discovery of domain controllers for all domains in the same forest as the DirectAccess server and DirectAccess client computers.
- Microsoft System Center Configuration Manager servers. DirectAccess servers perform auto-discovery of System Center Configuration Manager servers for all domains in the same forest as the DirectAccess server and DirectAccess client computers.

- Management servers in DirectAccess are:
  - Domain controllers
  - System Center Configuration Manager servers
- Management servers are detected by DirectAccess:
  - Automatically
  - Manually if modified
- Management server requirements:
  - Should be accessible for the infrastructure tunnel
  - Must fully support IPv6

Discovery of domain controllers and Configuration Manager servers is performed automatically during the initial DirectAccess configuration.

You can use the following Windows PowerShell cmdlet to display the detected management servers:

```
Get-DAMgmtServer -Type All
```

After the initial DirectAccess deployment, if you make any changes such as adding or removing management servers (domain controllers or servers running System Center Configuration Manager), you can update the management servers list by clicking **Refresh Management Servers** in the **Remote Access Management** console.

Management servers should meet following requirements:

- Management servers should be accessible over the first (infrastructure) tunnel. During the initial DirectAccess deployment, management servers are, by default, configured automatically to be accessible over the infrastructure tunnel.
- Management servers must fully support IPv6. If native IPv6 is deployed, management servers communicate with DirectAccess clients by using native IPv6 address. In an IPv4 environment, management servers communicate with DirectAccess clients by using ISATAP.

## Demonstration: Modifying the DirectAccess infrastructure

In this demonstration, you will learn how to:

- Modify the DirectAccess infrastructure that you deployed by using the Getting Started Wizard.
- Apply advanced configuration settings.

### Demonstration Steps

#### Configure the Remote Access server role

1. On **EU-RTR**, in **Server Manager**, open the **Remote Access Management** console, and then click **DirectAccess and VPN**.
2. In the details pane of the **Remote Access Management** console, under **Step 1**, click **Edit**, and then specify the following settings:
  - Select Groups: **DA\_Clients**
  - Network Connectivity Assistant – Resource: Delete the current resource, and then add **https://lon-svr1.adatum.com**.
3. In the details pane of the **Remote Access Management** console, under **Step 2**, click **Edit**.
4. On the **Network Topology** page, verify that **Edge** is selected, and then type **131.107.0.10**.
5. Select **Use a self-signed certificate created automatically by DirectAccess**.
6. On the **Network Adapters** page, verify that **CN=131.107.0.10** is being used as a certificate to authenticate the IP-HTTPS connection.
7. On the **Authentication** page, click **Use computer certificates**, click **Browse**, and then click **AdatumCA**.
8. Click **Enable Windows 7 client computers to connect via DirectAccess**.
9. On the **Authentication** page, click **Finish**.
10. In the details pane of the **Remote Access Management** console, under **Step 3**, click **Edit**.
11. 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**.
12. On the **DNS** page, examine the values, and then click **Next**.
13. In the **DNS Suffix Search List**, examine the values, and then click **Next**.
14. On the **Management** page, click **Finish**.
15. In the details pane of the **Remote Access Management** console, display the settings for Step 4.
16. In the **Remote Access Setup** windows, review the settings, and then click **Finish**.

17. In the details pane of the **Remote Access Management** console, click **Finish**.
18. 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.

## How to monitor DirectAccess connectivity

You can monitor DirectAccess connectivity by using the Remote Access Management Console. This console contains information on how DirectAccess server components work. By using the Remote Access Management console, you also can monitor DirectAccess client connectivity information. By monitoring DirectAccess connectivity, you can obtain information about DirectAccess role service health that will help you troubleshoot potential connectivity issues.

The Remote Access Management Console includes the following monitoring components:

Remote Access Management Console monitoring components:

- Dashboard
- Operations Status
- Remote Access Client Status
- Remote Access Reporting

- **Dashboard.** The Remote Access Management Console includes a centralized dashboard for monitoring multiple DirectAccess components. The dashboard contains the following information: Operation status, Configuration status, DirectAccess, and VPN client status. Information about each of these components is available in separate windows in the Remote Access Management Console.
- **Operations Status.** Operation status provides information about the health of each DirectAccess component: DNS, DNS64, domain controllers, IP-HTTPS, Kerberos authentication, NAT64, network adapters, network location server, and Network security and services. If the DirectAccess component is healthy, it has a green check mark. If there is any issue with the DirectAccess component, it has a blue question mark. By clicking the component, you can obtain more detailed information about the related issue, the cause of the issue, and how to resolve it.
- **Remote Access Client Status.** Remote Access Client Status displays information about the DirectAccess client computers that connect to the DirectAccess server. The information displaying in this window includes User Name, Host Name, ISP Address, Protocol/Tunnel, and Duration. For each DirectAccess client connection, you can view more detailed information.
- **Remote Access Reporting.** Remote Access Reporting provides the same information as Remote Access Client Status, but as a historical DirectAccess client usage report. You can choose the start date and end date for the report. In addition, Remote Access Reporting displays Server Load Statistics, which is statistical connectivity information for the following: Total DirectAccess sessions, Average sessions per day, Maximum concurrent sessions, and Unique DirectAccess clients.

## How to troubleshoot DirectAccess connectivity

Organizations should develop a troubleshooting methodology for DirectAccess connectivity to quickly eliminate any problem that DirectAccess client computers face. Troubleshooting methodology should contain step-by-step instructions on how to diagnose the problem.

You can use the following list to troubleshoot DirectAccess connectivity:

- Troubleshooting methodology. Whenever DirectAccess client computers are not able to connect to the DirectAccess server, we recommend that you follow the methodology for problem diagnostics. Troubleshooting methodology includes the following steps:
    - Check if DirectAccess supports the operating system version.
    - Check if the DirectAccess client computer is a member of the domain.
    - Check if the DirectAccess client computer received computer configuration Group Policy settings for DirectAccess.
    - Check if the DirectAccess server computer received computer configuration Group Policy settings for DirectAccess.
    - Check if the DirectAccess client computer has a global IPv6 address.
    - Check if the DirectAccess client computer is able to connect to the IPv6 addresses of the DirectAccess server.
    - Check if the intranet servers have a global IPv6 address.
    - Check if the DirectAccess client computer on the Internet correctly determines that it is not on the intranet.
    - Ensure that the DirectAccess client computer is assigned the domain firewall profile.
    - Check if the DirectAccess client computer has IPv6 reachability to its intranet DNS servers, and if the DirectAccess client computer is able to use intranet DNS servers to resolve and to reach intranet FQDNs.
- Also, check if the DirectAccess client computer is able to communicate with intranet servers by using application layer protocols.
- Check if the DirectAccess client computer is able to establish both IPsec infrastructure and intranet tunnels with the DirectAccess server.

You can troubleshoot DirectAccess connectivity by using:

- A troubleshooting methodology
- Command-line tools
- GUI tools

- Command-line tools. Use following command-line tools for performing the checks as per your troubleshooting methodology:
  - **Netsh**
  - **Ping**
  - **Nslookup**
  - **Ipconfig**
  - **Certutil**
  - **Nltest**
- GUI tools. Use the following graphical user interface (GUI) tools for performing the checks as per your troubleshooting methodology:
  - Remote Access Server Management console
  - Group Policy Management Console and Group Policy Management Editor
  - Windows Firewall with Advanced Security
  - Event Viewer
  - Certificates

## Demonstration: Monitoring and troubleshooting DirectAccess connectivity

In this demonstration, you will learn how to monitor and troubleshoot 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 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Open a **Command Prompt** window, and then type the following commands:

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

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

#### Move the client computer to the Internet virtual network

1. Simulate moving **LON-CL1** out of the corporate network and to the Internet by disabling **London\_Network** network adapter, and then enabling the **Internet** network adapter.
2. Close the **Network Connections** window.

### Verify connectivity to the DirectAccess server

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

```
ipconfig
```

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

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

```
Netsh name show effectivepolicy
```

3. Open **Settings**, select **Network & Internet**, and then click **DirectAccess**.
4. Verify that **Your PC is set up correctly for single-site DirectAccess** is displayed under **Location**.
5. 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 center 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 **LON-CL1**, and then 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**, review the options for monitoring historical data.
9. Close the **Remote Access Management Console**.

## Implementing DirectAccess offline domain join

When deploying DirectAccess in your organization, you should determine which client computers will use DirectAccess to connect from the Internet. To do this, you first define a security group that will be granted access to the corporate network with DirectAccess, and then configure client computer accounts to be members of that security group. Therefore, only domain-joined client computers can be members of a DirectAccess security group. However, there might be nondomain remote computers that need to connect by using DirectAccess. To enable

To configure DirectAccess offline domain join:

1. Create a new computer account for the remote client computer and run the `djoin.exe` command to generate a provisioning package
2. Add the client computer account to the `DirectAccessClients` security group
3. Copy the provisioning package to the remote client computer that will be joining the domain
4. Apply the provisioning package to the remote client computer
5. Reboot the remote client computer



nondomain computers to join the domain even if they are not connected to the corporate network, you can use the DirectAccess offline domain join feature that is available in the Windows Server 2016, Windows Server 2012 R2, Windows 10, and Windows 8.1 operating systems.

To configure DirectAccess offline domain join, perform the following steps:

1. Create a new computer account for the remote client computer and run the **djoin.exe** tool to generate a provisioning package. You need to create a computer account in AD DS for each remote client computer that will be joined to the domain. In addition, run the following command to generate a provisioning package for each computer account that is created.

```
Djoin /provision /domain <your domain name> /machine <remote machine name> /policynames DA Client GPO name /rootcacerts /savefile c:\files\provision.txt /reuse
```

2. Add the client computer account to the DirectAccessClients security group. You must now join all client computer accounts that you created in the previous step to the DirectAccessClients security group. DirectAccess then configures and allows access to those computers from the Internet.
3. Copy the provisioning package to the remote client computer that will be joining the domain. You need to copy the provisioning package to the remote client computers so that the provisioning package is applied.
4. Apply the provisioning package to the remote client computer. Use the following command to apply the provisioning package to the remote client computer:

```
Djoin /requestodj /loadfile C:\provision\provision.txt /windowspath %windir% /localos
```

5. Reboot the remote client computer. After rebooting the remote client computer, the DirectAccess offline domain join process will complete, and the remote client computer becomes a member of the domain. It now can now access the corporate network by using DirectAccess.

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

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

## Lab B: Deploying an advanced DirectAccess solution

### Scenario

The DirectAccess proof of concept deployment was a success, so IT management has decided to enable DirectAccess for all mobile clients, including computers running Windows 7. IT management also wants to ensure that the DirectAccess deployment is scalable and provides redundancy.

You need to modify the proof of concept deployment to meet the new requirements.

### Objectives

After completing this lab, you will be able to:

- Prepare the infrastructure for the advanced DirectAccess deployment.
- Implement the advanced DirectAccess infrastructure.
- Validate the DirectAccess deployment.

### Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20741A-LON-DC1, 20741A-LON-SVR1, 20741A-EU-RTR, 20741A-LON-CL1, 20741A-LON-CL2**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**


Virtual machine: **20741A-INET1**

User name: **Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, on the **Start** screen, click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1, 20741A-EU-RTR, 20741A-LON-CL1, and 20741A-LON-CL2**.
6. In Hyper-V Manager, click **20741A-INET1**, and in the **Actions** pane, click **Start**.
7. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
8. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**

 **Note:** You may not be able to connect to the internal file share or the internal Web site since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

## Exercise 1: Preparing the environment for DirectAccess

### Scenario

As a first step in implementing the advanced DirectAccess solution, you need to prepare the network infrastructure. To do this, you will configure an internal network location server, and configure and distribute the required certificates.


The main tasks for this exercise are as follows:

1. Configure the Active Directory Domain Services (AD DS) and Domain Name System (DNS) requirements.
2. Configure certificate revocation list (CRL) distribution.
3. Configure client certificate distribution.
4. Configure the network location server and DirectAccess server certificates.

### ► Task 1: Configure the Active Directory Domain Services (AD DS) and Domain Name System (DNS) requirements

#### Modify the security group for DirectAccess client computers


1. Switch to **LON-DC1**.
2. Open the **Active Directory Users and Computers** console, and then in the Organizational Unit named **Special Accounts**, modify the membership of the **DirectAccessClients** group to include **LON-CL1** and **LON-CL2**.

 **Note:** The DirectAccessClients security group will control which computer will be able to connect to the internal resources by using DirectAccess.

3. Close the **Active Directory Users and Computers** console.

#### Create the required DNS records

1. Open the **DNS Manager** console, and then create new host records with the following settings:
  - o Name: **nls**
  - o IP Address: **172.16.0.11**
  - o Name: **crl**
  - o IP Address: **172.16.0.1**
2. Close the **DNS Manager** console.

 **Note:** The client will use the NLS record to determine its network location. The internal clients will use the CRL record to check the revocation status on the certificates that are used in DirectAccess.

### Configure the DNS suffix on EU-RTR

1. Switch to **EU-RTR**.
2. Right-click **Start**, and then click **Network Connections**.
3. Open the **Internet Properties** dialog box.
4. In the **Internet Properties** dialog box, open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, open **Advanced TCP/IP Settings** dialog box, and then add the **adatum.com** DNS suffix.
5. Close the **Internet Properties** dialog box.



**Note:** The Internet client needs the DNS suffix to resolve names for internal resources.

### ► Task 2: Configure certificate revocation list (CRL) distribution

#### Configure certificate requirements

1. Switch to **LON-DC1**, and then open the **Certification Authority** console.
2. Configure the **AdatumCA** CA with the following extension settings:
  - Add Location: **http://crl.adatum.com/crld/**
  - Variable: **CaName, CRLNameSuffix, DeltaCRLAllowed**
  - Location: Type **.crl** at the end of the **Location** string
  - Select **Include in CRLs. Clients use this to find Delta CRL locations**.
  - Select **Include in the CDP extension of issued certificates**.
3. When prompted, do not restart Certificate Services.
4. Configure the **AdatumCA** CA with the following extension settings:
  - Add Location: **\\EU-RTR\crlldist\$**
  - Variable: **CaName, CRLNameSuffix, DeltaCRLAllowed**
  - Location: Type **.crl** at the end of the Location string
  - Select **Publish CRLs to this location**
  - Select **Publish Delta CRLs to this location**
  - Restart **Certificate Services**
  - Close the **Certification Authority** console



**Note:** You perform these steps to prepare the CA with proper extensions for the CRL distribution point, which will be included in the future certificates that the CA will use.

### ► Task 3: Configure client certificate distribution

#### Configure computer certificate auto-enrollment

1. On **LON-DC1**, open the **Group Policy Management Console**.
2. In the console tree, navigate to **Forest: Adatum.com\Domains\Adatum.com**.

3. Click to edit the **Default Domain Policy**, and then in the **Group Policy Management Editor** console tree, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.
4. Under **Automatic Certificate Request Settings**, configure **Automatic Certificate Request** to issue the **Computer** certificate.
5. Close both the **Group Policy Management Editor** and the **Group Policy Management Console**.

► **Task 4: Configure the network location server and DirectAccess server certificates**

**Request a certificate for LON-SVR1**

1. On **LON-SVR1**, open a Windows PowerShell prompt, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
mmc
```

3. Add the **Certificates** snap-in for the Local computer.
4. In the **Certificates** snap-in console tree, navigate to **Certificates (Local Computer)\Personal\Certificates**, and then request a new certificate.
5. Under **Request Certificates**, configure the **Adatum Web Certificate** with the following setting:
  - o Subject name: Under **Common name**, type **nls.adatum.com**.
6. In the **Certificates snap-in** window, in the details pane, verify that a new certificate with the name **nls.adatum.com** is enrolled with **Intended Purposes of Server Authentication**.
7. Close the **MMC**.
8. When you are prompted to save the settings, click **No**.

**Change the HTTPS bindings**

1. From **Server Manager**, open the **Internet Information Services (IIS) Manager** console.
2. In **Internet Information Services (IIS) Manager**, in the console tree, navigate to **LON-SVR1/Sites**, and then click **Default Web site**.
3. Configure **HTTPS Site Bindings** by selecting **nls.adatum.com** as **SSL Certificate**.
4. Close the **Internet Information Services (IIS) Manager** console.



**Note:** The client will use the HTTPS bindings that you configure for the host name nls.adatum.com to determine the network location in the DirectAccess scenario.

**Configure the DirectAccess server with the appropriate certificate**

1. Switch to **EU-RTR**.
2. Open a Windows PowerShell prompt, and then refresh group policy by typing the following command:

```
gpupdate /force
```

3. Open a **MMC** by typing the following command:

```
mmc
```

4. Add the **Certificates** snap-in for the Local computer.
5. In the **Certificates snap-in** window, in the **MMC**, request a new certificate with the following settings:
  - o Certificate template: **Adatum Web Certificate**
  - o Common name: **131.107.0.10**
  - o Friendly name: **IP-HTTPS Certificate**
6. Close the console.



**Note:** Instead of issuing a certificate with the IP address in the subject name, in a real environment, you will use the FQDN of the Internet-facing server that will be reachable by the external client.

### Create a CRL distribution point on EU-RTR

1. On **EU-RTR**, open **Server Manager**.
2. Open **Internet Information Services (IIS) Manager**, and create new virtual directory named **CRLD**.
3. Enable browsing for the **CRLD directory**, and then assign **c:\crl-dist** as a home directory.
4. Using the **Internet Information Services (IIS) Manager configuration editor**, locate the **Section** drop-down list, and navigate to **system.webServer\security\requestFiltering**.
5. In the middle pane of the **Internet Information Services (IIS) Manager** console, locate the **allowDoubleEscaping** entry. Change the value from **False** to **True**, and then apply the changes.
6. Close **Internet Information Services (IIS) Manager**.



**Note:** You need to modify the value of **allowDoubleEscaping** to allow clients to access CRL deltas that will have a plus (+) sign appended to the filename.

### Share and secure the CRL distribution point

1. Open **File Explorer**.
2. In the **File Explorer** details pane, configure the following permissions for **CRLDist\$** share name:
  - o Grant **Full Share and NTFS permission** to the **LON-DC1** computer.



**Note:** The following steps will make the CRL distribution point available for external clients. Internal clients will still have the possibility to reach CRL either by using a Lightweight Directory Access Protocol (LDAP) query to AD DS, or by accessing the file share from the internal network adapter on **EU-RTR**.

## Publish the CRL to EU-RTR



**Note:** These step makes the CRL available on the edge server for Internet-based DirectAccess clients.

1. Switch to **LON-DC1**.
2. Start the **CA** console.
3. In the console tree, open **AdatumCA**.
4. Right-click **Revoked Certificates**, point to **All Tasks**, click **Publish**, and then select the **New CRL** option.
5. Open **File Explorer**, and browse to the following location: **\\EU-RTR\CRLDist\$**.
6. In File Explorer, notice the **AdatumCA** files that display.
7. Close **File Explorer**.



**Note:** If you receive an error while publishing the certificate, it is because either you did not enter the extensions for CRL in the CA properly, or you did not grant appropriate permission for the **LON-DC1** computer account on the **\\EU-RTR\CRLDIST\$** share.

**Results:** After completing this exercise, you should have prepared the environment for implementing advanced DirectAccess infrastructure.

## Exercise 2: Implementing the advanced DirectAccess infrastructure

### Scenario

Now that you have prepared the environment, you can modify the DirectAccess configuration to use the advanced infrastructure components.

The main tasks for this exercise are as follows:

1. Modify the DirectAccess deployment.
2. Verify the server and GPO configuration.

### ► Task 1: Modify the DirectAccess deployment

#### Reset the DirectAccess configuration



**Note:** The steps in this section is only required because Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

1. On **EU-RTR**, in **Server Manager**, start the **Remote Access Management Console**. Then click **DirectAccess and VPN**.
2. Click **Remove Configuration Settings** under **Tasks**. When prompted by the **Confirm Remove Configuration**, click **OK**.

3. Wait for the **Removing Configuration Settings** wizard to complete and then click **Close**.
4. Complete the **Run the Getting Started Wizard** with the following settings:
  - a. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
  - b. Verify that **Edge** is selected and that **131.107.0.10** is listed in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** text box. Then click **Next**.
  - c. On the **Remote Access Review** page, click the **here** link.
  - d. Change remote clients to **DirectAccessClients**.
  - e. Clear the **Enable DirectAccess for mobile computers only** check box.
  - f. In the **Helpdesk email address** text box, type **DAHelp@adatum.com**.
  - g. In the **DirectAccess connection name** text box, type **A. Datum DirectAccess**.
5. Close the **Applying Getting Started Wizard Settings** dialog box.



**Note:** You might receive the following warning, **“To deploy a network load balancing cluster or multisite deployment, obtain a certificate for the network location server with a subject name that is different from the internal name of the Remote Access server.”** This warning can be safely ignored.

### Configure the Remote Access server role

1. On **EU-RTR**, open **Server Manager**.
2. In the **Server Manager** console, start the **Remote Access Management Console** and then click **DirectAccess and VPN**.
3. In the details pane of the **Remote Access Management Console**, under **Step 1**, click **Edit**, and then specify the following:
  - o Select Groups: Verify that **DirectAccessClients (ADATUM\DirectAccessClients)** group is listed.
  - o Network Connectivity Assistant: Delete the current resource, and add **https://nls.adatum.com**.
4. In the details pane of the **Remote Access Management Console**, under **Step 2**, click **Edit**.
5. On the **Network Topology** page, verify that **Edge** is selected.
6. On the **Network Adapters** page, verify that **Use a self-signed certificate created automatically by DirectAccess** is not selected, and that **CN=131.107.0.10** is listed. Then click **Next**.
7. On the **Authentication** page, click **Use computer certificates**, click **Browse**, and then click **AdatumCA**.
8. Click **Enable Windows 7 client computers to connect via DirectAccess**, and then click **Finish**.



**Note:** You need to enable certificate authentication with the certificates issued from a trusted CA to support Windows 7 clients.

9. In the details pane of the **Remote Access Management Console**, under **Step 3**, click **Edit**.
10. On the **Network Location Server** page, click **The network location server is deployed on a remote web server (recommended)**.
11. In the **Type in the URL of the network location server** text box, type **https://nls.adatum.com**, and then click **Validate**. Ensure that the URL is validated.



12. On the **DNS** page, ensure that **nls.adatum.com** is listed, and then add the entry **crl.adatum.com** into the NRPT table.
13. On the **Management** page, click **Finish**.
14. In the details pane of the **Remote Access Management Console**, display the settings for **Step 4**.
15. On the **DirectAccess Application Server Setup** page, review the settings, and then click **Finish**.
16. In the **Remote Access Management Console**, in the details pane, click **Finish**.
17. On the **Remote Access Review** page, click **Apply**.
18. In the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

► **Task 2: Verify the server and GPO configuration**

1. On **EU-RTR**, open the Windows PowerShell prompt, and then run the following commands:

```
gpupdate /force  
Ipconfig
```

2. Verify that **EU-RTR** has an IPv6 address for **Tunnel adapter IPHTTPSInterface** that starts with **2002**.

**Results:** After completing this exercise, you should have implemented the advanced DirectAccess infrastructure.

## Exercise 3: Validating the DirectAccess deployment

### Scenario

With the advanced DirectAccess infrastructure in place, you now need to test deployment. You will verify that a Windows 10 client can connect to the internal network by using DirectAccess.

The main tasks for this exercise are as follows:

1. Verify Windows 10 client connectivity.
2. Monitor client connectivity.
3. Prepare for the next module.

► **Task 1: Verify Windows 10 client connectivity**

### Verify DirectAccess Group Policy configuration settings for Windows 10 clients

1. Switch to **LON-CL2**.
2. Restart **LON-CL2**.



**Note:** You must restart the **LON-CL2** machine because you added the machine account to the DirectAccess Clients security while the machine was running. In order to update the machine's security token, it must restart.

3. After **LON-CL2** has restarted, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.

4. Open a **Command Prompt** window, and type the following command to verify that the **DirectAccess Client Settings** GPO is applied to the **Computer Settings**:

```
gpresult /R
```



**Note:** If the DirectAccess Client Settings GPO is not applied, restart **LON-CL2**, and then repeat steps 3 and 4 on **LON-CL2**.

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

```
netsh name show effectivepolicy
```

6. Verify that the following message displays: **DNS Effective Name Resolution Policy Table Settings**  
**Note: DirectAccess settings are inactive when this computer is inside a corporate network.**
7. Close all open windows.

### Verify client computer certificate distribution

1. On **LON-CL2**, open the **Certificates MMC**.
2. Verify that a certificate with the name **LON-CL2.adatum.com** displays with **Intended Purposes of Client Authentication and Server Authentication**.
3. Close the console without saving.

### Verify internal network access

1. On **LON-CL2**, from the taskbar, open **Internet Explorer**.
2. In the Internet Explorer Address bar, type **http://lon-svr1.adatum.com**, and then press Enter.
3. Verify that the default IIS 9.0 webpage for **LON-SVR1** displays.
4. On the Start screen, type **\\LON-SVR1\Corpdata**, and then press Enter.



**Note:** Note that you are able to access the folder content.

5. Close all open windows.
6. Open a **Command Prompt** window, and type **ipconfig**.



**Note:** Notice that you receive information about the Ethernet adapter and Tunnel adapter isatap. This is because **LON-CL2** is connected directly to the internal network and is not using DirectAccess.

### Move the client computer to the Internet virtual network

1. Simulate moving **LON-CL2** from the intranet network to the Internet by disabling the London\_Network network adapter and enabling the Internet network adapter.
2. Close the **Network Connections** window.

## Verify connectivity to the DirectAccess server

1. On **LON-CL2**, open a **Command Prompt** window, and type the following command:

```
ipconfig
```



**Note:** Notice the IP address that starts with **2002**. This is an IP-HTTPS address. If there is no IP address for **iphttpsinterface**, type the following commands, restart the computer, and then repeat step 1.

```
Netsh interface teredo set state disabled  
Netsh interface 6to4 set state disabled
```



**Note:** In this lab setup, IP-HTTPS connectivity on the firewall is enabled, and other connectivity methods from the client—such as the Teredo or 6to4 tunneling protocol—are disabled. If you are planning to use the Teredo or 6to4 tunneling protocol in the production environment, you should not disable them.

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

```
Netsh name show effectivepolicy
```

3. Verify that **DNS Effective Name Resolution Policy Table Settings** present three entries: **adatum.com**, **crl.adatum.com**, and **nls.Adatum.com**.
4. At the command prompt, type the following command, and then press Enter:

```
powershell
```

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

```
Get-DAClientExperienceConfiguration
```

6. Review the DirectAccess client settings.
7. Open **Settings**, select **Network & Internet**, and then click **DirectAccess**.
8. Under **Location**, verify that **Your PC is set up correctly for single-site DirectAccess** displays.
9. Notice the **Collect** button under **Troubleshooting info**.

## Verify connectivity to the internal network resources



**Note:** You may not be able to connect to the internal file share, the internal Web site, ping lon-dc1 or run gpupdate since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

1. Open **Internet Explorer**, and then in the Address bar, type **http://lon-svr1.adatum.com/**.
2. Verify that the default IIS 9.0 webpage for **LON-SVR1** displays.
3. Open **File Explorer**, in the address bar, type **\\LON-SVR1\Corpdata**, and then press Enter.
4. Verify that the **Corpdata** folder displays its contents.



**Note:** You are able to open **http://lon-svr1.adatum.com** and **\\lon-svr1\Corpdata** because there is a record in NRPT that resolves any internal namespace from adatum.com by using an internal DNS server.

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

```
ping lon-dc1.adatum.com
```

6. Verify that you are receiving replies from LON-DC1.adatum.com.
7. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

8. Close all open windows.
9. Switch to **EU-RTR**.
10. Start the **Remote Access Management Console**, and then review the information on Remote Client Status.
11. Notice that **LON-CL2** is connected via IP-HTTPS.
12. In the **Connection Details** pane, in the bottom-right of the screen, note that **Machine Certificate & User Ntlm**, are in use.
13. Close all open windows.

#### ► Task 2: Monitor client connectivity

1. On **EU-RTR**, open the **Remote Access Management Console**, and then in the left pane, click **Dashboard**.
2. Review the information in the central pane, under the **DirectAccess and VPN Client Status**.
3. In the left pane, click **Remote Client Status**, and then in the central pane, review the information under the **Connected Clients** list.
4. In the left pane, click **Reporting**, and then in the central pane, click **Configure Accounting**.
5. In the **Configure Accounting** window, under the **Select Accounting Method**, click **Use inbox accounting**, click **Apply**, and then click **Close**.
6. In the central pane, under **Remote Access Reporting**, review the options for monitoring historical data.

**Results:** After completing this exercise, you should have verified that a Windows 10 client can connect to the internal network by using DirectAccess.

#### ► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.

4. Repeat steps 2 and 3 for: **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-INET1**, **20741A-LON-CL1**, and **20741A-LON-CL2**.

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

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

## 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.

### 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.	
The DirectAccess client tries to connect to the DirectAccess server by using IPv6 and IPsec with no success.	

### Review Questions

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

**Question:** How do you configure DirectAccess clients?

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

**Question:** What is the use of an NRPT?

### Tools

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

Tool	Use for	Where to find it
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

**MCT USE ONLY. STUDENT USE PROHIBITED**



# Module 8

## Implementing VPNs

### Contents:

Module Overview	8-1
<b>Lesson 1:</b> Planning VPNs	8-2
<b>Lesson 2:</b> Implementing VPNs	8-12
<b>Lab:</b> Implementing VPN	8-20
Module Review and Takeaways	8-30

## Module Overview

Remote-access technologies in Windows Server 2016 enable users to connect securely to data and resources in organizational networks. In Windows Server 2016, four component technologies—virtual private network (VPN), DirectAccess, Routing, and Web Application Proxy—integrate into a single, unified server role called Remote Access.



**Note:** The VPN, DirectAccess, and Routing technologies are available in Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012. However, Web Application Proxy is a new feature in Windows Server 2012 R2.

In this module, you will learn how you can use VPNs to implement and manage remote access in Windows Server 2016. You also will learn about the different implementation scenarios for small and medium-sized organizations, and enterprise organizations.

### Objectives

After completing this module, you will be able to:

- Plan a VPN solution.
- Implement VPN access.

## Lesson 1

# Planning VPNs

VPN provides secure access to organizations' internal data and applications for clients and devices that are using the Internet. If you want to implement and support a VPN environment properly within your organization, you must understand how to select a suitable tunnelling protocol, configure VPN authentication, and configure the server role to support your chosen configuration.

As discussed in "module 7 Implementing DirectAccess", DirectAccess offers many advantages in comparison to VPN. However, some devices that must connect from the Internet to an internal network do not support DirectAccess. These devices include mobile devices, tablet devices, computers that are not domain members, workgroup computers, and computers that are running nonenterprise versions of Windows 10, Windows 8, or Windows 7 operating systems. For these devices, organizations should deploy VPN.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the various VPN scenarios.
- Describe the tunnelling protocols that a VPN connection uses.
- Describe the VPN authentication options.
- Describe the VPN Reconnect feature.
- Describe app-triggered VPN.

### VPN scenarios

Similar to previous Windows Server versions, Windows Server 2016 supports two types of VPN connections:

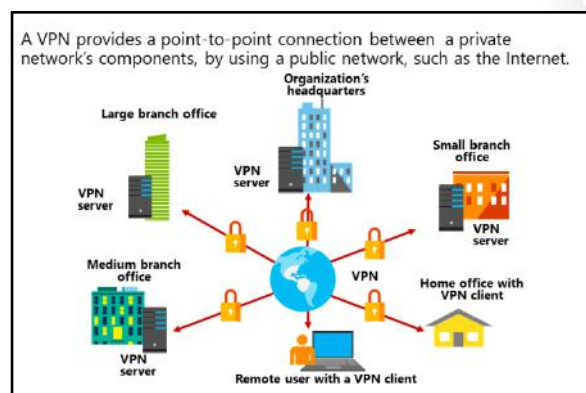
- Remote access
- Site-to-site

#### Remote-access VPN connections

Remote-access VPN connections enable users who work offsite, such as at home, at a customer site, or from a public wireless-access point, to access a server on your organization's private network by using the infrastructure that a public network provides, such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computer, the VPN client, and your organization's server. The exact infrastructure of the shared or public network is irrelevant, because it appears logically as if the data is sent over a dedicated private link.

#### Site-to-site VPN connections

Site-to-site VPN connections, or *router-to-router VPN connections*, enable your organization to establish routed connections between separate offices or with other organizations over a public network, while helping to maintain secure communications.



## Properties of VPN connections

VPN connections that use the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol with Internet Protocol Security (L2TP/IPsec), and Secure Socket Tunneling Protocol (SSTP) have the following properties:

- Encapsulation. VPN technology encapsulates private data with a header that contains routing information, which allows the data to traverse the transit network.
- Authentication. There are three types of authentication for VPN connections, including:
  - User-level authentication by using Point-to-Point Protocol (PPP) authentication. To establish the VPN connection, the VPN server authenticates the VPN client that is attempting to connect by using a PPP user-level authentication method. It then verifies that the VPN client has the appropriate authorization. If you use mutual authentication, the VPN client also authenticates the VPN server.
  - Computer-level authentication by using Internet Key Exchange (IKE). To establish an IPsec security association, the VPN client and the VPN server use the IKE protocol to exchange computer certificates or a preshared key. In either case, the VPN client and server authenticate each other at the computer level. We recommend computer-certificate authentication, because it is a much stronger authentication method than a preshared key. Please note, however, that computer-level authentication occurs only for L2TP/IPsec connections.
  - Data-origin authentication and data integrity. To verify that the data sent on a VPN connection originated at the connection's other end and was not modified in transit, the data contains a cryptographic checksum that is based on an encryption key known only to the sender and the receiver. Note that data-origin authentication and data integrity are available only for L2TP/IPsec connections.
- Data encryption. To ensure data confidentiality as it traverses the shared or public transit network, the sender encrypts the data, and the receiver decrypts it. The encryption and decryption processes depend on the sender and the receiver both using a common encryption key.

Packets that are intercepted in the transit network are unintelligible to anyone who does not have the common encryption key. The encryption key's length is an important security parameter. Therefore, it is important to use the largest possible key size to ensure stronger data encryption and confidentiality. However, stronger encryption consumes more central processing unit (CPU) resources. Therefore, organizations should plan for hardware resources if they plan to require stronger encryption.

## Site-to-site VPN

A site-to-site VPN connection connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server attaches. The calling router, which is the VPN client, authenticates itself to the answering router, which is the VPN server. For mutual authentication, the answering router authenticates itself to the calling router. In a site-to-site VPN connection, the packets sent from

- Connects two portions of a private network
- The calling router (the VPN client) authenticates itself to the answering router (the VPN server)
- Requires that you create a demand-dial interface
- You can create three types of site-to-site VPNs:
  - PPTP
  - L2TP
  - IKEv2
- Can be persistent or on-demand
- You can control traffic by using either IP demand-dial filters or dial-out filters

either router across the VPN connection typically do not originate at the routers. You must create a demand-dial interface on the calling router. This interface is a VPN profile that connects to the answering router.

When you create a demand-dial interface, you specify the same information as you would when creating a VPN profile. Furthermore, you must specify the credentials used to connect to the answering router. The name of the answering router's demand-dial interface must match the name of the user account that the calling router specifies.

When you configure site-to-site VPN, you can create a one-way connection or a two-way connection. If you configure a one-way connection, one VPN server always initiates the connection and one VPN server always answers. If you configure a two-way connection, either of your VPN routers can initiate the connection and both can act as the calling or answering router.

You can restrict a calling router from initiating unnecessary connections by using demand-dial filtering or dial-out hours. You can use demand-dial filtering to configure the type of traffic that can initiate a connection, or you can specify the traffic that cannot initiate a connection. You do this by right-clicking the demand-dial interface, and then clicking **Set IP Demand-dial Filters**. You also can configure times during which a calling router can, or cannot, initiate a connection. You do this by right-clicking the demand-dial interface, and then clicking **Dial-out Hours**.

A routed VPN connection across the Internet operates logically as a dedicated wide area network (WAN) link. When networks connect over the Internet, a router forwards packets to another router across a VPN connection. To the routers, the VPN connection operates as a data-link layer link.

You can create three types of site-to-site VPNs in Windows Server 2016, including:

- PPTP, which uses the Microsoft Point-to-Point Encryption (MPPE) for encryption and the PPP protocol for authentication.
- L2TP, which uses certificates for encryption, integrity, and data authentication, and PPP for authentication.
- IKE version 2 (IKEv2), which uses Advanced Encryption Standard (AES) 256, AES 192, AES 128, and Triple Data Encryption Standard (3DES) for encryption.

Additionally, a site-to-site VPN connection can be persistent or on-demand:

- On-demand VPN Connection: When traffic is being forwarded to the remote location, a site-to-site VPN connection occurs. When the transfer completes, the connection closes shortly thereafter, contingent on the configuration for your remote access policy. You also can configure the calling router (VPN client) to close the connection after a specified idle timeout interval. You can configure this in the properties of the demand-dial interface.
- A persistent VPN Connection: A persistent site-to-site VPN has a constant connection. Additionally, if the connection inadvertently closes or drops, it is reestablished immediately. To configure the connection as persistent, on the **Properties** page of the Demand dial interface, on the **Options** tab, select **Persistent connection**. You also can configure this on the answering router by clearing the **Idle Timeout** and **Session Timeout** boxes on the network policy's **Constraints** tab.

## Options for VPN tunneling protocols

PPTP, L2TP, and SSTP depend heavily on the features that you specified originally for PPP. PPP sends data across dial-up or dedicated point-to-point connections. For IP, PPP encapsulates IP packets within PPP frames, and then transmits the encapsulated PPP packets across a point-to-point link. PPP originally was the protocol to use between a dial-up client and a network access server.

### PPTP

You can use PPTP for remote access and site-to-site VPN connections. When you use the Internet as the VPN public network, the PPTP server is a PPTP-enabled VPN server that has one Internet interface and one on your intranet.

PPTP enables you to encrypt and encapsulate multiprotocol traffic in an IP header that it then sends across an IP network or a public IP network, such as the Internet:

- **Encapsulation.** PPTP encapsulates PPP frames in IP datagrams for network transmission. PPTP uses a TCP connection for tunnel management, and a modified version of Generic Route Encapsulation (GRE) to encapsulate PPP frames for tunneled data. Payloads of the encapsulated PPP frames can be encrypted, compressed, or both.
- **Encryption.** You can encrypt the PPP frame with MPPE by using encryption keys that are generated from the Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication process. VPN clients must use the MS-CHAPv2 or EAP-TLS authentication protocol to ensure encryption of payloads of PPP frames. PPTP uses the underlying PPP encryption and encapsulates a previously encrypted PPP frame.

### L2TP

L2TP enables you to encrypt multiprotocol traffic that is sent over any medium that supports point-to-point datagram delivery, such as IP or asynchronous transfer mode (ATM). L2TP is a combination of PPTP and Layer 2 Forwarding (L2F). L2TP represents the best features of PPTP and L2F.

Unlike PPTP, the Microsoft implementation of L2TP does not use MPPE to encrypt PPP datagrams. L2TP relies on IPsec in transport mode for encryption services. The combination of L2TP and IPsec is *L2TP/IPsec*.

To utilize L2TP/IPsec, both the VPN client and server must support L2TP and IPsec. The Windows 10, Windows 8, and Windows 7 remote access clients include client support for L2TP. Windows Server 2016, Windows Server 2012, and Windows Server 2008 operating systems all contain VPN server support for L2TP.

Windows Server 2016 supports four VPN tunneling protocols:

Tunneling protocol	Firewall access	Description
PPTP	TCP port 1723	Provides data confidentiality, but not data integrity or data authentication
L2TP/IPsec	UDP port 500, UDP port 1701, UDP port 4500, and IP protocol ID 50	Uses either certificates or preshared keys for authentication; we recommend certificate authentication
SSTP	TCP port 443	Uses SSL to provide data confidentiality, data integrity, and data authentication
IKEv2	UDP port 500	Supports the latest IPsec encryption algorithms to provide data confidentiality, data integrity, and data authentication

The encapsulation and encryption methods for L2TP are as follows:

- Encapsulation. Encapsulation for L2TP/IPsec packets consists of two layers, L2TP encapsulation and IPsec encapsulation. L2TP encapsulates and encrypts data as follows:
  - First layer. The first layer is the L2TP encapsulation. A PPP frame (an IP datagram) is wrapped with an L2TP header and a User Datagram Protocol (UDP) header.
  - Second layer. The second layer is the IPsec encapsulation. The resulting L2TP message is wrapped with an IPsec Encapsulating Security Payload (ESP) header and trailer, an IPsec Authentication trailer that provides message integrity and authentication, and a final IP header. The IP header contains the source and destination IP address that corresponds to the VPN client and server.
- Encryption. The L2TP message is encrypted with AES or 3DES by using encryption keys that the IKE negotiation process generates.

### **SSTP**

SSTP is a tunneling protocol that uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and web proxies, which otherwise might block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the SSL channel of the HTTPS protocol. The use of PPP allows support for strong authentication methods, such as EAP-TLS. SSL provides transport-level security with enhanced key negotiation, encryption, and integrity checking.

When a client tries to establish a SSTP-based VPN connection, SSTP first establishes a bidirectional HTTPS layer with the SSTP server. Over this HTTPS layer, the protocol packets flow as the data payload by using the following encapsulation and encryption methods:

- Encapsulation. SSTP encapsulates PPP frames in IP datagrams for transmission over the network. SSTP uses a TCP connection (over port 443) for tunnel management and as PPP data frames.
- Encryption. SSTP encrypts the message with the SSL channel of the HTTPS protocol.

### **IKEv2**

IKEv2 uses the IPsec Tunnel Mode protocol over UDP port 500. IKEv2 supports mobility, making it a good protocol choice for a mobile workforce. IKEv2-based VPNs enable users to move easily between wireless hotspots, or between wireless and wired connections.

The use of IKEv2 and IPsec enables support for the following strong authentication and encryption methods:

- Encapsulation. IKEv2 encapsulates datagrams by using IPsec ESP or Authentication Header (AH) for transmission over the network.
- Encryption. IKEv2 encrypts the message with one of the following protocols by using encryption keys that it generates during the IKEv2 negotiation process: AES 256, AES 192, AES 128, and 3DES encryption algorithms.

IKEv2 is supported only on computers that are running the Windows Server 2016, Windows 10, Windows 8, Windows Server 2012, Windows 7, and Windows Server 2008 R2 operating systems. IKEv2 is the default VPN tunneling protocol in Windows 10, Windows 7, and Windows 8.

## VPN authentication options

The authentication of access clients is an important security concern. Authentication methods typically use an authentication protocol that is negotiated during the connection establishment process. The Remote Access server role supports the methods that the following sections describe.

### PAP

Password Authentication Protocol (PAP) uses plaintext passwords and is the least secure authentication protocol. It typically is negotiated if the remote access client and Remote Access server cannot negotiate a more secure form of validation. Windows Server 2016 includes PAP to support older client operating systems that support no other authentication method.

Protocol	Description	Security level
PAP	Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.	The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.
CHAP	A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme	An improvement over PAP in that the password is not sent over the PPP link. Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.
MS-CHAPv2	An upgrade of MS-CHAP. Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server to which it is dialing in to has access to the user's password.	Provides stronger security than CHAP.
EAP	Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.	Offers the strongest security by providing the most flexibility in authentication variations.

### CHAP

The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme to encrypt the response. Various vendors of network access servers and clients use CHAP. However, because CHAP requires that you use a reversibly encrypted password, you should consider using another authentication protocol, such as MS-CHAPv2.

### MS-CHAPv2

MS-CHAPv2 is a one-way, encrypted password, mutual-authentication process that works as follows:

1. The authenticator, which is the Remote Access server or computer that is running Network Policy Server (NPS), sends a challenge to the remote access client. The challenge consists of a session identifier and an arbitrary challenge string.
2. The remote access client sends a response that contains a one-way encryption of the received challenge string, the peer challenge string, the session identifier, and the user password.
3. The authenticator checks the response from the client, and then sends back a response that contains an indication of the connection attempt's success or failure and an authenticated response based on the sent challenge string, the peer challenge string, the client's encrypted response, and the user password.
4. The remote access client verifies the authentication response and, if correct, uses the connection. If the authentication response is not correct, the remote access client terminates the connection.

### EAP

If you use EAP, an arbitrary authentication mechanism authenticates a remote access connection. The remote access client and the authenticator, which is either the Remote Access server or the Remote Authentication Dial-In User Service (RADIUS) server, negotiate the exact authentication scheme they will use. Routing and Remote Access includes support for EAP-TLS by default. You can plug in other EAP modules to the server that is running Routing and Remote Access to provide other EAP methods.



**Note:** We highly recommend that you disable the PAP and CHAP authentication protocols, because they are less secure when compared to the MS-CHAPv2 and EAP authentication protocols.

## Other authentication options

You can enable two additional options when you select an authentication method, including:

- **Unauthenticated Access.** This is not an authentication method, but rather is the lack of an authentication method. Unauthenticated access allows remote systems to connect without authentication. You should never enable this option in a production environment, as it leaves your network at risk. However, this option can be useful for troubleshooting authentication issues in a test environment.
- **Allow machine certificate authentication for IKEv2.** Select this option if you want to use VPN Reconnect.

## What is VPN Reconnect?

In dynamic business scenarios, users must be able to access data securely at anytime, from anywhere, and be able to access it continuously without interruption. For example, users might want to access data securely that is on the company's server, from a branch office, or while they are traveling.

Therefore, to meet this requirement, you can configure the VPN Reconnect feature that is available in Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows 10, Windows 8, and Windows 7. This feature allows users to access organizational data by using a VPN connection, which reconnects automatically if connectivity inadvertently disconnects. VPN Reconnect also enables roaming between different networks.

- VPN Reconnect maintains connectivity across network outages
- VPN Reconnect:
  - Provides seamless and consistent VPN connectivity
  - Uses the IKEv2 technology
  - Automatically reestablishes VPN connections when connectivity is available
  - Maintains the connection if users move between different networks
  - Provides transparent connection status to users

VPN Reconnect uses the IKEv2 technology to provide seamless and consistent VPN connectivity. Users who connect via a wireless mobile broadband will benefit most from this capability. Consider a user with a laptop that is running Windows 10. When the user travels to work in a train, he or she connects to the Internet with a wireless mobile broadband card, and then establishes a VPN connection to the organization's network. When the train passes through a tunnel, the Internet connection is lost. After the train emerges from the tunnel, the wireless mobile broadband card reconnects automatically to the Internet. With earlier versions of Windows client and server operating systems, the VPN did not reconnect automatically. Therefore, the user would have to repeat the multistep process of connecting to the VPN manually. This was time-consuming and frustrating for mobile users, as it provided intermittent connectivity.

However, with VPN Reconnect, clients that are running Windows Server 2016 and Windows 10 reestablish active VPN connections automatically when the network reestablishes Internet connectivity. Even though the reconnection might take several seconds, users need not reconnect manually, or authenticate again to access internal network resources.



The system requirements for using the VPN Reconnect feature include that you must have:


- 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.
- A public key infrastructure (PKI), because VPN Reconnect requires a computer certificate for a remote connection. You can use certificates that an internal certification authority (CA) or a public CA issue.

## The app-triggered VPN feature

App-triggered VPN enables a VPN profile to connect automatically when a specified app or set of apps starts. This extends a VPN's automatic-connection behavior and provides support for app-triggered VPN connections in Windows 10 VPN profiles. Windows 8.1 introduced this functionality as *On demand VPN*.

You can configure app-triggered VPN connections to start automatically, creating a secure connection when a trusted app needs a network resource. You can create trusted app lists that can include traditional desktop apps or universal apps.

- App-triggered VPN enables an app to trigger a VPN profile automatically
- You configure app-triggered VPN by using the **AddVpnConnectionTriggerApplication** PowerShell cmdlet
- Domain-member computers do not support app-triggered VPN
- App-triggered VPN requires that you enable split tunneling for the VPN profile

 **Note:** Domain-member computers do not support app-triggered VPNs. They require that you enable split tunneling for the VPN profile.

### Configuring app-triggered VPN

To configure app-triggered VPN, you must:

1. Find the Package Family Name for universal apps or find the path for desktop apps.
2. Enable the app to trigger the VPN.
3. Enable split tunneling for the VPN connection.

#### ***Find the Package Family Name for universal apps or find the path for desktop apps***

You can find the Package Family Name for universal apps by running the **Get-AppxPackage** cmdlet, and then looking at the value for the **PackageFamilyName** property.

The following example shows how you would determine this information for the Microsoft Skype universal app:

```
Name           : Microsoft.SkypeApp
Publisher      : CN=Skype Software Sarl, O=Microsoft Corporation, L=Luxembourg,
S=Luxembourg, C=LU
Architecture   : X86
ResourceId     :
Version       : 3.2.1.0
PackageFullName : Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf38zg5c
InstallLocation : C:\Program
Files\WindowsApps\Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf38zg5c
IsFramework   : False
PackageFamilyName : Microsoft.SkypeApp_kzf8qxf38zg5c
PublisherId    : kzf8qxf38zg5c
IsResourcePackage : False
IsBundle      : False
IsDevelopmentMode : False
Dependencies    : {Microsoft.VCLibs.140.00_14.0.22929.0_x86__8wekyb3d8bbwe,
Microsoft.NET.Native.Framework.1.0_1.0.22929.0_x86__8wekyb3d8bbwe,
Microsoft.NET.Native.Runtime.1.0_1.0.22929.0_x86__8wekyb3d8bbwe,
Microsoft.SkypeApp_3.2.1.0_neutral_split_language-ar_kzf8qxf38zg5c...}
```

As you can see from the output, the **PackageFamilyName** for the Skype app is **Microsoft.SkypeApp\_kzf8qxf38zg5c**.

### **Enable the app to trigger the VPN**

To define apps by using the Package Family Name for universal apps or a complete file path for traditional Windows desktop apps, use the **Add-VpnConnectionTriggerApplication** cmdlet:

```
Add-VpnConnectionTriggerApplication [-ConnectionName] <String> [-ApplicationID] <String[]>
```

The *ConnectionName* is the name of the VPN profile and the *ApplicationID* is either the Package Family Name for universal apps or the complete file path for desktop apps. You can add multiple apps at the same time by using a comma to separate the IDs. To add this as an app that triggers the VPN connection named **A. Datum VPN**, you would use the following command:

```
Add-VpnConnectionTriggerApplication -ConnectionName "A. Datum VPN" -ApplicationID
Microsoft.SkypeApp_kzf8qxf38zg5c
```

The following command will add Internet Explorer and trigger the *A. Datum VPN* connection when it is launched:

```
Add-VpnConnectionTriggerApplication -ConnectionName "A. Datum VPN" -ApplicationID
"C:\Program Files (x86)\Internet Explorer\iexplore.exe"
```

### **Enable split tunneling for the VPN connection**

If you enable split tunneling for a VPN Connection, it means that all traffic that is not intended for the internal network will be sent out through the local gateway. However, while this typically means that the browser operates more quickly, it might introduce a security risk.

To use an app-triggered VPN, you must configure the VPN profile for split tunneling, and when you create a new VPN profile by using the graphical user interface (GUI) on Windows 10, split tunneling is disabled.

To verify the split tunneling state on a VPN profile, you can run the **Get-VPNConnection** cmdlet. However, because a VPN profile can be global (**Allow other people to use this connection**) or local (only configured for the user), you must run the **Get-VPNConnection** cmdlet twice.

Running the following command will retrieve all global VPN profiles:

```
Get-VPNConnection -AllUserConnection
```

Running the following command will retrieve all local VPN profiles:

```
Get-VPNConnection
```

Following is an example of the output after running the **Get-VPNConnection** cmdlet with the **-AllUserConnection** switch:

```
Name           : A. Datum VPN
ServerAddress  : 131.107.0.10
AllUserConnection : True
Guid           : {2197A304-F889-4859-B015-D01A0BA3D6BE}
TunnelType    : Sstp
AuthenticationMethod : {Eap}
EncryptionLevel : Optional
L2tpIPsecAuth :
UseWinlogonCredential : False
EapConfigXmlStream : #document
ConnectionStatus : Disconnected
RememberCredential : False
SplitTunneling : False
DnsSuffix     :
IdleDisconnectSeconds : 0
```

You can see from the output that the **SplitTunneling** property is **False**. To set it to **True**, which enables split tunneling for the **A. Datum VPN** profile, you must run the following command:

```
Set-VpnConnection -name "A. Datum VPN" -AllUserConnection -SplitTunneling $true
```

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

**Question:** What are the requirements for VPN Reconnect?

**Question:** Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
You can use app-triggered VPN with domain-member computers.	

## Lesson 2

# Implementing VPNs

Remote access is a business-critical process for many organizations that have mobile employees who must connect to their corporate network from outside the network, or for organizations that have multiple locations around the world. The remote-access solutions in these organizations include complex components that provide high availability, scalability, and a high level of security. However, before you deploy complex remote-access solutions, you must create a detailed plan.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to configure VPN by using the Getting Started Wizard.
- Explain the various options for modifying the VPN Configuration.
- Describe how to configure VPN.
- Describe the purpose of the Connection Manager Administration Kit.
- Describe how to create a connection profile.
- Explain how to distribute VPN profiles

### Configuring a VPN by using the Getting Started Wizard

You can configure a VPN solution by using the **Getting Started Wizard** in the Remote Access Management Console. You can use this wizard to configure both DirectAccess and VPN, or only DirectAccess or VPN. If you choose to configure VPN only, the Routing and Remote Access console displays, in which you can specify VPN configuration settings and deploy the VPN solution.

Before you deploy your organization's VPN solution, you must:

- Ensure that your VPN server has two network interfaces. You must determine which network interface will connect to the Internet and which will connect to your private network. During configuration, you must choose which network interface connects to the Internet. If you specify the incorrect network interface, your remote-access VPN server will not operate correctly.
- Determine whether remote clients receive IP addresses from a Dynamic Host Configuration Protocol (DHCP) server on your private network or from the remote-access VPN server that you are configuring. If you have a DHCP server on your private network, the remote access VPN server can lease 10 addresses at a time from the DHCP server, and then assign those addresses to remote clients. If you do not have a DHCP server on your private network, the remote-access VPN server can automatically generate and assign IP addresses to remote clients. If you want the remote-access VPN server to assign IP addresses from a range that you specify, you must determine what that range should be.

- Configure VPN by using the **Getting Started Wizard** in the Remote Access Management console
- Requirements for VPN server configuration include:
  - Two network interfaces (public and private)
  - IP Address allocation (static pool or DHCP)
  - Authentication provider (NPS/RADIUS or the VPN server)
  - DHCP relay agent considerations
  - Membership in the local Administrators group or equivalent

- Determine whether you want a RADIUS server or a remote access VPN server that you configure to authenticate connection requests from VPN clients. Adding a RADIUS server is useful if you plan to install multiple remote-access VPN servers, wireless access points, or other RADIUS clients to your private network.



**Note:** To enable a RADIUS infrastructure, install the Network Policy and Access Services server role. The NPS can act as a RADIUS proxy or server.

- Remember that by default, the **Getting Started Wizard** configures Windows authentication for VPN clients.
- Ensure that the person who deploys your VPN solution has the necessary administrative group memberships to install server roles and configure necessary services. Membership of the local Administrators group is required to perform these tasks.

## Options for modifying VPN configurations

After you deploy and configure your VPN solution, your server is ready for use as a remote access server. However, you can perform additional tasks on your remote access server, including that you can:

- Configure static packet filters. Add static packet filters to provide additional network protection.
- Configure services and ports. Choose the services on the private network that you want to make available for remote users.
- Adjust logging levels. Configure the level of event details that you want to log. You can decide which information you want to track in log files.
- Configure the number of VPN ports. Add or remove VPN ports. For example, you might want to increase L2TP, and remove all PPTP and SSTP connections. Configure the ports to support the number of users and the types of connections that you want to allow.
- Create a Connection Manager profile for users. Manage the client connection experience for users, and simplify configuration and troubleshooting of client connections.
- Add Active Directory Certificate Services (AD CS). Configure and manage a CA on a server for use in a PKI.
- Increase remote access security. Protect remote users and the private network by implementing methods such as enforcing use of secure authentication methods, and requiring higher levels of data encryption.
- Increase VPN security. Protect remote users and the private network by implementing methods such as requiring use of secure tunneling protocols, and configuring account lockout.
- Implement VPN Reconnect. Consider adding VPN Reconnect to reestablish VPN connections automatically for users who lose their Internet connections temporarily.

To configure your VPN solution, you might need to:

- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure the number of available VPN ports
- Create a Connection Manager profile for users
- Add AD CS
- Increase remote access security
- Increase VPN security
- Implement VPN Reconnect

## Demonstration: Configuring VPN

In this demonstration, you will learn how to:

- Verify certificate requirements for IKEv2 and SSTP.
- Review the default VPN configuration.
- Configure the Remote Access policies.

### Demonstration Steps

#### Prepare the environment

1. On **LON-DC1**, open a Windows PowerShell command prompt, type the following command, and then press Enter:

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

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

```
.\mod8.ps1
```

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

#### Request certificate for EU-RTR

1. On **EU-RTR**, open a command prompt, type the following command, and then press Enter:

```
mmc
```

2. Add the **Certificates** snap-in for Local computer.
3. In the **Certificates snap-in** console tree, navigate to **Certificates (Local Computer)\Personal**, and then request a new certificate.
4. Under **Request Certificates**, configure the **Adatum Web Certificate** with the following setting:
  - o Subject name: Under **Common name**, type **131.107.0.10**
5. In the **Certificates** snap-in, 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**.
6. Close the **Microsoft Management Console (MMC)**. When you receive a prompt to save the settings, click **No**.

#### Change the HTTPS bindings

1. Open the **Internet Information Services (IIS) Manager** console.
2. In **Internet Information Services (IIS) Manager**, in the console tree, navigate to **EU-RTR/Sites**, and then click **Default Web site**.
3. Configure site bindings by selecting **131.107.0.10** as **SSL Certificate**.
4. Close the **Internet Information Services (IIS) Manager** console.

#### Review the default VPN configuration

1. On **EU-RTR**, open **Routing and Remote Access**.
2. Right-click **EU-RTR (local)**, and then click **Disable Routing and Remote Access**. When prompted, click **Yes**.

3. Right-click **EU-RTR (local)**, and then click **Configure and Enable Routing and Remote Access**.
4. On the **Welcome to Routing and Remote Access Server Setup Wizard**, click **Next**.
5. On the **Configuration** page, select **Custom configuration**, and then click **Next**.
6. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then click **Next**.
7. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**. When prompted, click **Start service**.
8. Expand **EU-RTR (local)**, right-click **Ports**, and then click **Properties**.
9. Verify that five ports exist for **Wan Miniport (SSTP)**, **Wan Miniport (IKEv2)**, **Wan Miniport (PPTP)**, and **Wan Miniport (L2TP)**. Modify the number of ports for each type of connection to **4**.
10. Close the **Ports Properties** dialog box, and when prompted, click **Yes**.
11. Right-click **EU-RTR (local)**, and then click **Properties**.
12. On the **General** tab, verify that **IPv4 Remote access server** is selected.
13. On the **Security** tab, click the drop-down arrow next to **Certificate**, and then select **131.107.0.10**.
14. Click **Authentication Methods**, and then verify that **EAP** is selected as the authentication protocol.
15. On the **IPv4** tab, verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
16. To close the **EU-RTR (local) Properties** dialog box, click **OK**, and when prompted click **Yes**.

### Configure the Remote Access policies

1. On **EU-RTR**, from **Server Manager**, open the **Network Policy Server console**.
2. In the **Network Policy Server console**, in the navigation pane, expand **Policies**, and then click **Network Policies**.
3. Create a new network policy by using the **New Network Policy Wizard** with following settings:
  - o Policy name: **Adatum IT VPN**
  - o Type of network access server: **Remote Access Server(VPN-Dial up)**
  - o Windows Groups: **IT**
  - o Specify Access Permission: **Access granted**
  - o Configure Authentication Methods:
    - Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box
    - Add **Microsoft Secured password (EAP-MSCHAP v2)**
    - Add **Microsoft: Smart Card or other certificate**.
4. Complete the **New Network Policy Wizard** by accepting the default settings on the other pages.
5. Close all open windows.

## What is the Connection Manager Administration Kit?

You can use the Connection Manager Administration Kit (CMAK) to customize users' remote connection options by creating predefined connections to remote servers and networks. CMAK is an optional component that is not installed by default. You must install CMAK to create connection profiles that your users can install to access remote networks. The CMAK Wizard creates an executable file, which you can then distribute to your users in many ways, or include during deployment activities as part of the operating system image.

- CMAK:
  - Allows you to customize users' remote connection experience by creating predefined connections on remote servers and networks
  - Creates an executable file that can be run on a client computer to establish a network connection that you have designed
- You can distribute CMAK profiles to client computers by using:
  - An operating system image
  - Removable media
  - Software distribution tools, such as Configuration Manager

Connection Manager is a client network-connection tool that allows a user to connect to a remote network, such as an Internet service provider (ISP) or an organizational network, that a VPN server protects. You can use this tool to customize the remote-connection experience for users on your network by creating predefined connections to remote servers and networks.

### Distributing the connection profile

You can deliver the connection profile, which the CMAK Wizard generates, to users by utilizing different methods, such as by:

- Including the connection profile as part of the image that new computers include. You can install your connection profile as part of the client computer images that install on your organization's new computers.
- Delivering the connection profile on removable media so that the user can install it manually. You can deliver the connection-profile installation program on a CD/DVD, universal serial bus (USB) flash drive, or any other removable media that you permit your users to access. Some removable media support autorun capabilities, which allow you to start the installation automatically when the user inserts the media into the client computer.
- Delivering the connection profile with automated software-distribution tools. Many organizations use a desktop management and software deployment tool, such as Microsoft System Center Configuration Manager, which allows you to package and deploy software that you want your client computers to receive. The installation can be invisible to your users, and you can configure it to report to a management console whether the installation was successful.

### Demonstration: Creating a connection profile

In this demonstration, you will learn how to:

- Install CMAK.
- Create a connection profile.
- Examine the profile.



## Demonstration Steps

### Install CMAK

1. If necessary, on **LON-CL1**, sign in as **Adatum\administrator** with the password **Pa\$\$w0rd**.
2. Open **Program and Features**, and turn on the Windows feature **RAS Connection Manager Administration Kit (CMAK)**.

### Create a connection profile

1. From **Administrative Tools**, open the **Connection Manager Administration Kit**.
2. Complete the **Connection Manager Administration Kit Wizard** to create the connection profile.

### Examine the created profile

- Use File Explorer to examine the contents of the folder that you created with the **Connection Manager Administration Kit Wizard**. These files create the connection profile. Usually, you then would distribute this profile to your users.

## Distributing VPN profiles

Even though a user or administrator can create a VPN profile manually, we recommend that you automate this process whenever possible. You can deploy VPN profiles to your end users by using:

- Configuration Manager (current branch)
- Microsoft Intune
- Group Policy
- Scripts

### Deploy a VPN profile by using Configuration Manager (current branch)

You can deploy a VPN profile to the following operating systems: Windows 10, Windows 8.1, Windows Phone 8.1, iOS, and Android. Furthermore, to support Windows Phone 8.1, iOS, and Android, the device must be enrolled in Microsoft Intune.

System Center Configuration Manager supports several VPN connections, including:


- Cisco AnyConnect
- Pulse Secure
- F5 Edge Client
- Dell SonicWALL Mobile Connect
- Check Point Mobile VPN
- Microsoft SSL (SSTP)
- Microsoft Automatic
- IKEv2

You can create and distribute a VPN profile by using:

- Configuration Manager
- Intune
- Group Policy
- Scripts

- PPTP
- L2TP

If you deploy a non-Microsoft VPN profile, you must ensure that the VPN software is installed on the device. Otherwise, the user will not be able to use the VPN profile to connect to a VPN server.


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

### Deploy a VPN profile by using Intune

You can deploy VPN profiles by using Intune, which support the following VPN profiles natively:

- Cisco AnyConnect
- Pulse Secure
- F5 Edge Client
- Dell SonicWALL Mobile Connect
- CheckPoint Mobile VPN

Before you can deploy the VPN profiles, the device must be enrolled in Intune. You can create VPN profiles natively for devices running the Windows, Android, and iOS operating systems by creating a VPN profile in Microsoft Intune. You also can build a VPN policy manually by creating a Configuration Policy, and then specifying the various Open Mobile Alliance Uniform Resource Identifier (OMA-ORI) settings.


 **Additional Reading:** For more information, refer to: “VPN connections in Microsoft Intune” at <http://aka.ms/vp3kds>

### Deploy a VPN profile by using Group Policy and scripts

You can use Group Policy preferences to deploy VPN profiles to a user or to a computer. The settings for the User or Computer configuration can be found at the following locations:

- **Computer Configuration/Preferences/Control Panel Settings/Network Option**
- **User Configuration/Preferences/Control Panel Settings/Network Option**

Microsoft has provided a solution—a customized PowerShell script—for deploying VPN profiles by using a custom Windows PowerShell script and then deploying the Windows PowerShell script by using a Group Policy logon script.

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

You also can create and deploy VPN profiles by using the **Add-VPNConnection** PowerShell cmdlet, and then deploy the VPN profile by using a Group Policy logon script. The **Add-VPNConnection** cmdlets is available only on Windows 8 and newer operating systems.

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

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

**Check Your Knowledge**

Question	
What is the maximum number of ports that you can configure for SSTP?	
Select the correct answer.	
<input type="checkbox"/>	25
<input type="checkbox"/>	75
<input type="checkbox"/>	128
<input type="checkbox"/>	500
<input type="checkbox"/>	999

## Lab: Implementing VPN

### Scenario

The DirectAccess deployment is working very well. However, several computers that are deployed at A. Datum cannot connect to the organization's network by using DirectAccess. For example, some home users are utilizing computers that are not members of the Adatum.com domain. Other users are running operating-system versions that do not support DirectAccess. To enable remote access for these computers, you must deploy a VPN solution.

Furthermore, you must investigate why Logan cannot connect to the A. Datum VPN.

### Objectives

After completing this lab, you will be able to:

- Implement a VPN solution.
- Validate the VPN deployment.
- Troubleshoot a SSTP VPN connection.

### Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-INET1**, **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, on the **Start** screen, click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-EU-RTR**, and **20741A-LON-CL1**.
6. In Hyper-V Manager, click **20741A-INET1**, and then in the **Actions** pane, click **Start**.
7. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
8. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**

## Exercise 1: Implementing VPN

### Scenario

The first step to implementing VPN is to verify and configure certificate requirements for a SSTP VPN. You then must configure the Remote Access server to provide VPN connectivity, and you also must create a remote access policy to ensure that the clients can connect to the server by using IKEv2 and SSTP.

The main tasks for this exercise are as follows:

1. Verify certificate requirements for IKEv2 and SSTP.
2. Review the default VPN configuration.
3. Configure the Remote Access policies.

### ► Task 1: Verify certificate requirements for IKEv2 and SSTP

#### Prepare the environment

1. On **LON-DC1**, open an elevated Windows PowerShell prompt, type the following command, and then press Enter:

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

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

```
.\mod8.ps1
```

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

#### Request a certificate for EU-RTR

1. On **EU-RTR**, open a command prompt, type the following command, and then press Enter:

```
mmc
```

2. Add the **Certificates** snap-in for Local computer.
3. In the **Certificates snap-in** console tree, navigate to **Certificates (Local Computer)\Personal**, and then request a new certificate.
4. Under **Request Certificates**, configure the **Adatum Web Certificate** with the following setting:
  - o Subject name: Under **Common name**, type **131.107.0.10**
5. In the Certificates snap-in, 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**.
6. Close the **MMC**. When you are prompted to save the settings, click **No**.

#### Change the HTTPS bindings

1. On **EU-RTR**, open **Server Manager**, and then open the **Internet Information Services (IIS) Manager console**.
2. In **Internet Information Services (IIS) Manager**, in the console tree, navigate to **EU-RTR/Sites**, and then click **Default Web site**.
3. Configure site bindings by selecting **131.107.0.10** and configuring it as an **SSL Certificate**.
4. Close the **Internet Information Services (IIS) Manager console**.

► **Task 2: Review the default VPN configuration**

1. On **EU-RTR**, from **Server Manager**, open **Routing and Remote Access**.
2. Right-click **EU-RTR (local)**, click **Disable Routing and Remote Access**, and then when prompted, click **Yes**.
3. Right-click **EU-RTR (local)**, and then click **Configure and Enable Routing and Remote Access**.
4. On the **Welcome to Routing and Remote Access Server Setup Wizard**, click **Next**.
5. On the **Configuration** page, select **Custom configuration**, and then click **Next**.
6. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then click **Next**.
7. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**. When prompted, click **Start service**.
8. Expand **EU-RTR (local)**, right-click **Ports**, and then click **Properties**.
9. Verify that five ports exist for **SSTP**, **IKEv2**, **PPTP**, and **L2TP**. Modify the number of ports for each type of connection to **4**.
10. Close the **Ports Properties** dialog box, and when prompted, click **Yes**.
11. Right-click **EU-RTR (local)**, and then click **Properties**.
12. On the **General** tab, verify that **IPv4 Remote access server** is selected.
13. On the **Security** tab, click the drop-down arrow next to **Certificate**, and then select **131.107.0.10**.
14. Click **Authentication Methods**, and then verify that **EAP** is selected as the authentication protocol.
15. On the **IPv4** tab, verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
16. To close the **EU-RTR (local) Properties** dialog box, click **OK**, and when prompted, click **Yes**.

► **Task 3: Configure the Remote Access policies**

1. On **EU-RTR**, from **Server Manager**, open the **Network Policy Server console**.
2. In the **Network Policy Server console**, in the navigation pane, expand **Policies**, and then click **Network Policies**.
3. Create a new network policy by using the **New Network Policy Wizard** with following settings:
  - Policy name: **Adatum IT VPN**
  - Type of network access server: **Remote Access Server(VPN-Dial up)**
  - Windows Groups: **IT**
  - Specify Access Permission: **Access granted**
  - Configure Authentication Methods:
    - Clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box
    - Add **Microsoft Secured password (EAP-MSCHAP v2)**
    - Add **Microsoft: Smart Card or other certificate**.

4. Complete the **New Network Policy Wizard** by accepting the default settings on the other pages.
5. Close all open windows.

**Results:** After completing this exercise, you should have modified the Remote Access server configuration successfully to provide VPN connectivity.

## Exercise 2: Validating the VPN deployment

### Scenario

Now that you have deployed the VPN solution, you need to verify that the clients that cannot connect to the organization's network by using DirectAccess can connect by using VPN. You also need to test the Network Sign-in feature.

The main tasks for this exercise are as follows:

1. Remove the client computer from the domain.
2. Move **LON-CL1** to the Internet.
3. Configure a VPN connection and verify connectivity.
4. Sign in to the domain by using VPN.
5. Verify connectivity.

#### ► Task 1: Remove the client computer from the domain

1. Switch to **LON-CL1**.
2. Open **Control Panel**.
3. In Control Panel, remove **LON-CL1** from the **adatum.com** domain, and then add **LON-CL1** to the **WORKGROUP** workgroup.
4. If you receive a prompt, in the **Windows Security** dialog box, sign in as **Administrator** with the password **Pa\$\$w0rd**, and then click **OK**.
5. Restart **LON-CL1**.

#### ► Task 2: Move LON-CL1 to the Internet

1. When the **LON-CL1** computer has restarted, sign in with the user name **Admin** and the password **Pa\$\$w0rd**.
2. When prompted by the **Networks** dialog box, click **Yes**.
3. On **LON-CL1**, right-click **Start**, and then click **Network Connections**.
4. In the **Network Connections** window, right-click **London\_Network**, and then click **Disable**.
5. Right-click **Internet**, and then click **Enable**.
6. Right-click **Internet**, and then click **Properties**.
7. In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.

8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, ensure that the following settings display, and then click **OK**:
  - o IP address: **131.107.0.20**
  - o Subnet mask: **255.255.255.0**
  - o Preferred DNS server: **131.107.0.100**
9. In the **Internet Properties** dialog box, click **Cancel**.
10. Close all open windows.
11. On the **taskbar**, click the **File Explorer** icon.
12. In File Explorer, in the **address bar**, type `\\Lon-DC1\`, and then press Enter. Notice that a **Network Error** message displays.
13. Close all open windows.



**Note:** The client is unable to open the resources, because it is not on the internal network.

### ► Task 3: Configure a VPN connection and verify connectivity

#### Create a VPN profile

1. On **LON-CL1**, open **Network and Sharing Center**.
2. Start the **Set up a new connection or network** wizard, and then use the following settings:
  - o Choose a connection option: **Connect to a workplace**
  - o How do you want to connect: **Use my Internet connection (VPN)**
  - o Do you want to set up Internet connection before continuing: **I'll set up an Internet connection later**
  - o Internet address: **131.107.0.10**
  - o Destination name: **A. Datum VPN**, and click **Allow other people to use this connection**
3. Open the **A. Datum VPN** connection, and then sign in with the user name **adatum\logan** and the password **Pa\$\$w0rd**.
4. Verify that you are connected to Adatum by using the PPTP connection.



**Note:** To verify the type of connection, you can view the status in **Network Connections**. By default, the client will attempt to connect to the VPN server by using a secure connection, such as L2TP with IPsec, IKEv2, or SSTP. In this case, however, because the client does not have a computer certificate or a preshared key, the client cannot establish an L2TP or IKEv2 connection. Additionally, the client cannot establish an SSTP connection because it requires that the client trusts the certificate on the VPN server. Therefore, the only possible connection in this case is PPTP with the CHAP v2 authentication.



### Export a root CA certificate

1. Switch to **LON-DC1**.
2. Open the **Certification Authority** console.
3. In the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.
4. On the **General** tab, click **View Certificate**, click the **Details** tab, and then click **Copy to File**.
5. In the **Certificate Export Wizard**, click **Next**.
6. On the **Export file format** page, click **Next**.
7. In the **File Name** text box, type **c:\AdatumRootCA.cer**, click **Next**, and then click **Finish**.
8. Click **OK** three times, and then close the **Certification Authority** console.

### Import a root CA certificate on a client

1. Switch to **LON-CL1**, click **File Explorer**, and then open **\\172.16.0.10\C\$**.
2. Install the **Root.cer** certificate on **LON-CL1** to **Local Machine** by selecting the **Place all certificates in the Trusted Root Certification Authorities** option.
3. Open a command prompt, type **mmc**, and then add the **Certificate -Local Computer** snap-in.
4. In the **Certificates** console, in the navigation pane, navigate to **Trusted Root Certification Authorities\Certificates**, and then verify that the **AdatumCA** certificate exists.



**Note:** These steps will import the **AdatumCA** certificate into the Trusted Root Certification Authorities store, so that clients will trust the certificate on the VPN server and establish a VPN connection by using the SSTP protocol.

### Connect to VPN by using IKEv2 and SSTP

1. Switch to **Network and Sharing Center**, and then open the **A. Datum VPN Properties** dialog box.
2. On the **Security** tab, select both **IKEv2** and **Use Extensible Authentication Protocol (EAP)**.
3. Disconnect the **A. Datum VPN**, and then connect again.
4. Open the **A. Datum VPN** connection, and then sign in with the user name **Adatum\logan** and the password **Pa\$\$w0rd**.
5. Verify that the connection is established by using the IKEv2 protocol.
6. Open the **Adatum VPN Properties** dialog box, and then on the **Security** tab, select both **Secure Socket Tunneling Protocol (SSTP)** and **Use Extensible Authentication Protocol (EAP)**.
7. Disconnect the **A. Datum VPN**, and then connect once again.
8. If the **Network sign-in** dialog box displays, sign in with the user name **Adatum\logan** and the password **Pa\$\$w0rd**.
9. Verify that now the connection is established by using the SSTP protocol.



**Note:** Do not disconnect the A. Datum VPN connection.

**► Task 4: Sign in to the domain by using VPN**

1. On **LON-CL1**, open a command prompt, type **mmc**, and then press Enter.
2. In the **Console** window, click **File**, and then click **Add/Remove Snap-in**.
3. Select **Group Policy Object Editor**, click **Add**, click **Finish**, and then click **OK**.
4. In the **Console** window, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
5. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**, select **Enabled**, and then click **OK**.
6. Close the window.
7. Open **System**, click **Advanced system settings**, and then click the **Computer Name** tab.
8. On the **Computer name** tab, click **Change**.
9. In the **Computer Name/Domain Changes** dialog box, click **Domain**, in the **Domain** text box, type **adatum.com**, and then click **OK**.
10. In the **Windows Security** dialog box, use **adatum\administrator** as **User name** and **Pa\$\$w0rd** as **Password**, and then click **OK**.
11. In the **Welcome to the adatum.com domain** dialog box, click **OK**.
12. In the **Computer Name/Domain Changes** dialog box, click **OK**.
13. To close the **System Properties** dialog box, click **Close**.
14. Click **Restart Now**.

**► Task 5: Verify connectivity**

1. When **LON-CL1** has restarted, press Ctrl+Alt+End.
2. On the **sign-in** screen, click the **Network sign-in** icon.
3. On the **Network sign-in** screen, sign with the user name **Adatum\logan** and the password **Pa\$\$w0rd**.



**Note:** You now are signed in to the domain via the VPN connection.

4. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have verified that the clients that cannot connect by using DirectAccess now can connect by using VPN, and that they can use Network Sign-in to sign in directly to the domain.

## Exercise 3: Troubleshoot VPN access

### Scenario

Logan has complained because he cannot connect to the A. Datum VPN. You received an incident report, and you must investigate and fix the issue.

Incident Record	
Incident Reference Number: IN24578	
Date of Call	November 8
Time of Call	13:42
User	Logan Boyle (IT department)
Status	OPEN
<b>Incident Details</b> The A. Datum VPN connection is suddenly not working on Logan's computer, and he cannot access intranet resources from his home network.	
<b>Additional Information</b> <ul style="list-style-type: none"> <li>Logan cannot connect to intranet resources from home.</li> <li>Logan must be able to connect by using VPN from his computer, LON-CL1.</li> </ul>	
<b>Plan of Action</b>	

The main tasks for this exercise are as follows:

1. Read the help-desk incident record for incident IN24578.
2. Update the **Plan of Action** section of the incident record.
3. Try to connect by using the A. Datum VPN connection on Logan's computer (**LON-CL1**).
4. Implement the fix, and test the solution.
5. Prepare for the next module.

#### ► Task 1: Read the help-desk incident record for incident IN24578

- Read the help-desk incident record **IN24578**.

#### ► Task 2: Update the Plan of Action section of the incident record

1. Read the **Additional information** section of the incident record.
2. Update the **Plan of Action** section of the incident record with your recommendations.

#### ► Task 3: Try to connect by using the A. Datum VPN connection on Logan's computer (LON-CL1)

1. On **LON-CL1**, sign in with the user name **.\Admin** and the password **Pa\$\$w0rd**. If prompted, click **Yes**.
2. Right-click **Start**, and then click **Command Prompt (Admin)**. When prompted, click **Yes**.

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

```
cd C:\Labfiles\Mod08
```

- At the command prompt, type the following commands, and then press Enter after each one:

```
PowerShell
.\Mod8LabB.ps1
```

- Wait for the script to complete.
- Type **.\Mod8LabB.ps1** to run the script a second time and wait for it to complete.
- Right-click **Start**, and then click **Network Connections**.
- Double-click the **A. Datum VPN** icon.
- On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
- Sign in as **Adatum\logan** with the password **Pa\$\$wOrd**.
- Wait for the connection to fail, and then write down the error message in the **Plan of Action** section of the incident record in the Student Handbook. (If the connection is successful, disconnect and the re-attempt the connection. It should fail.)

► **Task 4: Implement the fix, and test the solution**

- On **LON-CL1**, click the **File Explorer** icon, in the address bar, type **\\172.16.0.10\C\$\**, and then press Enter.
- Click **Use another account**. When prompted for the username and password, type **Adatum\Administrator** and **Pa\$\$wOrd**.
- Right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
- In the **Open File – Security Warning** dialog box, click **Open**.
- On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
- In the **User Account Control** dialog box, click **Yes**.
- On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
- On the **Certificate Store** page, click **Next**, and then click **Finish**.
- In the **Certificate Import Wizard**, click **OK**.
- Right-click **Start**, and then click **Command Prompt**.
- In the **Command Prompt** window, type **mmc**, and then press Enter. When prompted by UAC, click **Yes**.
- In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
- In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
- In the **Certificates snap-in** dialog box, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
- In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**. Verify that **AdatumCA** exists.
- In the **Network Connections** window, double-click the **A. Datum VPN** icon.

17. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
18. In the **Network sign-in** dialog box, in the **User name** text box, type **Adatum\logan**, in the **Password** text box, type **Pa\$\$w0rd**, and then click **OK**.
19. Verify that you are now able to connect to the **A. Datum** VPN server.

**Results:** After completing this exercise, you should have resolved the VPN access issue successfully, and Logan should be able to connect to the A. Datum VPN.

#### ► Task 5: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for: **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-INET1**, and **20741A-LON-CL1**.

**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?

**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?

**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?

## Module Review and Takeaways

### Review Questions

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

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

### 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
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

### 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 unsecure.
- You can restrict connections to your VPN server by user name or IP address.

# Module 9

## Implementing networking for branch offices

### Contents:

Module Overview	9-1
<b>Lesson 1:</b> Networking features and considerations for branch offices	9-2
<b>Lesson 2:</b> Implementing DFS for branch offices	9-12
<b>Lab A:</b> Implementing DFS for branch offices	9-25
<b>Lesson 3:</b> Implementing BranchCache for branch offices	9-28
<b>Lab B:</b> Implementing BranchCache	9-37
Module Review and Takeaways	9-42

## Module Overview

Branch offices can provide challenges for network administrators. When organizations have centralized infrastructure, such as database servers in a datacenter or file servers in the head office, access from branch offices is often limited because of the decreased network bandwidth of wide area network (WAN) connections.

In this module, you will learn several different ways that you can use Windows Server 2016 to overcome the limitations of branch office scenarios.

### Objectives

After completing this module, you will be able to:

- Describe networking features and considerations for branch offices.
- Explain how to implement DFS for branch offices.
- Explain how to implement Windows BranchCache for branch offices.

## Lesson 1

# Networking features and considerations for branch offices

Branch office locations or other locations in your organization that are joined by WAN links require special consideration when planning and implementing networking solutions. You should consider the aspects of your Windows Server 2016 infrastructure that would require additional or alternate configuration when a WAN link between locations is involved, especially infrastructure that involves centrally located Windows Server 2016 computers in the datacenter or head office.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe the scenarios related to branch offices.
- Identify the considerations for branch office network connectivity.
- Identify the options available in Windows Server 2016 for providing network connectivity to branch offices.
- Explain the considerations for providing Active Directory Domain Services (AD DS) and Domain Name System (DNS) services to branch offices.
- Explain the considerations for providing presentation virtualization to branch offices.
- Explain the considerations for providing file services to branch offices.
- Explain the considerations for providing print services to branch offices.

### Scenarios for branch offices

Providing adequate levels of information technology resources to the users in branch offices can be a challenging task. The most common scenarios are unreliable or slow WAN connections, offices with a small number of users, lack of information technology (IT) staff, lack of security, and dependency on infrastructure that resides in the head office.

#### Unreliable or slow WAN connection

Your branch office location might have a WAN connection to the datacenter or head office, where centralized infrastructure and services are hosted. If the branch office location depends on connectivity to centralized services, an unreliable or slow network connection can be frustrating for users and make it difficult to provide services that require constant connectivity or high bandwidth. Companies that do not have dedicated WAN connections and that use site-to-site virtual private network (VPN) connections might also have reliability and bandwidth issues.

Several scenarios affect the IT infrastructure in branch offices:

- Unreliable or slow WAN connection
- Small user population in branch office
- Lack of IT staff in branch office
- Lack of physical security or secure infrastructure storage
- Dependency on head office infrastructure



### Small group of users

Some branch locations might have only a few users, sometimes fewer than five. It is often difficult to justify placing infrastructure resources into branch offices with so few users. If a branch office does not have onsite server infrastructure, it can be a challenge to provide branch office users with the same functionality as users in locations with server resources. Small branch offices with slow WAN connections face additional problems because all communication with centralized servers, such as AD DS domain controllers, DNS servers, file servers, or application servers, must be transmitted over the WAN link.

### Lack of IT staff

When a branch office location does not have IT staff, it can be difficult to provide adequate management for its on-premises infrastructure. Common administrative tasks such as server backup, routine maintenance, upgrades, and troubleshooting must be performed either by local users, who might lack training and expertise, or remote IT staff, who might find administration tasks difficult or impossible to perform from their offsite location.

### Lack of physical security or secure infrastructure storage

Your branch office locations might not have the secure locations to store server infrastructure that most head offices and datacenters have. If you cannot physically secure a server, such as in a locked server cabinet, the server is susceptible to theft, damage, or environmental influences, such as heat and humidity. Servers that contain important organizational information cannot be located in such conditions. The lack of this infrastructure can negatively affect the productivity of branch office users.

### Dependency on head office infrastructure

When a branch office must access resources from a datacenter or head office location, WAN connectivity becomes critical to the operation of that location. If the WAN connection is unavailable, the branch location cannot operate. Similarly, if the files or applications hosted on a server become unavailable because of server failure or maintenance, productivity at the branch location is affected.

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

## Branch office considerations

Several factors can determine which configuration is suitable for a branch office. Along with technical considerations, such as service redundancy and server performance, you must also consider business requirements such as available personnel and legal or regulatory factors.

The following list highlights the considerations that are important when determining how to provide services to a branch office:

- Security. Hosting services in a branch office can introduce potential security risks. Considerations such as the physical security of servers or encryption levels on the WAN should be factored into a decision regarding where to host services.



- Availability and reliability. The quality of a branch office's WAN link to the head office or datacenter is usually the most significant factor that can affect availability and reliability. If a branch office cannot always contact a server in the head office as a result of an unreliable WAN link, the better choice is often to host that server in the branch location. However, the server's dependencies on other services, the lack of proper disaster recovery, or infrastructure redundancy at the branch office location can prevent relocation.
- Performance and capacity. The key determiner for the location of a service or application might be simple performance requirements. If a branch location cannot provide or host the hardware required by an application or service, central hosting in the datacenter is the only option. Conversely, if a branch office's WAN link is limiting the performance of an application or service, the resources for that application or service might need to be relocated to the branch office.
- 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. For example, a branch office might not be able to host encrypted data on a file server because of legal requirements for availability of data within those countries.
- IT organization. Head office sites and branch office locations often have different IT resources available to manage onsite infrastructure. It is important to record and consider IT resources when determining how to provide a service. For example, if the branch office does not have an onsite database administrator, it might not be viable to locally locate multiple servers that host business-critical databases running Microsoft SQL Server.
- Business considerations. The political structure of your organization can affect service placement. For each service, you should determine whether any political factors such as ownership, need for autonomy, or isolation could limit where a service is located.
- Cost. Typically, centralizing server infrastructure results in greater cost savings. IT support, power and energy, and building rental and maintenance are a few of the costs that can be decreased by employing a centralized server infrastructure. If servers are hosted in a branch office, you must consider the costs that your organization will incur in these areas.

## Options for providing network connectivity to branch offices

From a network perspective, branch offices are typically characterized by the presence of a WAN connection between the branch office and a head office or central hub. Individual branch offices can be connected to each other by using WAN links, but the connection to the head office should usually be your primary consideration. The key characteristics of WAN connections are as follows:

- Link type. Link type is one of the most important characteristics. Leased lines that provide point-to-point connection to branch offices over a private network connection are the most robust and require the least security consideration, but they are also the most expensive. VPN links, which encrypt and send traffic over the Internet, are less secure than leased lines. However, Internet-based WAN links are less expensive than leased lines and often provide more bandwidth relative to their cost.

- A WAN link is the most critical component for providing network services
- WAN link properties include:
  - Link type
  - Link bandwidth
  - Link latency
  - Link utilization
  - Link reliability
- Use the Remote Access role to provide secure WAN links over Internet connections

- **Link bandwidth.** Link bandwidth is a critical parameter for a WAN link. You can provide more services when that WAN link can handle more bandwidth. Typically, a higher bandwidth WAN enables you to host more services within the head office location and provide those services over the WAN link, similar to the way you would provide services to LAN clients.
- **Link latency.** *Latency* specifies the amount of time that a WAN link takes to send a packet between link endpoints. Latency has significant impact on two-way communications and can affect the perceived bandwidth of a WAN link. Latency is typically measured based on round-trip packet travel. High-latency links often provide low performance, especially when an application or service, such as Remote Desktop Services, requires constant two-way communication.
- **Link utilization.** *Link utilization* is the percentage of total link capacity being consumed. Links with high utilization can appear slow to applications that do not have high priority on the link. For this reason, many WAN links have the ability to establish Quality of Service (QoS) to give higher priority to important traffic.
- **Link reliability.** *Reliability* refers to the consistency in the quality of the bandwidth and availability of the WAN link. A WAN link that has periods of downtime or limited bandwidth is considered unreliable and might not be suitable for hosting business-critical network traffic.

### **Establishing WAN connectivity by using the Remote Access role**

The Remote Access role in Windows Server 2016 provides service for the VPN role, which you can use to configure a Windows Server 2016 VPN server.

You can use the Remote Access Management console to enable VPN by using one of the two wizards:

- **Getting Started Wizard.** Use this wizard to configure a server hosting VPN with basic configuration settings. This configuration can be useful for testing or establishing internal or basic VPN environments.
- **Remote Access Setup Wizard.** Use this wizard to configure a server hosting VPN with custom settings that provide the security and functional requirements of your organization.

### **VPN Server**

You can use the Windows Server 2016 VPN server to configure a VPN connection for individual VPN clients, which mobile users typically use, or you can configure it to work with a VPN server in another location in a site-to-site configuration. Site-to-site VPN configurations enable client computers in the branch office to operate without requiring individual VPN client connections. Using a site-to-site VPN configuration is common when connecting two locations by using VPN. All VPN-related traffic is routed through VPN servers at the branch office and head office, both of which encrypt and transmit the data over the Internet connection.

## Considerations for providing AD DS and DNS services to branch offices

A number of factors specific to the infrastructure design and behavior of AD DS domain controllers and DNS servers make providing AD DS and DNS services to branch offices challenging. The recommended best practice for hosting AD DS and DNS databases is to co-locate them on a single server because of the interdependency of AD DS and DNS. In such a configuration, every writeable AD DS domain controller also functions as a writeable DNS server and participates in standard replication of the two services with other writeable domain controllers.

An RODC provides the following services to branch offices:

- Read-only AD DS
- Read-only DNS
- Credential caching
- Administrative role separation

For a branch office, you have two options for providing AD DS and DNS services by using writeable domain controllers:

- Host domain controllers in the head office. This configuration removes the requirement for infrastructure in the branch office and ensures that replication between domain controllers happens reliably. However, this configuration is also dependent on the WAN link to enable communications between client computers and domain controllers. If the WAN link is unavailable, the connectivity to a domain controller is also unavailable, which impacts the functionality of the client computer significantly.
- Host one or more domain controllers in the branch office. Doing so removes the functional dependency on the WAN link, because branch office clients can contact a domain controller on the LAN to perform AD DS-related tasks. However, this configuration also requires physical infrastructure in the branch office and requires that AD DS and DNS replication traffic be sent across the WAN link.

### Implementing read-only domain controllers to provide AD DS and DNS services for branch offices

You can use a read-only domain controller (RODC) in a branch office to provide locally available AD DS and DNS services without the security and replication concerns that are associated with a writeable domain controller. An RODC has a read-only copy of an Active Directory domain, which contains all of the domain's objects but not all of the objects' attributes. System-critical attributes, such as passwords, do not replicate to an RODC because passwords are not considered secure. You can prevent additional attributes from being replicated to RODCs by marking the attribute as confidential and adding it to the filtered attribute set.

#### ***Understanding RODC functionality***

You cannot make changes to the domain database on the RODC, because the AD DS database on the RODC does not accept modification requests from clients and applications. All requests for changes are forwarded to a writable domain controller. Because no changes occur on the RODC, there is one-way replication of AD DS changes, from the writeable controller to the RODC.

#### ***Credential caching***

By default, user and computer credentials are not replicated to an RODC. To use an RODC to enhance user logon, you must configure a Password Replication Policy (PRP) that defines which user credentials can be cached. Limiting the credentials cached on the RODC reduces security risks. If the RODC is stolen, only passwords for the cached user and computer accounts must be reset.

If user and computer credentials are not replicated to an RODC, a writable domain controller must be contacted during the authentication process. In a branch office scenario, the credentials for users and computers in the branch location typically are cached on an RODC. When RODCs are placed in a perimeter network, the credentials for users and computers are not cached.

### ***Administrative role separation***

To manage a writable domain controller, you must be a member of the domain local Administrators group. Any user placed in the domain local Administrators group is given permissions to manage all domain controllers in the domain. This causes problems for remote-office administration with a writable domain controller, because the administrator in a remote office should not have access to the organization's other domain controllers.

Administrative role separation gives the administrator of a remote office permission to manage only that RODC, which might also be configured to provide other services such as file shares and printing.

### ***Read-only DNS***

DNS is a critical resource for a Windows network. If you configure an RODC as a DNS server, you can replicate DNS zones through AD DS to the RODC. DNS on the RODC is read-only. DNS update requests are referred to a writable copy of DNS.

### ***Deploying RODCs***

To deploy an RODC, do the following:

- Ensure that the forest functional level is Windows Server 2008 or newer. This means that all domain controllers must be Windows Server 2008 or newer, and each domain in the forest must be at the domain functional level of Windows Server 2008 or newer.
- Run `adprep/rodcrep`. This action configures permissions on DNS application directory partitions to allow them to replicate to RODCs. This is required only in a forest where the domain controller has been upgraded from Windows Server 2003 to Windows Server 2008 or Windows Server 2008 R2.
- Ensure that there is a writable domain controller running Windows Server 2008 or newer. An RODC replicates the domain partition only from these domain controllers. Therefore, each domain with RODCs must have at least one domain controller running Windows Server 2008 or newer. You can replicate the Schema and Configuration partitions from Windows Server 2008.

### ***RODC installation***

As with a writable domain controller, you can install an RODC by using an attended or an unattended installation. If you perform an attended installation by using the graphical interface, you select the RODC as one of the additional domain controller options.

You also can delegate the RODC installation to the administrator in the remote office by using a staged installation. In a staged installation, the following steps must be performed:

1. Ensure that the server to be configured as the RODC is not a member of the domain.
2. A domain administrator uses Active Directory Users and Computers or the Active Directory Administrative Center to pre-create the RODC account in the Domain Controllers organizational unit. The wizard for performing this process prompts for the necessary information, including the user or group that is allowed to join the RODC to the domain.
3. The administrator in the remote office runs the AD DS installation wizard and follows the steps in the wizard to join the domain as the pre-created RODC account.

## Considerations for implementing presentation virtualization for branch offices

*Presentation virtualization* involves running applications or desktop environments on a server, and then displaying the application or desktop on a remote client. Clients connect to the presentation virtualization server by using a remote desktop client, and then interact with the application or desktop in much the same way as if the application or operating system were running locally. By using presentation virtualization, users can run resource-intensive applications from relatively inexpensive client computers.

Presentation virtualization also enables applications and the server infrastructure that supports those applications to be hosted in the same network environment, increasing the network performance of the application and reducing the amount of bandwidth consumed between the client and the application server infrastructure.

Presentation virtualization can help you provide applications and services to branch offices in which server resources are not available to host applications, or when client computers do not meet the minimum requirements for an application or a service. You can run the application or service in the head office on suitably configured hardware. Then, you can connect to the server from the branch office so that you can use the application or service by using presentation virtualization.

- Remote Desktop Services allows users to run Windows-based applications remotely or to access full desktops virtually from multiple types of devices
- Installation of the Remote Desktop Services role is scenario-based
- Benefits include:
  - Quick deployment of applications
  - Ease of application maintenance
  - Support for multiple device types
  - High-end applications can be run from low-end systems
  - Good performance across slow connections

### Using Remote Desktop Services for presentation virtualization

*Remote Desktop Services* is a server role in the Windows Server 2016 operating system. It enables users to access remote computers or Windows-based programs that are installed on a Remote Desktop Session Host (RD Session Host) server, or to access a full Windows virtual desktop to run applications.

Remote Desktop Connection (RDC) client software enables users to connect to remote desktops and to run applications that are installed on an RD Session Host server. RDC client software also can connect to a Remote Desktop Virtualization Host (RD Virtualization Host) to request a virtual desktop running on a virtual machine from a Hyper-V host.

You can extend Remote Desktop Services across the Internet to support remote users who work from home, branch offices, public computers, client sites, or any place where there is access to an Internet connection. Most types of devices, including tablets and mobile devices, are supported.

Remote Desktop Services has two major components:

- Virtual machine-based desktop deployment. This provides users with access to a full Windows client operating system, such as Windows 8.1, based on a virtual machine.
- Session-based virtualization deployment. This provides users the ability to connect to an RD Session Host server and run remote applications as if they were installed locally on their computers.

### Benefits of Remote Desktop Services

Deploying applications to an RD Session Host server instead of on each client computer provides many benefits, such as:

- Applications can be deployed quickly to the whole organization.
- Application interoperability—clipboard sharing and moving data between applications—is improved.
- Applications can be upgraded and maintained more easily because they are installed on centralized servers.

- Users can access Remote Desktop Services from many types of computing devices.
- Applications that have high RAM and CPU requirements can be run by users on systems that have low computing power, because all the data processing takes place on the server.
- Remote Desktop Services provides good performance across low-speed connections. Programs that have intensive data interactions with other back-end services, such as SQL, can perform better over a Remote Desktop Services session than across typical WAN connections.

## Considerations for providing file services to branch offices

File services is one of the first and most common server roles configured on a network. Providing shared files and folders to network users is an important part of your network's functionality. From a branch office perspective, providing access to network file services can be problematic, primarily because of WAN bandwidth or reliability constraints. When access to file services from a branch office does not meet the requirements of your organization, you can use Windows Server 2016 to improve access to file services across the WAN for branch office clients.

The File and Storage Services role has several features that can improve network file access from branch offices:

- DFS
- BranchCache
- SMB 3.0

## Implementing the File and Storage Services Role for branch offices

You can use role services within File and Storage Services to make files and folders hosted on file servers running Windows Server 2016 more accessible to branch office locations. You use DFS to replicate and synchronize files to and from branch office servers, whereas you use BranchCache to provide access to locally-cached network files for clients within the branch office location.

### **DFS**

DFS makes use of efficient compression and transmission technology to replicate file and folder structures between file servers. You can use DFS to host an exact copy of a file share in a branch office, synchronize branch office files to a central location, distribute centrally stored files to branch office file servers, or maintain synchronization of files between multiple branch offices.

### **BranchCache**

BranchCache is implemented on network file servers to enable client computers in branch office locations to maintain cached copies of network files locally or on a BranchCache host server in their location. Clients in the branch office use the cached copies of the network files instead of copying them again from the head office file server. BranchCache is designed to reduce file traffic over WAN links and is especially effective for file shares in which frequently accessed, but infrequently changed, files exist.

### **Server Message Block 3.0**

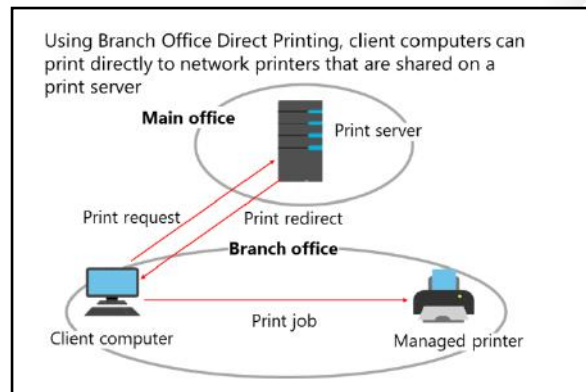
Windows Server 2016 supports server message block (SMB) 3.0 file shares, which make the most effective use of WAN and network bandwidth between clients and servers. In Windows Server 2016, SMB 3.0 supports several features that can be used to provide better access to files for branch office locations:

- SMB Encryption provides end-to-end encryption of SMB data. This feature is valuable when you must provide shared folder access over an untrusted network or prevent the interception of SMB data over the network. SMB Encryption can be enabled on a per-share or entire server basis.

- SMB Multichannel enables the network bandwidth and network fault tolerance to be aggregated if multiple paths are available between the SMB 3.0 client and the SMB 3.0 server. SMB Multichannel enables server applications to take full advantage of all available network bandwidth to a branch office and be resilient if a WAN link fails, provided multiple paths are available over the network to the branch office.
- SMB Directory Leasing enables a longer-living directory cache, which clients use for access to metadata for SMB 3.0 file shares. This means that roundtrips from client to server are quicker.

## Considerations for providing print services to branch offices

Print services are required in most enterprise networks. You can configure network printing by using Windows Server 2016 as a print server for users. In this configuration, client computers submit print jobs to the print server for delivery to a printer that is connected to the network. When print servers are centrally located in the head office and provide connectivity to branch office printers, data from print jobs must make two trips over the WAN link: one from the client computer sending the print job in the branch office to the print server in the head office, and another from the print server to the printer located in the branch office. This configuration consumes extra WAN bandwidth but is widely used because of the benefits of centralized network printing.



### Benefits of network printing

The benefits of network printing are the following:

- Centralized management. The biggest benefit of using Windows Server 2016 as a print server is centralized management of printing. Instead of managing client connections to many individual devices, you manage their connections to the server. You install printer drivers centrally on the server, and then distribute them to workstations.
- Simplified troubleshooting. By installing printer drivers centrally on a server, you also simplify troubleshooting. Determining whether printing problems are caused by the printer, server, or client computer is relatively easy.
- Lower costs. A network printer is more expensive than typical local printers, but the cost of consumables for a network printer is lower and the printing quality is better. Therefore, the cost of printing is minimized, because the initial cost of the printer is offset by the number of computers that can connect to it. For example, a single network printer could service 100 users or more.
- Users can search for printers easily. You can publish network printers in AD DS so that users can search for printers in their domain.



## Using Branch Office Direct Printing

Branch Office Direct Printing reduces network costs for organizations that have centralized their Windows Server roles. When Branch Office Direct Printing is enabled, Windows clients obtain printer information from the print server but send the print jobs directly to the printer. The print data no longer travels to the central server and then back to the branch office printer. This configuration reduces traffic between the client computer, the print server, and the branch office printer, and results in increased network efficiency.

Branch Office Direct Printing is transparent to the user. In addition, the user can print even if the print server is unavailable for some reason (for example, if the WAN link to the datacenter is down). The user can do this because the printer information is cached on the client computer in the branch office.

## Configuring Branch Office Direct Printing

You can configure Branch Office Direct Printing by using the Print Management console or a Windows PowerShell command-line interface.

To configure Branch Office Direct Printing from the Print Management console, perform the following steps:

1. In **Server Manager**, open the **Print Management** console.
2. In the navigation pane, expand **Print Servers**, and then expand the print server that is hosting the network printer for which Branch Office Direct Printing will be enabled.
3. Click the **Printers** node, right-click the desired printer, and then click **Enable Branch Office Direct Printing**.

To configure Branch Office Direct Printing by using Windows PowerShell, type the following cmdlet at a Windows PowerShell prompt:

```
Set-Printer -name "<Printer Name Here>" -ComputerName <Print Server Name Here>  
-RenderingMode BranchOffice
```

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

## Lesson 2

# Implementing DFS for branch offices

Providing files across multiple locations can be a challenging task. You must consider how to maintain easily accessible files and balance that access with file consistency between locations. You can use DFS to provide highly available, easily accessible files to branch offices. DFS performs WAN-friendly replication between multiple locations and is capable of maintaining consistency between file locations.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how to implement DFS namespaces.
- Explain how to implement DFS replication.
- Describe the scenarios for implementing DFS.
- Plan DFS deployment.
- Explain how to optimize namespaces and replication.
- Explain how to configure DFS namespaces and replication.
- Manage DFS databases.
- Explain how to monitor and troubleshoot DFS.

### Implementing DFS namespaces

You can use DFS namespaces to create a virtual representation of shared folder structures. You can create either a domain-based or standalone namespace. Each type has different characteristics.

#### Domain-based namespaces

A domain-based namespace can be used when:

- High availability of the namespace is required. This is accomplished by replicating the namespace to multiple namespace servers.
- You must hide the name of the namespace servers from users. Domain-based namespace servers also make it easier to replace a namespace server or migrate the namespace to a different server. Users can then access the `\\domainname\namespace` format as opposed to the `\\servername\share` format.

DFS namespaces can be configured as:

- Domain-based namespaces
- Stand-alone namespaces

To configure a namespace for publishing content:

1. Create a namespace
2. Create a folder in the namespace
3. Add folder targets
4. Set the ordering method for targets in referrals

Windows Server provides support for access-based enumeration, and it increases the number of folder targets from 5,000 to 50,000. With access-based enumeration, you can also hide folders that users do not have permission to view.

To use the DFS features, the following requirements must be met:

- The AD DS forest must be at the forest functional level of Windows Server 2008 or newer.
- The AD DS domain must be at the domain functional level of Windows Server 2008.
- All namespace servers must be running Windows Server 2008 or newer version.

## Standalone namespaces

A standalone namespace is used when:

- An organization has not implemented AD DS.
- An organization does not meet the requirements for a domain-based namespace, and there are requirements for more than 5,000 DFS folders. Standalone DFS namespaces support up to 50,000 folders with targets.
- An organization is hosting a DFS namespace in a failover cluster.

## Deploying DFS namespaces

Most DFS implementations consist primarily of content that is published within the DFS namespace. To configure a namespace for publishing content to users, perform the following procedures:

1. Create a namespace. Use the **New Namespace Wizard** to create the namespace from within the DFS Management console. When a new namespace is created, you must provide the name of the server that you want to use as the namespace server, namespace name, and type (either domain-based or standalone). You can also specify whether the namespace is enabled for Windows Server 2008 mode.
2. Create a folder in the namespace. After you create the namespace, add a folder in the namespace that will be used to contain the content that you want to publish. While creating the folder, you have the option to add folder targets, or you can perform a separate task to add, edit, or remove folder targets later.
3. Add folder targets. After you create a folder within the namespace, the next task is to create folder targets. The folder target is a shared folder's Universal Naming Convention (UNC) path on a specific server. You can browse for shared folders on remote servers and create shared folders as needed. Additionally, you can add multiple folder targets to increase the folder's availability in the namespace. If you add multiple folder targets, consider using DFS Replication (DFSR) to ensure that the content is the same between the targets.
4. Set the ordering method for targets in referrals. A *referral* is an ordered list of targets that a client computer receives from the namespace server when a user accesses a namespace root or folder. When a client receives the referral, the client attempts to access the first target in the list. If the target is not available, the next target is attempted. By default, targets in the client's site are always listed first in the referral. You can configure the method for ordering targets outside the client's site on the **Referrals** tab of the **Namespace Properties** dialog box. You have the choice of configuring the lowest cost and random order, or configuring the ordering method to exclude targets outside the client's site.



**Note:** Folders inherit referral settings from the namespace root. You can override the namespace settings on the **Referrals** tab of the **Folder Properties** dialog box by excluding targets outside the client's site.

## Optional management tasks

You can use a number of optional management tasks to modify DFS namespace behavior:

- Set target priority to override referral ordering. You can have a specific folder target that you want everyone to use from all site locations or a specific folder target that should be used last among all targets. You can configure these scenarios by overriding the referral ordering on the **Advanced** tab of the **Folder Target Properties** dialog box.

- Enable client failback. If a client cannot access a referred target, the next target is selected. *Client failback* ensures that clients fail back to the original target after it is restored. You can configure client failback on the **Referrals** tab of the **Namespace Properties** dialog box by selecting the **Clients Fail Back To Preferred Targets** check box. All folders and folder targets inherit this option. However, you can also override a specific folder to enable or disable client failback features, if required.
- Replicate folder targets by using DFSR. You can use DFSR to keep the contents of folder targets in sync. The next topic discusses DFSR in detail.

## Implementing DFS replication

DFSR provides a way to keep folders synchronized between servers across well-connected and limited bandwidth connections. The following are the characteristics of DFSR:

- DFSR uses *remote differential compression*, which is a client-server protocol that can be used to efficiently update files over a limited bandwidth network. Remote differential compression detects data insertions, removals, and rearrangements in files, enabling DFSR to replicate only the changed file blocks when files are updated. By default, remote differential compression is used only for files that are 64 kilobytes (KB) or larger. DFSR also supports cross-file remote differential compression, which allows DFSR to use remote differential compression, even when a file with the same name does not exist at the client. Cross-file remote differential compression can determine files that are similar to the file that needs to be replicated; it uses blocks of similar files that are identical to the replicating file to minimize the amount of data that needs to be replicated.
- DFSR uses a hidden staging folder to stage a file before sending or receiving it. Staging folders act as caches for new and changed files to be replicated from sending members to receiving members. The sending member begins staging a file when it receives a request from the receiving member. The process involves reading the file from the replicated folder and building a compressed representation of the file in the staging folder. After it has been constructed, the staged file is sent to the receiving member; if remote differential compression is used, only a fraction of the staging file might be replicated. The receiving member downloads the data and builds the file in its staging folder. After the file download completes on the receiving member, DFSR decompresses the file and installs it into the replicated folder. Each replicated folder has its own staging folder, which by default is located in the local path of the replicated folder in the `DfsrPrivate\Staging` folder.
- DFSR detects volume changes by monitoring the file system update sequence number (USN) journal and replicates changes only after the file is closed.
- DFSR uses a version vector exchange protocol to determine which files must be synchronized. The protocol sends less than 1 KB per file across the network to synchronize the metadata associated with changed files on the sending and receiving members.

- When DFSR is implemented, it:
  - Uses remote differential compression
  - Uses a staging folder to stage a file before sending or receiving the file
  - Detects changes on the volume by monitoring the USN journal
  - Uses a vector version exchange protocol
  - Recovers from failure
- Configure and manage DFSR by using the cmdlets from the DFSR module for Windows PowerShell

- DFSR uses a conflict resolution heuristic of *last writer wins* for files that are in conflict (that is, a file that is updated at multiple servers simultaneously) and *earliest creator wins* for name conflicts. Files and folders that lose the conflict resolution are moved to a folder known as the *Conflict and Deleted folder*. You can also configure the service to move deleted files to the Conflict and Deleted folder for retrieval, should the file or folder be deleted. Each replicated folder has its own hidden Conflict and Deleted folder, which is located in the local path of the replicated folder in the DfsrPrivate\ConflictandDeleted folder.
- DFSR is self-healing and can automatically recover from USN journal wraps, USN journal loss, or DFSR database loss.
- DFSR uses a Windows Management Instrumentation (WMI) provider that provides interfaces to obtain configuration and monitoring information from the DFSR service.

### Deploying and configuring DFSR

After a DFS namespace and folder target are created, you can enable DFSR by configuring a replication group and enabling replication between group members.

### Additional DFSR functionalities

The DFSR functionality also includes the following additions:

- Windows PowerShell module for DFSR. There are several new Windows PowerShell cmdlets that are available to perform administrative tasks for DFS.
- WMI provider. This provider enables the latest WMI-based methods for managing DFS.
- Database prestaging for initial sync. When prestaging DFSR data, you can bypass the initial replication phase when you create new replicated folders.
- Database corruption recovery. This feature enables you to rebuild corrupt databases without data loss resulting from nonauthoritative initial sync.
- File staging tuning. You can configure variable file staging sizes on individual servers.

### DFSR module for Windows PowerShell

You can configure and manage DFSR by using the cmdlets from the DFSR module for Windows PowerShell. The DFSR module supplies new cmdlets for managing all facets of DFSR functionality.

For example, the following cmdlet creates a new replication folder named Promotions and adds it to the replication group named Adatum-Marketing.

```
New-DfsReplicatedFolder -GroupName "Adatum_Marketing" -FolderName "Promotions"
```

This example retrieves the members of the Adatum\_Marketing DFSR replication group on LON-SVR1.

```
Get-DfsrMember -GroupName "Adatum_Marketing" -ComputerName "LON-SVR1"
```

To view all of the cmdlets available in the DFSR module for Windows PowerShell, use the following Windows PowerShell cmdlet.

```
Get-Command -Module DFSR
```

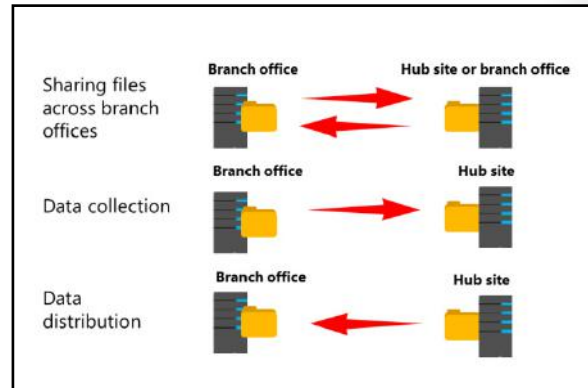
## Scenarios for implementing DFS

You can implement DFS 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.

### Sharing files across branch offices

Large organizations that have many branch offices often have to share files or collaborate between these locations. DFS can help replicate files between branch offices or from a branch office to a hub site. Having files in multiple branch offices also benefits users who travel from one branch office to another. The changes that users make to their files in a branch office are replicated to other branch offices.



**Note:** This scenario is recommended only if users can tolerate some file inconsistencies, because changes are replicated throughout the branch servers. Also, note that DFS replicates a file only after it is closed. Therefore, DFS is not recommended for replicating database files or any files that are held open for long periods of time.

### Data collection from branch offices

DFS technologies can collect files from a branch office and replicate them to a hub site, thus allowing the files to be used for a number of specific purposes. Critical data can be replicated to a hub site by using DFS and then backed up at the hub site by using standard backup procedures. This increases data recoverability at the branch office if a server fails, because files will be available and backed up in two separate locations. Additionally, companies can reduce branch office costs by eliminating backup hardware and onsite IT personnel expertise. Replicated data can also be used to make branch office file shares fault tolerant. If the branch office server fails, clients in the branch office can access the replicated data at the hub site.

### Data distribution to branch offices

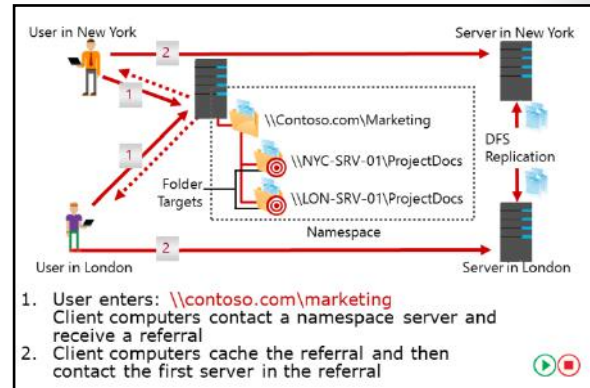
You can use DFS to publish and replicate documents, software, and other line-of-business (LOB) data throughout your organization. DFS can also increase data availability and distribute client load across various file servers.

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

## Planning for DFS

When implementing DFS, you must have a general understanding of the overall topology of your DFS implementation. In general, DFS topology functions as follows:

1. The user accesses a folder in the virtual namespace. When a user attempts to access a folder in a namespace, the client computer contacts the server that is hosting the namespace root. The host server can be a standalone server that is hosting a standalone namespace, or a domain-based configuration that is stored in AD DS and then replicated to various locations to provide high availability. The namespace server sends back to the client computer a referral containing a list of servers that host the shared folders (called *folder targets*) and are associated with the folder being accessed. DFS is a site-aware technology, so, to ensure the most reliable access, client computers can be configured to access the namespaces that arrive within their site first.
2. The client computer accesses the first server in the referral. A *referral* is a list of targets that a client computer receives from a domain controller or namespace server when the user accesses a root or folder with namespace targets. The client computer caches the referral information and then contacts the first server in the referral. This referral typically is a server in the client's own site, unless no server is located within the client's site. In this case, the administrator can configure the target priority.



On the slide example, the Marketing folder that is published within the namespace actually contains two folder targets. One share is located on a file server in New York, and the other share is located on a file server in London. The shared folders are kept synchronized by DFSR. Even though multiple servers host the source folders, this fact is transparent to users, who access only a single folder in the namespace. If one of the target folders becomes unavailable, users are redirected to the remaining targets within the namespace.

### Permissions required to create and manage a DFS namespace

To perform DFS namespace management tasks, a user either has to be a member of an administrative group or has to be delegated specific permission to perform the task. To delegate the required permissions, right-click the namespace, and then click **Delegate Management Permissions**.

The following table describes the groups that can perform DFS administration by default and the method for delegating the ability to perform DFS management tasks.

Task	Groups that can perform the task by default	Delegation method
Create a domain-based namespace	Domain admins	Click <b>Delegate Management Permissions</b> .
Add a namespace server to a domain-based namespace	Domain admins	Add users to local administrators group on the namespace server.
Manage a domain-based namespace	Local administrators on each namespace server	Click <b>Delegate Management Permissions</b> .

Task	Groups that can perform the task by default	Delegation method
Create a standalone namespace	Local administrators on each namespace server	Add users to local administrators group on the namespace server.
Manage a standalone namespace	Local administrators on each namespace server	Click <b>Delegate Management Permissions</b> .
Create a replication group, or enable DFSR on a folder	Domain admins	Add users to local administrators group on the namespace server.

### Using Data Deduplication

Data Deduplication can help provide a more robust and efficient DFS environment when combined with DFSR:

- Capacity optimization. Data Deduplication enables a server to store more data in less physical disk space.
- Scale and performance. Data Deduplication is highly scalable in Windows Server 2016. It can run on multiple volumes without affecting other services and applications running on the server. Data Deduplication can be throttled to accommodate other heavy workloads on the server so that no performance degradation occurs for important server tasks.
- Reliability data integrity. Windows Server 2016 uses checksum consistency and validation to ensure that the integrity of data affected by Data Deduplication remains intact. Data Deduplication also maintains redundant copies of the most frequently used data on a volume to protect against data corruption.
- Bandwidth efficiency. In combination with DFSR, Data Deduplication can greatly reduce the bandwidth consumed when replicating file data, provided that replication partners are also running Windows Server 2016.
- Simple optimization management. Windows Server 2016 and Windows PowerShell 5.0 contain integrated support for Data Deduplication. Implementation and management within Windows Server 2016 is accomplished with familiar tools.

When you want to configure Data Deduplication for use with DFS, you enable it on the volume or volumes that are hosted in the replicated DFS folders. You must enable Data Deduplication for volumes on all Windows Server 2016-based computers that are participating in the DFSR topology.

**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?



## Optimizing namespaces and replication

DFS has a number of configuration options with which you can optimize its usability and performance. Options include renaming or moving a folder, disabling referrals to a folder, specifying the referral cache duration, configuring namespace polling, creating replication groups, creating multiple replication folders, and modifying replication topology.

You can optimize DFS by:

- Renaming or moving a folder
- Disabling referrals to a folder
- Specifying referral cache duration
- Configuring namespace polling
- Configuring replication groups
- Creating multiple replicated folders
- Modifying replication topology

### Rename or move a folder

You can rename or move a folder in a namespace.

This capability enables you to reorganize the hierarchy of folders to best suit your

organization's users. For example, when your company reorganizes, you can reorganize the namespace to match the new structure.

### Disable referrals to a folder

By disabling a folder target's referral, you prevent client computers from accessing that folder target in the namespace. This is useful when you are moving data between servers.

### Specify referral cache duration

Clients do not contact a namespace server for a referral each time they access a folder in a namespace; instead, namespace root referrals are cached. Clients that use a cached referral renew the cache duration value of the referral each time a file or folder is accessed using the referral. This means that the clients use the referral indefinitely until the client's referral cache is cleared or the client is restarted. You can customize the referral cache duration. The default time is 300 seconds (5 minutes).

### Configure namespace polling

To maintain a consistent domain-based namespace across namespace servers, namespace servers must poll AD DS periodically to obtain the most current namespace data. The two modes for namespace polling are:

- Optimize for consistency. Namespace servers poll the primary domain controller (PDC) emulator each time a namespace change occurs. This activity is the default.
- Optimize for scalability. Each namespace server polls its closest domain controller at periodic intervals.

### Configure replication groups

You can configure replication groups for two different purposes:

- Multipurpose replication group. This replication group helps to configure replication between two or more servers for publication, content sharing, or other scenarios.
- Replication group for data collection. This replication group configures a two-way replication between two servers, such as a branch office server and a hub server. This group type is used to collect data from the branch office server to the hub server. You can then use standard backup software to back up the hub server data.

## Create multiple replicated folders

A replicated folder is synchronized between each member server. Creating multiple replicated folders within a single replication group helps to simplify the following for the entire group:

- Replication group type
- Topology
- Hub and spoke configuration
- Replication schedule
- Bandwidth throttling

The replicated folders that are stored on each member can be located on different volumes in the member. Replicated folders do not need to be shared folders or part of a namespace, although the DFS Management snap-in makes it easy to share replicated folders and, optionally, publish them to an existing namespace.

## Modify replication topology

When configuring a replication group, you can modify its topology to provide the most effective replication. To do so, select among the following:

- Hub and spoke. To select this option, you require at least three member servers in the replication group. This topology works well in publication scenarios in which data originates at the hub and is replicated to members at the spokes.
- Full mesh. If 10 or fewer members are in the replication group, this topology works well, with each member replicating to all others, as required.
- No topology. Choose this option if you want to manually configure a custom topology after creating the replication group.

## Demonstration: Configuring DFS namespaces and replication

In this demonstration, you will see how to:

- Install the DFS Replication role service.
- Create a new namespace.
- Create a new folder and folder target.
- Configure DFSR.

### Demonstration Steps

#### Install the DFS Replication role service

1. On **LON-SVR1**, under the **File and Storage Management** role, install the **DFS Namespaces** and **DFS Replication** role services.
2. Repeat steps 1 and 2 for **TOR-SVR1**.

#### Create a new namespace

1. Open the **DFS Management** console.
2. Create a domain-based namespace on **LON-SVR1** named **Research**.

### Create a new folder and folder target

1. Create a new folder named **Proposals** in the **\\Adatum.com\Research** namespace.
2. Create a folder target for **Proposals** that points to **\\LON-SVR1\Proposal\_docs**.
3. Confirm namespace functionality by browsing to **\\Adatum.com\Research** and then confirming that the **Proposals** folder is displayed.

### Create a new folder target for replication

- On **LON-SVR1**, create a folder target for **\\TOR-SVR1\Proposal\_docs**.

### Create a new replication group

1. Add the **Proposal\_docs** folder to the replication group for **LON-SVR1** and **TOR-SVR1**.
2. Declare **LON-SVR1** as the primary member, and then create a full-mesh replication.

## Managing DFS databases

DFS includes database management tasks that use database cloning to help administrators perform initial database replication. Furthermore, DFS includes tasks that can recover the DFS database in the event of data corruption.

### DFS database cloning

The initial replication can take a long time to complete and can consume a large amount of bandwidth when replicating a large set of files. Windows Server 2016 provides a feature that clones the database for the initial replication. To create a clone of the database, use the **Export-DfsrClone** cmdlet to export the DFSR database and volume configuration XML file settings for a given local computer volume. On a large dataset, exports may take a long time to complete. You can use the **Get-DfsrCloneState** cmdlet to determine the status of the export operation.

After you clone the data and copy the exported database and XML file to the new DFS member server, use the **Import-DfsrClone** cmdlet to inject the database onto a volume and validate the files on the file system. This provides dramatic performance improvements during the initial synchronization.

The following cmdlet exports a database and creates a clone of the database in a folder named **Dfsrclone**.

```
Export-DfsrClone -Volume C: -Path "C:\Dfsrclone"
```

After copying the cloned database to the C:\Dfsrclone folder on the new DFS member server, use the following cmdlet to import the cloned database.

```
Import-DfsrClone -Volume C: -Path "C:\Dfsrclone"
```

#### When managing a DFS database:

- Use these cmdlets to clone a DFS database:
  - **Export-DfsrClone**
  - **Import-DfsrClone**
- Use these cmdlets to recover a DFS database:
  - **Get-DfsrPreservedFiles**
  - **Restore-DfsrPreservedFiles**

## DFS database recovery

When DFSR detects database corruption, it rebuilds the database and then resumes replication normally, with no files arbitrarily losing conflicts. When replicating with a read-only partner, DFSR resumes replication without waiting indefinitely for an administrator to set the primary flag manually. The database corruption recovery feature rebuilds the database by using local file and USN information and marks each file with a normal replicated state. You cannot recover files from the ConflictAndDeleted and Preexisting folders except from backup. Use the Windows PowerShell cmdlets **Get-DfsrPreservedFiles** and **Restore-DfsrPreservedFiles** to allow the recovery of files from these folders. You can restore these files and folders into their previous location or a new location. You can choose to move or copy the files, and you can keep all versions of a file or only the latest version.

## Monitoring and troubleshooting DFS

Windows Server 2016 provides a number of tools that you can use to monitor and troubleshoot DFS. The tools include:

- Diagnostic Reports. Use Diagnostic Reports to run a diagnostic report for the following:
  - Health Report. Shows extensive replication statistics and reports on replication health and efficiency.
  - Propagation Test. Generates a test file in a replicated folder to verify replication and provide statistics for the propagation report.
  - Propagation Report. Provides information about the progress of the test file that is generated during a propagation test. This report ensures that replication is functional.
- Verify Topology. Use Verify Topology to verify and report on the status of the replication group topology. This reports any members that are disconnected.
- Dfsrdiag.exe. Use this command-line tool to monitor the replication state of the DFSR service.

Tool	Use
Health Report	Report replication statistics and general health of the topology
Propagation Test	Generate a test file to verify replication
Propagation Report	Report on the propagation test and provide replication statistics
Verify Topology	Report on the current status of the members of the topology
Dfsrdiag.exe	Monitor replication state of the DFS replication service
Windows PowerShell	Configure, monitor, and troubleshoot DFS

## Using Windows PowerShell to monitor and troubleshoot DFS

DFS has a complete set of Windows PowerShell cmdlets that you can use to monitor and troubleshoot DFS. Windows Server 2016 provides a new DFSR module for Windows PowerShell that you can use to manage all aspects of DFS replication. You can access the cmdlets listed in the following tables by installing the DFS role services or by installing the DFS Tools from Remote Server Administration Tools (RSAT).

### Commonly used DFS Namespace Windows PowerShell cmdlets

Cmdlet	Description
<b>Get-DfsnAccess</b>	Gets permissions for a DFS namespace folder
<b>Get-DfsnFolder</b>	Gets settings for a DFS namespace folder
<b>Get-DfsnFolderTarget</b>	Gets settings for targets of a DFS namespace folder
<b>Get-DfsnRoot</b>	Gets settings for DFS namespaces

Cmdlet	Description
<b>Get-DfsnRootTarget</b>	Gets settings for root targets of a DFS namespace
<b>Get-DfsnServerConfiguration</b>	Gets DFS namespace settings for a DFS namespace root server
<b>Grant-DfsnAccess</b>	Grants permissions to users and groups to access a DFS namespace folder
<b>Move-DfsnFolder</b>	Moves or renames a DFS namespace folder
<b>New-DfsnFolder</b>	Creates a folder in a DFS namespace
<b>New-DfsnFolderTarget</b>	Adds a target to a DFS namespace folder
<b>New-DfsnRoot</b>	Creates a DFS namespace
<b>New-DfsnRootTarget</b>	Adds a root target to a DFS namespace
<b>Remove-DfsnAccess</b>	Removes users and groups from the ACL for a folder in a DFS namespace
<b>Remove-DfsnFolder</b>	Removes a DFS namespace folder
<b>Remove-DfsnFolderTarget</b>	Removes a target for a DFS namespace folder
<b>Remove-DfsnRoot</b>	Removes a DFS namespace
<b>Remove-DfsnRootTarget</b>	Removes a target for a DFS namespace root
<b>Revoke-DfsnAccess</b>	Revokes permissions for users to access and enumerate the contents of a DFS namespace folder
<b>Set-DfsnFolder</b>	Changes settings for a DFS namespace folder
<b>Set-DfsnFolderTarget</b>	Changes settings for a target of a DFS namespace folder.
<b>Set-DfsnRoot</b>	Changes settings for a DFS namespace
<b>Set-DfsnRootTarget</b>	Changes settings for a root target of a DFS namespace
<b>Set-DfsnServerConfiguration</b>	Changes settings for a DFS namespace root server

### ***Commonly used DFSR Windows PowerShell cmdlets***

Cmdlet	Description
<b>Get-DfsrBacklog</b>	Retrieves the list of pending file updates between two DFS Replication partners
<b>Get-DfsrCloneState</b>	Gets the status of a database cloning operation
<b>Get-DfsrConnection</b>	Gets a connection between DFS Replication partners
<b>Get-DfsrConnectionSchedule</b>	Gets a connection schedule between DFS Replication partners.
<b>Get-DfsReplicatedFolder</b>	Gets a replicated folder from a replication group

Cmdlet	Description
<b>Get-DfsReplicationGroup</b>	Retrieves a replication group
<b>Get-DfsrGroupSchedule</b>	Retrieves a replication group schedule
<b>Get-DfsrMember</b>	Gets member computers in a replication group
<b>Get-DfsrMembership</b>	Gets membership settings for members of replication groups
<b>Get-DfsrServiceConfiguration</b>	Gets settings for the DFS Replication service on group members
<b>Get-DfsrState</b>	Gets the DFS Replication state for a member
<b>Reset-DfsrCloneState</b>	Cancels a cloning operation
<b>Start-DfsrPropagationTest</b>	Creates a propagation test file in a replicated folder
<b>Suspend-DfsReplicationGroup</b>	Suspends replication between computers regardless of schedule
<b>Sync-DfsReplicationGroup</b>	Synchronizes replication between computers regardless of schedule
<b>Update-DfsrConfigurationFromAD</b>	Initiates an update of the DFS Replication service
<b>Write-DfsrHealthReport</b>	Generates a DFS Replication health report
<b>Write-DfsrPropagationReport</b>	Generates reports for propagation test files in a replication group

### Troubleshooting DFS

DFS problems generally fall into one of the following categories:

- Inability to access the DFS namespace. Ensure that both the Net Logon service and DFS service are running on all servers that are hosting the namespace.
- Inability to find shared folders. If clients cannot connect to a shared folder, use standard troubleshooting techniques to ensure that the folder is accessible and that clients have permissions. Remember that clients connect to the shared folder directly.
- Inability to access DFS links and shared folders. Verify that the underlying folder is available and that the client has permissions on it. If a replica exists, verify whether the problem is related to replication latency (refer to the replication latency entry in this list).
- Security-related issues. Remember that the client accesses the shared folder directly. Therefore, you must verify the shared folder and access control list (ACL) permissions on the folder.
- Replication latency. Remember that the DFSR topology is stored in the domain's AD DS. Consequently, there is some latency before any modification to the DFS Namespaces is replicated to all domain controllers.

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

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

## Lab A: Implementing DFS for branch offices

### Scenario

A. Datum has several key shared folders that must be accessible to users in Sydney and Toronto. The folders are accessed by users in Sydney only a few times per day, but are accessed from Toronto constantly throughout the day. To ensure that users have the optimal experience when accessing the files, A. Datum has decided to implement DFSR for the users in Toronto.

### Objectives

1. Implement DFS for the Toronto branch office.
2. Validate the deployment.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and, in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - o User name: **Adatum\Administrator**
  - o Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**.

## Exercise 1: Implementing DFS

### Scenario

The Toronto office of A. Datum Corporation has a single server, **TOR-SVR1**. To support branch staff requirements, you must configure DFS to replicate a shared folder named BranchDocs between **LON-SVR1** and **TOR-SVR1**. To avoid having to perform backups remotely, the BranchDocs folder in the London location will be replicated with **TOR-SVR1** to provide quicker access to the files, while still maintaining the files in London for centralized backup.

The main tasks for this exercise are as follows:

1. Install the DFS role on **LON-SVR1** and **TOR-SVR1**.
2. Create the BranchDocs DFS namespace.
3. Add the DataFiles folder to the BranchDocs namespace.

4. Create a folder target for DataFiles on **TOR-SVR1**.
  5. Configure replication for the namespace.
- **Task 1: Install the DFS role on LON-SVR1 and TOR-SVR1**
1. On **LON-SVR1**, in **Server Manager**, under the **File and Storage Management** role, install the **DFS Namespaces** and **DFS Replication** role services.
  2. Repeat step 1 on **TOR-SVR1**.
- **Task 2: Create the BranchDocs DFS namespace**
1. Switch to **LON-SVR1**.
  2. Open **DFS Management**.
  3. Create a new namespace with the following properties:
    - Server: **LON-SVR1**
    - Name: **BranchDocs**
    - Namespace type: **Domain-based namespace**, and select **Enable Windows Server 2008 mode**
  4. Under the **Namespaces** node, verify that the namespace has been created.
- **Task 3: Add the DataFiles folder to the BranchDocs namespace**
- On **LON-SVR1**, add a new folder to the **BranchDocs** namespace:
    - Folder name: **DataFiles**
    - Add a folder target:
    - Path: **\\LON-SVR1\DataFiles**
    - Create the share
    - Local path: **C:\BranchDocs\DataFiles**
    - Permissions: **All users have read and write permissions**
- **Task 4: Create a folder target for DataFiles on TOR-SVR1**
1. On **LON-SVR1**, in **DFS Management**, expand **Adatum.com\BranchDocs**, and then click **DataFiles**.
  2. In the **details** pane, notice that there is currently only one folder target.
  3. Add a new folder target:
    - Path to target: **\\TOR-SVR1\DataFiles**
    - Create the share
    - Local path: **C:\BranchDocs\DataFiles**
    - Permissions: **All users have read and write permissions**
    - Create the folder
  4. In the **Replication** dialog box, click **Yes**. The **Replicate Folder Wizard** starts.



► **Task 5: Configure replication for the namespace**

1. Complete the **Replicate Folder Wizard**:
  - Primary member: **LON-SVR1**
  - No topology
  - Use defaults elsewhere, and accept any messages
2. Create a new replication topology for the namespace:
  - Type: **Full mesh**
  - Schedule and bandwidth: Use default settings
3. In the details pane, on the **Memberships** tab, verify that the replicated folder displays on both **TOR-SVR1** and **LON-SVR1**.

**Results:** Upon completion of this exercise, you will have implemented DFS.

## Exercise 2: Validating the deployment

### Scenario

You must now verify that the file services availability configuration you implemented for the Toronto and Sydney locations are functioning properly.

The main task for this exercise is as follows:

1. Verify DFSR functionality for **TOR-SVR1**

► **Task 1: Verify DFSR functionality for TOR-SVR1**

1. On **LON-SVR1**, in **File Explorer**, navigate to **\\Adatum.com\BranchDocs\Datafiles**.
2. Create a new text file named **Repltest.txt**.
3. In **File Explorer**, navigate to **C:\BranchDocs\Datafiles**, and then confirm that the **Repltest.txt** file is located in the folder.
4. Switch to **TOR-SVR1**.
5. On **TOR-SVR1**, in **File Explorer**, navigate to **C:\BranchDocs\Datafile**, and then confirm that the **Repltest.txt** file is located in the folder.



**Note:** If Repltest.txt does not appear within 1 minute or even after refreshing the view, restart **TOR-SVR1**.

**Results:** Upon completion of this exercise, you will have validated the deployment of DFS in branch offices.

## Lesson 3

# Implementing BranchCache for branch offices

Branch offices have unique management challenges. A branch office typically has slow connectivity to the enterprise network and limited infrastructure for securing servers. In addition, you must back up data that you maintain in your remote branch offices, which is why organizations prefer to centralize data where possible. Therefore, the challenge is providing efficient access to network resources for users in branch offices. BranchCache helps you overcome these problems by caching files so they do not have to be transferred repeatedly over the network.

### Lesson Objectives

After completing this lesson, you will be able to:

- Explain how BranchCache works.
- Describe the requirements for BranchCache.
- Describe how BranchCache modes work.
- Explain how to configure BranchCache server settings.
- Explain how to configure BranchCache client settings.
- Explain how to use BranchCache for servers.
- Explain how to monitor and troubleshoot BranchCache.

### How does BranchCache work?

BranchCache reduces the network use on WAN connections between branch offices and headquarters by locally caching frequently used files on computers in the branch office. BranchCache improves the performance of applications that use one of the following protocols:

- HTTP or HTTPS. These protocols are used by web browsers and other applications.
- Server message block, including signed SMB traffic protocol. This protocol is used for accessing shared folders.
- Background Intelligent Transfer Service (BITS). BITS is a Windows component that distributes content from a server to clients by using only idle network bandwidth. Microsoft System Center Configuration Manager also uses BITS.

When the client requests data, BranchCache retrieves it from a server. Because BranchCache is a passive cache, it does not increase WAN use. BranchCache caches only the read requests and does not interfere when a user saves a file.

#### The benefits of BranchCache include:

- Reducing the network use on WAN connections between branch offices and headquarters
- Locally caching frequently used files on computers in the branch office
- Improving the performance of applications that use one of the following protocols:
  - HTTP or HTTPS
  - Server message block, including signed SMB traffic protocol
  - Background Intelligent Transfer Service

BranchCache improves the responsiveness of common network applications that access intranet servers across slow WAN links. Because BranchCache does not require additional infrastructure, you can improve the performance of remote networks by enabling its functionality. BranchCache is supported on client operating systems Windows 7 and newer, and server operating systems Windows Server 2008 R2 and newer.

BranchCache works seamlessly with network security technologies, including Secure Sockets Layer (SSL), SMB signing, and end-to-end IPsec. You can use BranchCache to reduce network bandwidth use and to improve application performance, even if the content is encrypted.

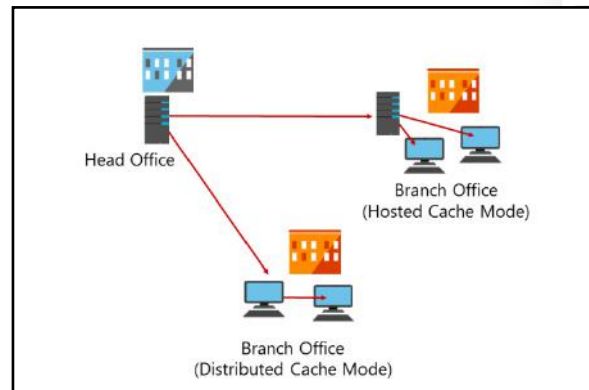
BranchCache functionality in Windows Server 2016 has the following benefits:


- Allows for scaling. BranchCache allows for more than one hosted cache server per location.
- An underlying database uses the Extensible Storage Engine (ESE) database technology from Exchange Server. This enables a hosted cache server to store up to terabytes of data.
- You do not need a Group Policy Object (GPO) for each location. To deploy BranchCache, you need only a single GPO that contains the settings. This also enables clients to switch between hosted cache mode and distributed mode when they are traveling and moving client computers between locations, without needing to use site-specific GPOs.

## Understanding BranchCache modes

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

- **Hosted cache mode.** This mode operates by deploying a computer that is running Windows Server 2008 R2 or newer versions as a hosted cache server in the branch office. Client computers locate the host computer so that they can retrieve content from the hosted cache when the hosted cache is available. If the content is not available in the hosted cache, the content is retrieved from the content server over a WAN link. The content is then provided to the hosted cache, which serves successive client requests.
- **Distributed cache mode.** For smaller remote offices, you can configure BranchCache in the distributed cache mode without requiring a server. In this mode, local client computers running Windows 7 or newer maintain a copy of the content and make it available to other authorized clients that request the same data. This eliminates the need to have a server in the branch office. However, unlike the hosted cache mode, this configuration works per subnet only. In addition, clients that hibernate or disconnect from the network cannot provide content to other requesting clients.



 **Note:** When using BranchCache, you can use both modes in your organization, but you can configure only one mode per branch office.

## How client computers retrieve data by using BranchCache in hosted and distributed cache modes

When BranchCache is enabled on both a client computer and on a server, and when the client computer is using the HTTP, HTTPS, or SMB protocol, the client computer performs the following process to retrieve data:

1. The client computer connects to a content server in the head office and requests content similarly to the way it would retrieve content without using BranchCache.
2. The content server in the head office authenticates the user and verifies that the user is authorized to access the data.
3. Instead of sending the content itself, the content server in the head office returns identifiers or hashes of the requested content to the client computer. The content server sends that data over the same connection that the content would have typically been sent.
4. Using retrieved identifiers, the client computer does the following:
  - o If you configure the client computer to use distributed cache, the client computer multicasts on the local subnet to find other client computers that have already downloaded the content.
  - o If you configure the client computer to use hosted cache, the client computer searches for the content on the configured hosted cache.
5. If the content is available in the branch office, either on one or more clients or on the hosted cache, the client computer retrieves the data from the branch office. The client computer also ensures that the data is updated and has not been tampered with or corrupted.
6. If the content is not available in the remote office, the client computer retrieves the content directly from the server across the WAN link. The client computer then either makes the content available on the local network to other requesting client computers (distributed cache mode), or sends it to the hosted cache, where it is made available to other client computers.

## BranchCache requirements

BranchCache optimizes traffic flow between head offices and branch offices. Server operating systems newer than Windows Server 2008 R2 and client operating systems newer than Windows 7 can benefit from using BranchCache. (Earlier versions of Windows operating systems do not benefit from this feature.) You can use BranchCache to cache only the content that is stored on file servers or web servers that are running Windows Server 2008 R2 or newer server operating systems.

- Requirements for using BranchCache:
  - Install the BranchCache feature and, optionally, BranchCache for Network Files role service
  - Configure client computers by using either Group Policy or the **netsh** command
- Requirements for the modes:
  - For the distributed cache mode, configure the client firewall to enable incoming traffic, HTTP, and WS-Discovery
  - For hosted cache mode, configure a firewall to enable incoming HTTP traffic from the hosted cache server

## Requirements for using BranchCache

To use BranchCache for file services, you must perform the following tasks:

- Install the BranchCache feature or the BranchCache for Network Files role service on the host server that is running Windows Server 2016.
- Configure client computers either by using Group Policy or the **netsh branchcache set service** command.

If you want to use BranchCache to cache content from the file server, you must perform the following tasks:

- Install BranchCache for the Network Files role service on the file server.
- Configure hash publication for BranchCache.
- Create BranchCache-enabled file shares.

If you want to use BranchCache for caching content from the web server, you must install the BranchCache feature on the web server. You do not need additional configurations.

BranchCache is supported on the full installation and Server Core installation of Windows Server 2016. By default, BranchCache is not installed on Windows Server 2016.

## Requirements for distributed cache mode and hosted cache mode

In the distributed cache mode, BranchCache works without a dedicated server but rather between clients on the same site. If client computers are configured to use the distributed cache mode, any client computer can use a multicast protocol called WS-Discovery to search locally for the computer that has already downloaded and cached the content. You should configure the client firewall to enable incoming traffic: HTTP (TCP port 80), and WS-Discovery (UDP port 3702). Clients, however, will search for a hosted cache server, and if they discover one, will automatically self-configure as hosted cache mode clients.

In the hosted cache mode, the client computers automatically search for the host server so that they can retrieve content from the hosted cache. Furthermore, you can use Group Policy so that you can use the fully qualified domain name (FQDN) of the hosted cache servers or enable automatic hosted cache discovery by service connection points. You must configure a firewall to enable incoming HTTP traffic from the hosted cache server.

In both cache modes, BranchCache uses the HTTP protocol for data transfer between client computers and the computer that is hosting the cached data.

## Configuring BranchCache server settings

You can use BranchCache to cache web content, which is delivered by HTTP or HTTPS. You can also use BranchCache to cache shared folder content, which is delivered by the SMB protocol.

The following table lists the servers that you should configure for BranchCache and describes how to configure them.

You must configure the following BranchCache server components:

- Web server or BITS server
- File server
- Hosted cache server

Server	Description
Web server or BITS server	To configure a Windows Server 2016 web server or an application server that uses the BITS protocol, install the BranchCache feature. Ensure that the BranchCache service has started. Then, configure clients who will use the BranchCache feature. No additional web server configuration is required.
File server	Before you enable BranchCache for any file shares, you must install the BranchCache for the Network Files role service of the File Services server role. After you install the BranchCache for the Network Files role service, use Group Policy to enable BranchCache on the server. You must then configure each file share to enable BranchCache.
Hosted cache server	For the hosted cache mode, you must add the BranchCache feature to the Windows Server 2016 server that you are configuring as a hosted cache server.  To help secure communication, client computers use Transport Layer Security (TLS) when communicating with the hosted cache server.  By default, BranchCache allocates five percent of the disk space on the active partition for hosting cache data. However, you can change this value by using the Windows PowerShell <b>Set-BCCache</b> cmdlet or Group Policy or by running the <b>netsh branchcache set cachesize</b> command.

## Configuring BranchCache client settings

You do not have to install the BranchCache feature on client computers, because BranchCache is already included if the client is running Windows 7 or newer. However, BranchCache is disabled by default on client computers. To enable and configure BranchCache, you must perform the following steps:

1. Enable BranchCache.
2. Enable the distributed cache mode or the hosted cache mode. Windows 8 clients can use either mode dynamically.
3. Configure the client firewall to enable BranchCache protocols.

### Enabling BranchCache

You can enable the BranchCache feature on client computers by using Group Policy, Windows PowerShell, or the **netsh branchcache set service** command.

To enable and configure BranchCache:

1. Enable BranchCache by using Group Policy, Windows PowerShell, or **netsh branchcache set service**
2. Enable distributed cache mode or hosted cache mode by using Group Policy, Windows PowerShell, or **netsh branchcache set service**
3. Configure the client firewall

You can modify BranchCache settings and perform additional configuration tasks, such as:

- Setting the cache size
- Setting the location of the hosted cache server
- Clearing the cache
- Creating and replicating a shared key for using in a server cluster

To enable BranchCache settings by using Group Policy, perform the following steps for a domain-based GPO:

1. Open the **Group Policy Management** console.
2. Create a GPO that will be linked to the organizational unit in which client computers are located.
3. In the GPO, browse to **Computer Configuration\Policies\Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer\Network**, and then click **BranchCache**.
4. Enable the **Turn on BranchCache** setting in the GPO.

### Enabling the distributed cache mode or hosted cache mode

You can configure the BranchCache mode on client computers by using Group Policy, Windows PowerShell, or the **netsh branchcache set service** command.

To configure the BranchCache mode by using Group Policy, perform the following steps for a domain-based GPO:

1. Open the **Group Policy Management** console.
2. Create a GPO that will be linked to the organizational unit in which client computers are located.
3. In the GPO, browse to **Computer Configuration\Policies\Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer\Network**, and then click **BranchCache**.
4. Select either the distributed cache mode or the hosted cache mode. You can also enable both the distributed cache mode and automatic hosted cache discovery by Service Connection Point policy settings. The client computers operate in distributed cache mode unless they find a hosted cache server in the branch office. If they find a hosted cache server in the branch office, they work in hosted cache mode.

To enable BranchCache with Windows PowerShell, use the **Enable-BCDistributed** or **Enable-BCHostedServer** cmdlet. You can also use the **Enable-BCHostedClient** cmdlet to configure BranchCache to operate in hosted cache mode.

For example, the following cmdlet enables hosted cache mode by using the LON-SVR1.adatum.com computer as a hosted cache server for HTTPS and clients running Windows 10:

```
Enable-BCHostedClient -ServerNamesLON-SVR1.adatum.com -UseVersion Windows10
```

The following cmdlet enables hosted cache mode and register service connection point in AD DS:

```
Enable-BCHostedServer -RegisterSCP
```

The following cmdlet enables distributed cache mode on the server:

```
Enable-BCDistributed
```

To configure BranchCache settings by using the **netsh branchcache set service** command, open a Command Prompt window and perform the following steps:

1. Type the following **netsh** syntax for the distributed cache mode:

```
netsh branchcache set service mode=distributed
```

2. Type the following **netsh** syntax for the hosted cache mode:

```
netsh branchcache set service mode=hostedclient location=<hosted cache server>
```

### Configuring the client firewall to enable BranchCache protocols

In the distributed cache mode, BranchCache clients use the HTTP protocol for data transfer between client computers and the WS-Discovery protocol for cached content discovery. You should configure the client firewall to enable the following incoming rules:

- BranchCache–Content Retrieval (Use HTTP)
- BranchCache–Peer Discovery (Use WS–Discovery)

In hosted cache mode, BranchCache clients use the HTTP protocol for data transfer between client computers, but this mode does not use the WS-Discovery protocol. In the hosted cache mode, you should configure the client firewall to enable the incoming rule, BranchCache–Content Retrieval (Use HTTP).

### Additional configuration tasks for BranchCache

After you configure BranchCache, clients can access the cached data in BranchCache-enabled content servers, which are available locally in the branch office. You can modify BranchCache settings and perform additional configuration tasks, such as:

- Setting the cache size.
- Setting the location of the hosted cache server.
- Clearing the cache.
- Creating and replicating a shared key for using in a server cluster.

## Demonstration: Configuring BranchCache

In this demonstration, you will learn how to:

- Add BranchCache for the Network Files role service.
- Configure BranchCache in Local Group Policy Editor.
- Enable BranchCache for a file share.

### Demonstration Steps

#### Add BranchCache for the Network Files role service

1. Sign in to **LON-DC1** and open **Server Manager**.
2. In the **Add Roles and Features Wizard**, install the following role service to the local server:
  - **File and Storage Services (Installed)\File and iSCSI Services\BranchCache for Network Files**



### Enable BranchCache for the Server

1. On the **Start** screen, type **gpedit.msc**, and then press Enter.
2. Browse to **Computer Configuration\Administrative Templates\Network\Lanman Server**, and then do the following:
  - o Enable **Hash Publication for BranchCache**.
  - o Select **Allow hash publication only for shared folder on which BranchCache is enabled**.

### Enable BranchCache for a file share

1. Open a **File Explorer** window, and, on **drive C**, create a folder named **Share**.
2. Configure the **Share** folder properties as follows:
  - o Enable **Share this folder**.
  - o Check **Enable BranchCache** in **Offline Settings**.

### Using BranchCache for servers

Servers that use BranchCache represent BranchCache-enabled content servers. There are three types of servers that can act as BranchCache-enabled content servers:

- Web servers. You can configure your organization internal web servers as BranchCache-enabled content servers by installing the BranchCache feature on a computer running Internet Information Services (IIS) in the main office.
- File servers. File servers located in the organization main office can be enabled as BranchCache content servers by installing the File Services server role and the BranchCache for Network Files role service.
- Application servers. Application servers can be enabled as BranchCache-enabled content servers by installing and enabling BITS. Furthermore, BranchCache should be installed and enabled on the application server. For example, WSUS and Configuration Manager branch distribution points also can use BranchCache to share content across WAN links.

- BranchCache-enabled content servers include:
  - Web servers
  - Application servers
  - File servers
- WAN connectivity is critical for BranchCache

When configuring servers as BranchCache-enabled content servers, you should consider that WAN connectivity is required for BranchCache. The hosted cache server, or client in case of distributed cache, still requires access to the server that has BranchCache enabled to verify the hash for the file being accessed. BranchCache is not a high availability technology; it is used for file distribution in high latency or expensive WAN links.

## Monitoring BranchCache

After the initial configuration, verify that BranchCache is configured correctly and functioning correctly. You can use the **netsh branchcache show status all** command to display the BranchCache service status. You can also use the Windows PowerShell cmdlet **Get-BCStatus** to provide BranchCache status and configuration information. The client and hosted cache servers display additional information, such as the location of the local cache, the size of the local cache, and the status of the firewall rules for HTTP and WS-Discovery protocols that BranchCache uses.

The BranchCache monitoring tools include:

- **Netsh branchcache shows status all** command
- **Get-BCStatus** Windows Powershell cmdlet
- Event Viewer
- Performance monitor counters

You can also use the following tools to monitor BranchCache:

- **Event Viewer.** Use this tool to monitor the BranchCache events that are recorded in both the Application log and the Operational log. In the Event Viewer console, the Application log is located in **Windows Logs\Application**, and the Operational log is located in **Application and Service Logs\Microsoft\Windows\BranchCache**.
- **Performance counters.** Use this tool to monitor BranchCache performance monitor counters. BranchCache performance monitor counters are useful debugging tools for monitoring BranchCache effectiveness and health. You can also use BranchCache performance monitoring to determine the bandwidth savings in the distributed cache mode or in the hosted cache mode. If you have implemented Microsoft System Center 2012 Operations Manager in the environment, you can use the Windows BranchCache Management Pack for Operations Manager.

**Question:** What modes can you configure for BranchCache?

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

## Lab B: Implementing BranchCache

### Scenario

A. Datum Corporation has several key shared folders that must be accessible to users in remote locations. The Sydney office hosts files from a sales application that are routinely accessed by clients in the London location. The files are viewed only by London users, not edited, and their sizes range from 25 MB to 150 MB. Toronto users need access to files that are being hosted in London. These files, which users access throughout the day, are modified by London users and Toronto users, and the London users would like quick, reliable access to them. To ensure that users have the optimal experience when accessing the files, A. Datum Corporation has decided to implement BranchCache for the file shares located in Sydney, and DFSR for the users in Toronto.

### Objectives

After completing this lab, you should be able to:

- Implement DFS.
- Implement BranchCache.
- Validate the deployment.

### Lab Setup

Estimated Time: 45 minutes

Virtual machines: **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**, **20741A-LON-CL2**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**, and **20741A-LON-CL2**.

## Exercise 1: Implementing BranchCache

### Scenario

The users in the London location require intermittent access to several read-only files hosted on the **SYD-SVR1** file server in Sydney. You have been asked to configure **LON-SVR1** with BranchCache in hosted cache mode to provide cached files from the file share on **SYD-SVR1** and to configure London clients so that they can take advantage of the hosted cache on **LON-SVR1**.

The main tasks for this exercise are as follows:

1. Configure **SYD-SVR1** to use BranchCache.
2. Prepare a file share for BranchCache.
3. Configure client firewall rules for BranchCache.
4. Install the BranchCache feature on **LON-SVR1**.
5. Start the BranchCache host server on **LON-SVR1**.
6. Configure client computers to use BranchCache in the hosted cache mode.

#### ► Task 1: Configure SYD-SVR1 to use BranchCache

1. Switch to **SYD-SVR1**.
2. From **Server Manager**, install the **BranchCache for network files** role service.
3. Open the **Local Group Policy Editor (gpedit.msc)**.
4. Browse to and open **Computer Configuration/Administrative Templates/Network /Lanman Server/Hash Publication for BranchCache**.
5. Enable the **BranchCache** setting, and then select **Allow hash publication only for shared folders on which BranchCache is enabled**.

#### ► Task 2: Prepare a file share for BranchCache

1. On **SYD-SVR1**, in a **File Explorer** window, create a new folder named **C:\Share**.
2. Share this folder with the following properties:
  - Share name: **Share**
  - Permissions: **default**
  - Caching: **Enable BranchCache**
3. Copy **C:\Windows\System32\mspaint.exe** to the **C:\Share** folder.

#### ► Task 3: Configure client firewall rules for BranchCache

1. On **LON-DC1**, open **Group Policy Management**.
2. Browse to **Forest: Adatum.com\Domains\Adatum.com\Default Domain Policy**, and then open the policy for editing.
3. Browse to **Computer Configuration\Policies\Windows Settings\Security Settings \Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules**.

4. Create a new inbound firewall rule with the following properties:
    - o Rule type: **predefined**
    - o Use **BranchCache – Content Retrieval (Uses HTTP)**
    - o Action: **Allow**
  5. Create a new inbound firewall rule with the following properties:
    - o Rule type: **predefined**
    - o Use **BranchCache – Peer Discovery (Uses WSD)**
    - o Action: **Allow**
  6. Close the **Group Policy Management Editor** and **Group Policy Management** console.
- **Task 4: Install the BranchCache feature on LON-SVR1**
- On **LON-SVR1**, in **Server Manager**, add the **BranchCache for Network Files** role service and the **BranchCache** feature.
- **Task 5: Start the BranchCache host server on LON-SVR1**
1. On **LON-SVR1**, open **Windows PowerShell**, and run the following cmdlet:
 

```
Enable-BCHostedServer -RegisterSCP
```
  2. On **LON-SVR1**, in **Windows PowerShell**, run the following cmdlet:
 

```
Get-BCStatus
```
  3. Ensure that **Branch Cache** is enabled and running.
- **Task 6: Configure client computers to use BranchCache in the hosted cache mode**
1. On **LON-DC1**, open **Server Manager**, and then open **Group Policy Management**.
  2. Edit the **Default Domain Policy**.
  3. In the **Group Policy Management Editor**, browse to **Computer Configuration \Policies\Administrative Templates\Network\BranchCache**, and then configure the following:
    - o Turn on **BranchCache: Enabled**
    - o Enable **Automatic Hosted Cache Discovery by Service Connection Point: Enabled**
    - o Configure **BranchCache** for network files: **Enabled**
    - o Type the maximum round trip network latency (milliseconds) after which caching begins: **0**
  4. Start **20741A-LON-CL1** and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
  5. Open a **Command Prompt** window, and then refresh the **Group Policy** settings by using the command **gpupdate /force**.
  6. At the command prompt, type **netsh branchcache show status all**, and then press Enter.
  7. Verify that BranchCache is **Enabled** with status **Running** and that the options from Group Policy are applied. If the status is **Stopped**, repeat steps 5 and 6.
  8. Restart **20741A-LON-CL2** and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
  9. Open the **Command Prompt** window, and then refresh the **Group Policy** settings by using the command **gpupdate /force**.

10. At the command prompt, type **netsh branchcache show status all**, and then press Enter.
11. Verify that BranchCache is **Enabled** with status **Running** and that the options from Group Policy are applied. If the status is **Stopped**, repeat steps 9 and 10.

**Results:** Upon completion of this exercise, you will have implemented BranchCache.

## Exercise 2: Validating the deployment

### Scenario

You must now verify that the availability configuration you implemented for file services at the Toronto and Sydney locations are functioning properly.

The main tasks for this exercise are as follows:

1. Simulate slow link to the branch office.
2. Verify BranchCache functionality for **SYD-SVR1**.
3. Prepare for the next module.

#### ► Task 1: Simulate slow link to the branch office

1. On **SYD-SVR1**, open the **Local Group Policy Editor** (gpedit.msc).
2. Navigate to the following local policy node: **Computer Configuration\Windows Settings\Policy-based QoS**.
3. Create a new policy with the following settings:
  - o Name: **Limit to 100 Kbps**
  - o Specify Outbound Throttle Rate: **100**



**Note:** This task is required to simulate a slow network connection in a test environment where all the computers are connected by a fast network connection.


#### ► Task 2: Verify BranchCache functionality for SYD-SVR1

1. Switch to **LON-CL1**, and open **Performance Monitor**.
2. In the navigation pane of the **Performance Monitor** console, under **Monitoring Tools**, click **Performance Monitor**. Remove existing counters, change to a report view, and then add the **BranchCache** object to the report.
3. Repeat steps 1 and 2 for **LON-CL2** and **LON-SVR1**.
4. On **LON-CL1**, open **File Explorer**, and then copy **\\SYD-SVR1\Share\mspaint.exe** to the desktop.



**Note:** This file copy will take some time because of the 100-Kbps bandwidth limit that is placed on **SYD-SVR1**.

5. In **Performance Monitor**, select all counters, and then select **Scale selected counters**.


 **Note:** Note that several counters are no longer at zero, which indicates that BranchCache is active.

6. On **LON-SVR1**, switch to **Performance Monitor**, and then note that counter statistics reflect BranchCache activity on **LON-SVR1**.
7. On **LON-SVR1**, open a **Windows PowerShell** window, type the following command, and then press Enter.

```
Get-BCStatus
```

Note that under **DataCache**, the **CurrentActiveCacheSize** value is **6560896** bytes, which is the size of mspaint.exe.

8. On **LON-CL2**, open **File Explorer**, and then copy **\\SYD-SVR1\Share\mspaint.exe** to the desktop.

 **Note:** Note that the file copy time is much faster than to **LON-CL1**, because the file is cached on **LON-SVR1**.

### ► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**, and **20741A-LON-CL2**.

**Results:** Upon completion of this exercise, you will have validated the deployment of network services in branch offices.

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

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

## Module Review and Takeaways

### Review Questions

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

**Question:** How does BranchCache differ from the DFS?

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



# Module 10

## Configuring advanced networking features

### Contents:

Module Overview	10-1
<b>Lesson 1:</b> Overview of high-performance networking features	10-2
<b>Lesson 2:</b> Configuring advanced Hyper-V networking features	10-12
<b>Lab:</b> Configuring advanced Hyper-V networking features	10-23
Module Review and Takeaways	10-28

## Module Overview

Windows Server 2016 introduces advanced high-performance networking features, such as Server Message Block (SMB) 3.1.1, new Quality of Service (QoS) options, and several enhancements on the receiving end of network packet processing. Additionally, new networking features are available to the Microsoft Hyper-V role and to the virtual machines running under Hyper-V, such as expanded virtual switch functionality and extensibility, single-root I/O virtualization (SR-IOV), dynamic virtual machine queuing, and NIC Teaming for virtual machines.

In this module, you will learn how to deploy and configure the advanced networking enhancements in Windows Server 2016 and the new features in Hyper-V networking.

### Objectives

After completing this module, you will be able to:

- Describe the high-performance networking enhancements in Windows Server 2016.
- Configure the advanced Hyper-V networking features.

## Lesson 1

# Overview of high-performance networking features

Datacenters are becoming increasingly connected to the cloud, to other datacenters, and to servers within the datacenters themselves. This connectivity can slow down the overall performance of the servers. Microsoft has introduced several high-performance networking features to enhance connectivity performance. In this lesson, you will learn about the new and improved networking technologies that Windows Server 2016 introduces.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe NIC Teaming.
- Describe how to configure NIC Teaming.
- Describe how to implement SMB 3.1.1 shared folders.
- Describe advanced SMB 3.1.1 functionality.
- Explain how to provide SMB 3.1.1 high availability in remote storage.
- Describe QoS.
- Describe Receive Side Scaling (RSS).
- Describe receive segment coalescing (RSC).

### What is NIC Teaming?

NIC Teaming allows you to combine up to 32 network adapters and then use them as a single network interface. NIC Teaming provides redundancy, allowing network communication to occur over the combined network interface even when one or more of the network adapters fail. The combination of network adapters also increases the bandwidth available to the combined network interface. NIC Teaming is a feature that is available in the Windows Server 2016 operating system. Both the Hyper-V host and the Hyper-V virtual machines can use the NIC Teaming feature. A NIC team can contain only one network adapter, but when it has only one network adapter, the NIC team cannot provide load balancing and failover. Still, you can use a NIC team with only one network adapter in it for the separation of network traffic when you are also using virtual local area networks (VLANs).

- **NIC Teaming:**
  - Provides redundancy and aggregates bandwidth
  - Is supported at the host and virtual machine levels
- **Considerations for NIC Teaming:**
  - Deploy multiple network adapters on a physical host
  - Configure separate teams on different switches for fault tolerance

### Considerations for NIC Teaming

If you want to enhance the connectivity fault tolerance and performance of your Hyper-V host, you should deploy multiple network adapters to the host and then configure those adapters as part of a team. This helps to ensure that network connectivity will be retained if individual network adapters fail. Configure multiple teams with network adapters that are connected to different switches to help ensure that connectivity remains if a hardware switch fails.



**Note:** NIC Teaming within a virtual machine is discussed later in this module.

With Windows Server 2016, you can now use Switch Embedded Teaming (SET) within a Microsoft Hyper-V virtual switch to team up to eight physical network adapters into one or more software-based virtual network adapters. These virtual network adapters deliver fast performance and fault tolerance in the event of a network adapter failure. You must install SET member network adapters in the same physical Hyper-V host in order to be placed in a SET team. You can also use Remote Direct Memory Access (RDMA)-capable network adapters within a SET team, which allows you to use both RDMA and SET teams while utilizing fewer network adapters in your servers. This also means you don't have to team at the host level. The big benefit that this allows is the RDMA can be managed at the virtual switch.

Dynamic NIC Teaming was introduced as a new load balancing option in Windows Server 2012 R2. Dynamic NIC Teaming should be compared to the address hash method used prior to Dynamic NIC Teaming in Windows Server 2012 R2. With address hash, when a new data flow is detected, that flow is assigned statically to a team member. The assignment is not based on existing traffic on any of the members of the team. Once assigned, a flow will never move to another team member. This means it is possible for several very large flows to all be on the same team member, while other team members have little traffic. This can result in delayed or dropped packets for these over-used members. Dynamic NIC Teaming constantly watches flows and any time there is a pause, when the flow resumes the traffic on all members is evaluated and the flow moved to the members with less traffic. This means traffic is constantly rebalanced in order to avoid any one member having significantly more than others.

## Demonstration: Implementing NIC Teaming

In this demonstration, you will learn how to implement NIC Teaming.

### Demonstration Steps


1. On the **LON-HOST1**, open **Hyper-V Manager**, and then select the **Local Server** node.
2. In the **Local Server** node, create a NIC team that uses the **Ethernet 2** network adapter, and then name it **Host NIC Team**.
3. In the **NIC Teaming** dialog box, in the **Teams** pane, note the following details:
  - o Team: **Host NIC Team**
  - o Status: **OK**
  - o Teaming Mode: **Switch Independent**
  - o Load Balancing: **Dynamic**
  - o Adapters: **1**

## Implementing SMB 3.1.1 shared folders


The latest version of SMB is SMB 3.1.1, which was introduced in Windows 10 and Windows Server 2016. SMB 3.1.1 supports Advanced Encryption Standard (AES) 128 Galois/Counter Mode (GCM) encryption in addition to the AES 128 Counter with CBC-MAC (CCM) encryption that is included in SMB 3.0, and it applies a preauthentication integrity check by using the Secure Hash Algorithm (SHA) 512 hash. SMB 3.1.1 also requires a security-enhanced negotiation when connecting to devices that use SMB 2.x and later.

- SMB 3.1.1 is available only in Windows Server 2016; SMB 3.0 is available in Windows Server 2012; both have similar functionality
- Hyper-V 10.0 can store the following on SMB 3.1.1 file shares:
  - XML-based configuration files
  - Virtual hard disk files (in .vhd or .vhdx format)
  - Checkpoint files

Hyper-V supports storing virtual machine data, such as virtual machine configuration files, checkpoints, and virtual hard disk files, on SMB 3.0 and later file shares. The file share must support SMB 3.0. This limits the placement of virtual hard disks on file shares that are hosted on file servers that are running Windows Server 2012 or later. Earlier Windows Server versions do not support SMB 3.0.

 **Note:** We recommend that the bandwidth for network connectivity to the file share be 1 gigabit per second (Gbps) or more.

An SMB 3.0 file share provides an alternative to storing virtual machine files on Internet Small Computer System Interface (iSCSI) or Fibre Channel storage area network (SAN) devices. When creating a virtual machine in Hyper-V on Windows Server 2012 or later, you can specify a network share when choosing the virtual machine location and the virtual hard disk location. You also can attach disks stored on SMB 3.0 and later file shares. You can use both .vhd and .vhdx disks with SMB 3.0 or later file shares.

 **Additional Reading:** For more information, refer to: "Server Message Block Overview" at <http://aka.ms/obyww0>

Since Windows Server 2012 R2, Microsoft has improved SMB 3.0 to allow shared storage for guest clustering that is stored on an SMB 3.0 file server. SMB 3.1.1 continues to support this functionality on Windows Server 2016.

## Using advanced SMB 3.1.1 functionality

In Windows Server 2012 R2, several enhancements were made to SMB 3.0 functionality. Windows Server 2016 continues to support the SMB 3.0 enhancements as well as several advanced functions that you can employ by using SMB 3.1.1. For example, you can store virtual machine files on a highly available SMB 3.1.1 file share. This is referred to as a Scale-Out File Server. By using this approach, you achieve high availability not by clustering Hyper-V nodes but by using file servers that host virtual machine

- SMB 3.0 features that are introduced in Windows Server 2012:
  - SMB Transparent Failover
  - SMB Scale Out
  - SMB Multichannel
  - SMB Direct
  - SMB Encryption.
  - VSS for SMB file shares
  - SMB Directory Leasing
  - Windows PowerShell commands for managing SMB



files on their file shares. With this capability, Hyper-V can store all virtual machine files, including configuration files, .vhd files, and checkpoints, on highly available SMB file shares.

The SMB 3.0 features that are introduced in Windows Server 2012 include:

- SMB Transparent Failover. This feature allows you to perform the hardware or software maintenance of nodes in a clustered file server without interrupting server applications that are storing data on file shares.
- SMB Scale Out. By using Cluster Shared Volumes (CSV) version 2, you can create file shares that provide simultaneous access to data files, with direct I/O, through all the nodes in a file server cluster.
- SMB Multichannel. This feature allows you to aggregate network bandwidth and network fault tolerance if multiple paths are available between the SMB 3.0 client and server.
- SMB Direct. This feature supports network adapters that have the Remote Direct Memory Access (RDMA) capability and can perform at full speed with very low data latency and by using very little CPU processing time.
- SMB Encryption. This feature provides the end-to-end encryption of SMB data on untrusted networks and helps to protect data from eavesdropping.
- Volume Shadow Copy Service (VSS) for SMB file shares. To take advantage of VSS for SMB file shares, both the SMB client and the SMB server must support SMB 3.0 at a minimum.
- SMB Directory Leasing. This feature improves branch office application response times. It reduces the number of round trips from client to server as metadata is retrieved from a longer living directory cache.
- Windows PowerShell commands for managing SMB. You can manage file shares on the file server, end to end, from the command line.

The new SMB 3.1.1 features that are introduced in Windows Server 2016 are:

- Preauthentication integrity. Preauthentication integrity provides improved protection from a man-in-the-middle attack that might tamper with the establishment and authentication of SMB connection messages.
- SMB Encryption improvements. SMB Encryption, introduced with SMB 3.0, used a fixed cryptographic algorithm: AES-128-CCM. However, AES-128-GCM performs better in most modern processors, so SMB 3.1.1 uses GCM as its first encryption option.
- Cluster Dialect Fencing. Cluster Dialect Fencing provides support for cluster rolling upgrades for the Scale-Out file Servers feature.
- The removal of the **RequireSecureNegotiate** setting. Because some third-party implementations of SMB do not correctly perform this negotiation, Microsoft provides a switch to disable **Secure Negotiate**. However, the default for SMB 3.1.1 servers and clients is to use preauthentication integrity, as described earlier.
- The x.y.z notation for dialects with a nonzero revision number. Windows Server 2016 uses three separate digits to notate the version of SMB. This information is then used to negotiate the highest level of SMB functionality.

## Providing highly available remote storage by using SMB 3.1.1

SMB in Windows Server 2016 provides a collection of enhancements that are designed to improve availability, performance, and reliability at the single-server and multiple-server (scale-up and scale-out) levels. These features significantly enhance the availability of remote storage. The SMB remote storage enhancements include:

- Hyper-V over SMB. You can use SMB 3.0 and later file shares as shared storage for Hyper-V in Windows Server. This allows Hyper-V to store virtual machine files, including configuration files, .vhd files, and snapshot files, on SMB file shares.
- SMB hardening improvements for SYSVOL and NETLOGON connections. Client connections to the Active Directory Domain Services (AD DS) default SYSVOL and NETLOGON shares on domain controllers now require SMB signing and mutual authentication in Windows 10 and Windows Server 2016.
- SMB Multichannel. SMB Multichannel allows file servers to simultaneously use multiple network connections. It allows for the aggregation of network bandwidth and network fault tolerance when multiple paths are available between the SMB 3.0 or later client and server. This capability allows server applications to take full advantage of all the available network bandwidth and makes them more resilient to network failures.
- SQL Server over SMB. SQL Server can store user database files on SMB file shares, and this feature adds support for clustered servers running SQL Server and system databases.
- Storage Spaces Direct. Storage Spaces Direct allows you to build highly available and scalable storage systems with local storage. This is a significant advancement in Windows Server software-defined storage for two reasons. First, it makes the deployment and management of software-defined storage systems easier. Second, it unlocks the use of new classes of disk devices, such as Serial ATA and Non-Volatile Memory Host Controller Interface Specification-Enhanced disk devices, that were previously not possible to use with clustered Storage Spaces with shared disks.

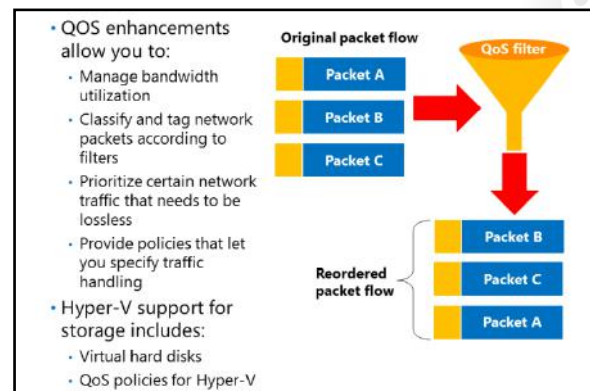
### SMB remote storage enhancements:

- Hyper-V over SMB
- SMB hardening improvements for SYSVOL and NETLOGON connections
- SMB Multichannel
- SQL Server over SMB
- Storage Spaces Direct
- Storage Replica
- QoS

- Storage Replica. Storage Replica is a new feature that supports storage-agnostic, block-level, synchronous replication between servers or clusters for disaster recovery as well as the stretching of a failover cluster between sites. Synchronous replication provides the mirroring of data in physical sites with crash-consistent volumes that helps to ensure no data loss at the file-system level. Asynchronous replication permits site extension outside metropolitan ranges when a possibility of data loss exists. The Storage Replica functionality:
  - Allows for a single-vendor disaster recovery solution for planned and unplanned outages.
  - Uses SMB 3-level transport, which provides enhanced reliability, scalability, and performance.
  - Stretches failover clusters to metropolitan distances.
  - Uses Microsoft software for end-to-end storage and clustering. Such software includes Hyper-V, Storage Replica, Storage Spaces, Failover Clustering, Scale-Out File Server, SMB 3-level transport, Data Deduplication, Resilient File System, and New Technology File System (NTFS).
  - Helps to reduce the cost and complexity in the following ways:
    - The functionality is hardware agnostic, so no requirement exists for a specific storage configuration, such as direct-attached storage or SAN.
    - The functionality permits commodity storage and networking technologies.
    - Failover Cluster Manager provides ease of graphical management for individual nodes and clusters.
    - Windows PowerShell now includes comprehensive, large-scale scripting options.
  - Helps to decrease downtime and increase the reliability and productivity fundamental to Windows Server.
  - Provides supportability, performance metrics, and diagnostic abilities.
- Storage QoS. You use QoS to centrally monitor end-to-end storage performance and make policies by using Hyper-V and Scale-Out File Server in Windows Server 2016.

## What is QoS?

QoS is a collection of technologies that allows you to meet the service requirements of a workload or an application by measuring network bandwidth; detecting changing network conditions, such as congestion or the availability of bandwidth; and then prioritizing or throttling network traffic. This means your priority traffic takes precedence over noncritical traffic, and priority traffic processes first. For instance, you can use QoS to prioritize traffic such as voice or video streaming, which are very latency-sensitive applications, and to control the impact of latency-insensitive traffic, such as bulk data transfers.



The following lists several important QoS feature benefits:

- Bandwidth management. Hyper-V administrators can use the QoS functionality to manage bandwidth for converging multiple traffic types through a virtual machine network adapter, which allows a predictable service level for each traffic type. You also can allocate minimum and maximum bandwidth allocations on a per-virtual machine basis.

- Classification and tagging. Before you can manage the bandwidth for a workload, you need to classify or filter out that workload so that either the QoS Packet Scheduler or a Data Center Bridging (DCB)–capable network adapter can act on it. Windows Server 2016 has an advanced traffic classification capability. A classification can be based on 5-tuples, user types, or Uniform Resource Identifiers (URIs). Windows Server 2016 streamlines the management task so that you can use built-in filters in Windows PowerShell to classify some of the more common workloads.
- Priority-based flow control (PFC). Certain workloads, like RDMA, need lossless transport. When RDMA is built directly on top of Ethernet, it is known as RDMA over Converged Ethernet (RoCE). In this case, the Ethernet transport must be lossless. Traditional link-level flow control, relying on the 802.3 Pause frame, is a solution for this. However, link-level flow control can cause problems—for example, head of line blocking. This issue is resolved by PFC, one of the standards defined by the Institute of Electrical and Electronics Engineers (IEEE) DCB workgroup. Windows Server allows you to enable PFC as long as the physical network adapter supports it. When you enable PFC for RoCE on both ends of the Ethernet link, only the virtual link selected for RoCE, which is designated by a priority value, becomes lossless, and other workloads on the same physical link do not have head of line blocking.
- Policy-based QoS and Hyper-V QoS. You use policy-based QoS to manage network traffic on a physical network. This allows you to specify what network bandwidth control measure to use based on application types, users, and computers. You use policy-based QoS to manage traffic, which helps to control bandwidth costs, negotiate service levels with bandwidth providers or business departments, and offer better end-user experiences. Policy-based QoS is configurable through AD DS Group Policy, is part of your existing management infrastructure, and is consequently a cost-effective solution. A new function in QoS, called Hyper-V QoS, allows you to manage traffic on the virtual network.

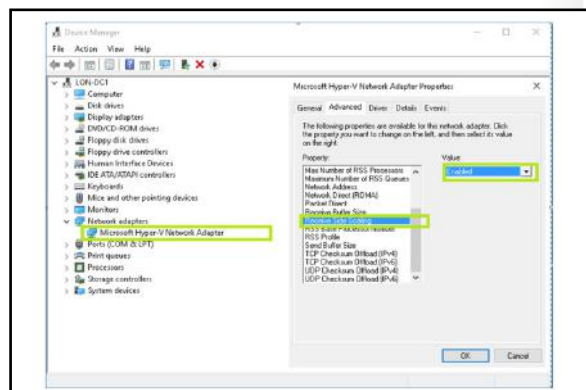
## Storage QoS

Starting in Windows Server 2012, Hyper-V includes the ability to set QoS parameters for storage on virtual machines. Virtual hard disks support the configuration of QoS parameters. When you configure the QoS parameters, you can specify the maximum number of input/output operations (IOPS) for the virtual hard disk, which minimizes the chance that a single virtual hard disk will consume the majority of the IOPS capacity of the underlying storage. You also can configure a virtual hard disk to trigger an alert if the number of IOPS falls below a threshold value. IOPS are measured in 8-kilobyte increments. You cannot configure storage QoS when you are using shared virtual hard disks.

Windows Server 2016 now uses storage QoS to manage QoS policies for Hyper-V and Scale-Out File Server. This allows the deployment of QoS policies for SMB 3.1.1 storage.

## What is RSS?

Windows Server 2016 supports virtual RSS on the virtual machine network path. This allows virtual machines to support greater network traffic loads. Virtual RSS accomplishes this by spreading the processing load across multiple processor cores on both the Hyper-V host and the virtual machine. A virtual machine can take advantage of virtual RSS improvements only if the processor on the Hyper-V host supports RSS and you have configured the virtual machine to use multiple processor cores.






Virtual RSS allows network adapters to balance the network processing load across the processor cores that are assigned to a virtual machine. Virtual RSS allows a virtual machine to process greater amounts of network traffic than it could process if only a single CPU core was responsible for processing traffic. You can implement virtual RSS by allocating a virtual machine multiple cores through the advanced network. To use virtual RSS, the host's processor must support RSS and the host's network adapters must support Virtual Machine Queue (VMQ).

### Enabling virtual RSS

You can use Device Manager or Windows PowerShell to enable virtual RSS. To enable RSS by using Device Manager, perform the following steps:

1. On the virtual machine, open **Device Manager**.
2. Expand **Network adapters**, right-click the network adapter you want to configure virtual RSS on, and then click **Properties**.
3. On the **Advanced** tab, in the network adapter's properties, locate the setting for RSS, and then make sure that it is enabled.

 **Note:** Some network adapters advertise the number of RSS queues they support on the **Advanced** tab.

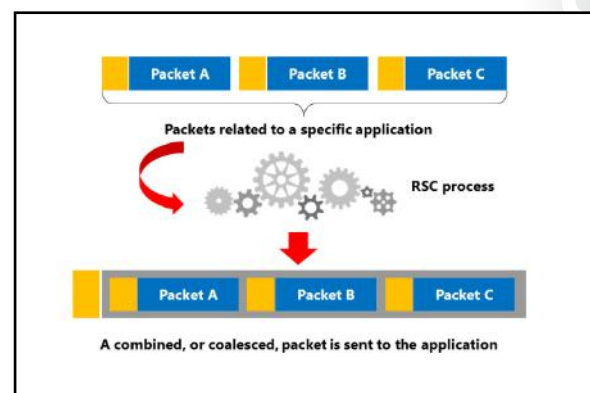
To enable RSS by using Windows PowerShell, perform the following steps:

1. On the virtual machine, open **Windows PowerShell**.
2. At the command prompt, type the following command, and then press Enter.

```
Enable-NetAdapterRSS -Name "AdapterName"
```

### What is RSC?

RSC is an offload technology that helps you to reduce how much CPU time is used in network processing. RSC works by having the network adapter look at the incoming data packets and strip them before joining the combined payloads, or *coalescing* the segments into a single packet. The network adapter then sends the coalesced packet to an application, which results in much less CPU time on the receive side. The CPU can then take care of other important tasks, resulting in increased productivity and scalability support. RSC supports only incoming packets; so it does not affect outgoing packets at all, which the CPU processes normally.



To use RSC, the server must have an RSC-capable network adapter. If you want to use RSC in a virtualized environment, the network adapter must also support SR-IOV.

RSC provides multiple benefits, including:

- Hosted cloud deployments. RSC reduces the number of CPU cycles used for network storage and live migration.
- Faster processing. I/O-heavy database applications and database replication are processed faster.

- Enhanced performance on file servers that are deployed with the Windows Server File Services server role. If your file server is also configured as a BranchCache-enabled content server, BranchCache performance is improved by RSC.
- Improvement on any server workloads that are I/O intensive. I/O intensive workloads are significant consumers of network traffic, and by coalescing the segments, cut down on I/O processing time.

You can use Windows PowerShell to manage RSC. You can use the cmdlets **Get-NetAdapterRsc** and **Get-NetAdapterStatistics** to see the network adapter's RSC configuration. Use the cmdlet **Enable-NetAdapterRsc** to enable 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>

### Categorize Activity

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

## Lesson 2

# Configuring advanced Hyper-V networking features

Hyper-V provides several options for allowing network communication among virtual machines. You can use Hyper-V to configure virtual machines that communicate with an external network in a manner similar to that for physical hosts that you deploy traditionally. You also can use Hyper-V to configure virtual machines that can communicate only with a limited number of other virtual machines that are hosted on the same Hyper-V host. Windows Server 2016 provides several advanced networking features for Hyper-V and virtual machines. This lesson describes the various advanced features that are available for Hyper-V virtual networks, which you can use to best meet your organization's needs.

## Lesson Objectives

After completing this lesson, you will be able to:

- Describe the virtual switch expanded functionality.
- Describe virtual switch extensibility.
- Describe SR-IOV.
- Describe dynamic virtual machine queuing.
- Describe the network adapter advanced features
- Describe NIC Teaming in virtual machines.
- Describe how to configure the network adapter advanced features.

## Virtual switch expanded functionality

Virtual switches are virtual devices that you can manage through the Virtual Switch Manager, which allows you to create three types of virtual switches. Virtual switches control how network traffic flows among the virtual machines that are hosted on a Hyper-V server and how network traffic flows between the virtual machines and the rest of the organizational network.

Hyper-V in Windows Server 2012 and in Windows Server 2016 supports three types of virtual switches, which the following table details.

- The virtual switch improvements in Windows Server 2016 include:
  - Extended port ACLs
  - Dynamic load balancing
  - Coexistence with third-party forwarding extensions
  - RSS support on the virtual machine network path
  - Network tracing enhancements
  - Router guarding
  - DHCP guarding
  - Trunk mode for virtual machine
  - Port mirroring
  - VLAN isolation through a Private VLAN
  - Extended bandwidth management

Type	Description
External	You use this type of switch to map a network to a specific network adapter or network adapter team. Windows Server 2012 supports mapping an external network to a wireless network adapter if you have installed the Wireless LAN service on the host Hyper-V server and if the Hyper-V server has a compatible network adapter.
Internal	You use internal virtual switches to communicate among the virtual machines on a Hyper-V host and to communicate between the virtual machines and the Hyper-V host itself.

Type	Description
Private	You use private switches only to communicate among the virtual machines on a Hyper-V host. You cannot use private switches to communicate between the virtual machines and the Hyper-V host.

When configuring a virtual network, you also can configure a VLAN ID to associate with the network. You can use this to extend the existing VLANs on an external network to VLANs within the Hyper-V host's network switch. You can use VLANs to partition network traffic. VLANs function as separate logical networks. Traffic can pass from one VLAN to another only if it passes through a router.

You can configure the following extensions for each virtual switch type:

- Microsoft Network Driver Interface Specification (NDIS) Capture. This extension allows for the capture of data that travels across a virtual switch.
- Microsoft Windows Filtering Platform (WFP). This extension allows filtering of data that travels across a virtual switch.

Windows Server 2012 introduced many new features that are now available in the virtual switch expanded functionality. Several more features were added in Windows Server 2012 R2. These features remain an important part of Windows Server 2016 and continue to improve network performance and the flexibility of virtual machines in private and public cloud environments.

### Features included in Windows Server 2012 Hyper-V networking

The features that were added in Windows Server 2012 Hyper-V networking include:

- Network virtualization. This feature allows IP addresses to be virtualized in hosting environments so that virtual machines that migrate to the host can keep their original IP addresses, rather than being allocated IP addresses on the Hyper-V server's network.
- Bandwidth management. You can use this feature to specify a minimum and a maximum bandwidth that Hyper-V will allocate to the adapter. Hyper-V reserves the minimum bandwidth allocation for the network adapter even when other virtual network adapters on virtual machines that are hosted on the Hyper-V host are functioning at capacity.
- Dynamic Host Configuration Protocol (DHCP) guard This feature drops DHCP messages from virtual machines that are functioning as unauthorized DHCP servers. This might be necessary in scenarios where you are managing a Hyper-V server that hosts virtual machines for others but where you do not have direct control over the virtual machines' configurations.
- Router guard. This feature drops router advertisement and redirection messages from virtual machines that are configured as unauthorized routers. This might be necessary in scenarios where you do not have direct control over the configuration of the virtual machines.
- Port mirroring. You can use this feature to copy incoming and outgoing packets from a network adapter to another virtual machine that you have configured for monitoring.
- NIC Teaming. You can use this feature to add a virtual network adapter to an existing team on the host Hyper-V server.
- VMQ. This feature requires the host computer to have a network adapter that supports the feature. VMQ uses hardware packet filtering to deliver network traffic directly to a guest. This improves performance because the packet does not need to be copied from the host operating system to the virtual machine. Only network adapters that are specific to Hyper-V support this feature.

- SR-IOV. This feature requires that specific hardware and special drivers be installed on the guest operating system. SR-IOV enables multiple virtual machines to share the same peripheral component interconnect (PCI) Express physical hardware resources. If sufficient resources are not available, network connectivity failback occurs so that the virtual switch provides that connectivity. This feature is supported only on network adapters that are specific to Hyper-V.
- Internet Protocol security (IPsec) task offloading. This feature requires that the guest operating system and network adapter are supported. This feature allows a host's network adapter to perform calculation-intensive security-association tasks. If sufficient hardware resources are not available, the guest operating system performs these tasks. You can configure a maximum number of offloaded security associations from 1 through 4,096. This feature is supported only on network adapters that are specific to Hyper-V.
- Private VLANs. A VLAN ID is a 12-bit number in the range 1 through 4,095. The configuration of multiple, isolated VLANs is complex and difficult. However, when you deploy Hyper-V Network Virtualization, many of these complex and difficult issues are solved, but not completely. A simpler solution is to use a private VLAN. A private VLAN tackles some of the scalability issues of VLANs. A private VLAN is a property of a switch port. With a private VLAN two VLAN IDs exist: a primary VLAN ID and a secondary VLAN ID. A private VLAN can exist in one of three modes:
  - Isolated. Communicates only with promiscuous ports in the private VLAN.
  - Promiscuous. Communicates with all ports in the private VLAN.
  - Community. Communicates with ports in the same community and with any promiscuous ports in the private VLAN.
- Trunk mode. Trunk mode allows network services or network appliances on a virtual machine to see traffic from multiple VLANs. In trunk mode, a switch port receives traffic from all the configured VLANs in an allowed VLAN list. You can also configure a switch port that is connected to a virtual machine, but it is not bound to the underlying network adapter.

### Features included in Windows Server 2012 R2 Hyper-V networking

The features that were added in Windows Server 2012 R2 Hyper-V networking include:

- Extended port access control lists (ACLs). You can use extended port ACLs in a Hyper-V virtual switch to help enforce security policies and firewall protection at the switch level for virtual machines. The differences between ACLs in Windows Server 2012 and Windows Server 2012 R2 Hyper-V include:
  - Administrators can now include socket port numbers when developing ACLs.
  - Hyper-V switches support unidirectional, stateful rules with a timeout parameter.
- The dynamic load balancing of network traffic. When you map a virtual network to a network adapter team on a Windows Server 2012 R2 Hyper-V host, the network traffic will be continuously load balanced across network adapters, with traffic streams moved as necessary to maintain this balance. In Windows Server 2012 Hyper-V, a traffic stream remained with the network adapter in the team that it was initially assigned to, and traffic streams were not dynamically moved to other network adapters in the team.
- Coexistence with non-Microsoft forwarding extensions. The Hyper-V Network Virtualization module forwards network traffic that is encapsulated through Network Virtualization Generic Routing Encapsulation (NVGRE). Non-Microsoft switch extensions are supported in coexistence scenarios with Hyper-V virtual switches. When a non-Microsoft extension is present, any non-NVGRE network traffic is forwarded via the non-Microsoft forwarding extensions.

- RSS on the virtual machine network path. Windows Server 2012 R2 supports virtual RSS on the virtual machine network path. This allows virtual machines to support greater network traffic loads. Virtual RSS accomplishes this by spreading the processing load across multiple processor cores on both the Hyper-V host and the virtual machine. A virtual machine can take advantage of virtual RSS improvements only if the processor on the Hyper-V host supports RSS and, if you configure the virtual machine to use multiple processor cores.
- Network tracing improvements. You use **Netsh Trace** commands to trace packets. The improvements in Windows Server 2012 R2 allow you to view port and switch information as you trace network traffic through Hyper-V virtual switches.

### Features added in Windows Server 2016 Hyper-V networking

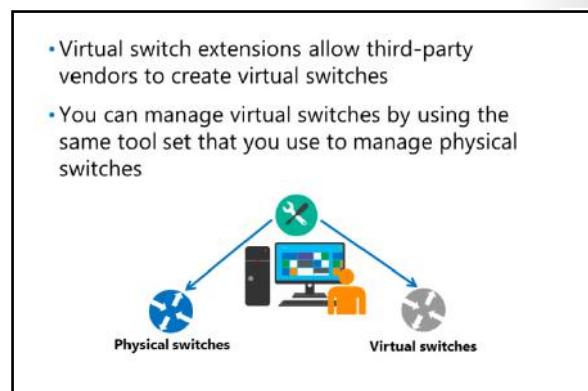
The features that were added in Windows Server 2016 Hyper-V networking include:

- Network function virtualization. In most datacenters, hardware appliances handle some network functions or services, such as software load balancing and network address translation, services provided by datacenter firewalls, and Remote Access Service gateway services. However, with software-defined networking, more appliances are becoming virtualized. All three functions are available in Windows Server 2016.
- Network Controller. By using Network Controller, you can have a central location to monitor, manage, troubleshoot, and configure both your physical and your virtual environment.
- Switch Embedded Teaming (SET). SET is a new NIC Teaming option that you can use for Hyper-V networks. SET has some integrated functionality with Hyper-V that provides faster performance and better fault tolerance than traditional teaming.
- RDMA with Hyper-V. RDMA services can now use Hyper-V switches. You can enable this feature with or without SET.
- Multiple queues for virtual machines. This feature allocates multiple hardware queues for each virtual machine, thereby improving throughput as compared to Windows Server 2012 R2.
- Converged network adapters. A converged network adapter supports using a single network adapter or a team of network adapters to handle multiple forms of traffic, management, RDMA, and virtual machine traffic. This reduces the number of specialized adapters that are needed on each host.

### Understanding virtual switch extensibility

The new Hyper-V Extensible Switch feature supports isolation policies, allows extensibility, and lets third-party vendors add filters to provide their own forwarding rules.

The Hyper-V Extensible Switch is a layer 2 virtual network switch that is used to connect virtual machines to the physical network by providing programmatically managed and extensible capabilities. The Hyper-V Extensible Switch permits policy enforcement for security enhancement, isolation, and service levels. The Hyper-V Extensible Switch provides for non-Microsoft extensible plug-ins that can provide enhanced networking and security capabilities by using NDIS filter drivers and WFP callout drivers for support.



You can implement and manage virtualized datacenters with the Hyper-V Extensible Switch through:

- An open platform. Built on an open platform, The Hyper-V Extensible Switch allows third-party software vendors to add or extend the capabilities that are natively provided by Microsoft. The abilities of the Hyper-V Extensible Switch can combine with the added capabilities of vendor extensions, which can then be applied to implement and manage virtualized datacenters.
- A standard API. The programming model uses the same NDIS and WFP application programming interface (API) that was used for network filters and drivers in earlier versions of Windows. Several new API functions and parameters have been added for virtual switch ports.
- Windows reliability and quality. The Hyper-V Extensible Switch uses the Windows operating system and the Windows Hardware Quality Logo program to set high standards for extension quality.
- Policy and configuration integration. The management of extensions provides a standard management approach by integrating Windows management through Windows Management Instrumentation calls and Windows PowerShell cmdlets. You can automatically migrate policies of extensions with the virtual machine configuration during a live migration.
- Easy troubleshooting options. Included with the Hyper-V Extensible Switch are various event logs and unified tracing, which makes it easier to diagnose and troubleshoot any issues.

You can extend or replace three aspects of the switching process with extensions: ingress filtering, destination lookup and forwarding, and egress filtering. Additionally, you can use extensions to gather statistical data by monitoring traffic at different layers of the Hyper-V Extensible Switch. Multiple monitoring and filtering extensions can be supported at the ingress and egress portions of the Hyper-V Extensible Switch. However, only one instance of the extension can be used per switch instance if you use a forwarding extension. In this case, it overrides the default forwarding option of the Hyper-V Extensible Switch.

The following table shows the types of extensions, their purposes, the components used to implement them, and examples.

Extension	Purpose	Component	Examples
Intrusion detection or firewall	Allows filtering and modifying TCP/IP packets, monitoring or authorizing connections, and filtering traffic that is protected by IPsec and filter remote procedure calls.	WFP callout driver	Virtual firewall, connection monitoring
Network forwarding	Provides a forwarding extension per Hyper-V Extensible Switch instance, which bypasses the default forwarding option (with a maximum of one per Hyper-V Extensible Switch instance).	NDIS filter driver	OpenFlow, Virtual Ethernet Port Aggregator, proprietary network fabrics
Network packet filter	Creates, filters, and modifies network packets that are entering or leaving the Hyper-V Extensible Switch and that exist in virtual machine-to-virtual machine traffic.	NDIS filter driver	Security enhancement

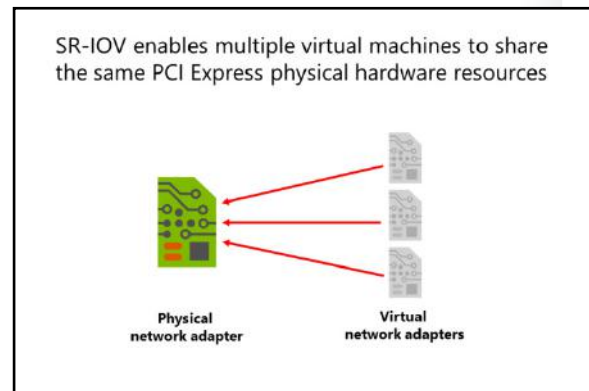


Extension	Purpose	Component	Examples
Network packet inspection	Views network packets for virtual machine-to-virtual machine traffic per Hyper-V Extensible Switch instance. This extension cannot alter network packets.	NDIS filter driver	sFlow, network monitoring

## What is SR-IOV?

SR-IOV allows multiple virtual machines to share the same PCI Express physical hardware resources. If sufficient resources are not available, network connectivity fallback occurs, and the virtual switch provides connectivity. SR-IOV requires that you install specific hardware and special drivers on the guest operating system, and you might need to enable it in the computer BIOS.

Note, however, that only 64-bit Windows and Windows Server guest virtual machines, starting with Windows Server 2012 and Windows 8, support SR-IOV. In this case, you should disable SR-IOV on all the virtual machines that do not support SR-IOV. For those guest operating systems that can use SR-IOV, the physical network adapter on the parent partition—that is the Hyper-V host—appears on the guest operating system. You can use Device Manager to see the physical network adapter and even to upgrade or manage the device driver for it within the guest operating system. In other words, the virtual machine communicates with the physical hardware.



SR-IOV uses Virtual Functions (VF). VFs are associated with a Physical Function (PF). The PF is what the parent partition uses in Hyper-V and is equivalent to the regular bus-addressed, device-addressed, or function-addressed PCI device. The responsibility for arbitration relating to policy decisions, such as those for link speed or media access control (MAC) addresses in use by virtual machines and for I/O from the parent partition, is handled by the PF. Although the parent partition can use a VF, in Windows Server, only virtual machines use VFs. A single PCI Express device can expose multiple VFs, such as a multiple-port networking device, with each port independent and with its own set of VF resources.

When using SR-IOV, a part of the network adapter's hardware is made available to the virtual machine. Because the guest operating system's networking code doesn't know how to directly manipulate that hardware, you will need to load a vendor-supplied driver in the virtual machine. Note that the VF is not a complete device or autonomous. It cannot make any decisions about policy and control. The VF can only read and write the parts of the device configuration that the PF lets it handle, and it can only see the parts of networking hardware in memory space that are allocated to the VF. VFs are transient, because the guest operating system is also transient, in the sense that you can start, stop, or even delete it. However, the PF is always available, and is the arbiter for all policy decisions.

## What is dynamic VMQ?

VMQ was developed to be a hardware virtualization technology for the efficient transfer of network traffic to a virtualized guest operating system. A VMQ-capable network adapter categorizes incoming frames to be routed to a receive queue based on filters that associate the queue with a virtual machine's virtual network adapter. A queue is assigned to each virtual machine device buffer, which avoids needless packet copies and route lookups in the virtual switch. VMQ makes a single network adapter on a physical host appear as multiple network adapters to the virtual machines. This, in turn, allows each virtual machine to have its own dedicated network adapter.

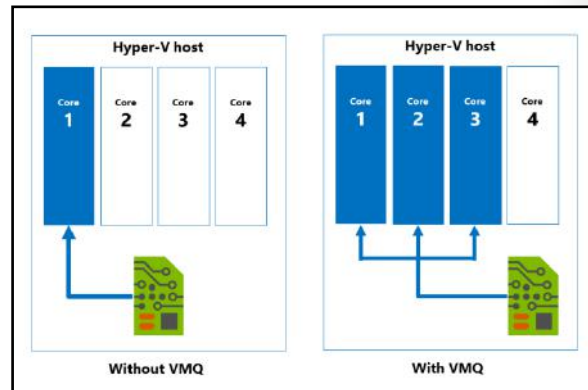
VMQ provides separate queues for the hardware device. In static VMQ, the Hyper-V administrator can manually set the processor affinity of the hardware queues to different CPU cores, which creates RSS on a per-virtual machine network adapter.

*Dynamic* VMQ dynamically distributes incoming network traffic processing to physical host CPU cores based on processor usage and network load. During periods of heavy network loads, dynamic VMQ automatically employs more processors. When the network load is light, dynamic VMQ relinquishes those same processors. Dynamic VMQ spreads interrupts for network traffic across the available processors. In Windows Server 2012 and later, dynamic VMQ allows an adaptive algorithm to modify the CPU affinity of queues without requiring the removal and re-creation of queues. This results in a better network load-to-processor use match, which helps to increase network performance.

Dynamic VMQ requires the host computer to have a network adapter that supports the feature. Dynamic VMQ uses hardware packet filtering to deliver network traffic directly to a guest. This helps to improve performance, because the packet does not need to be copied from the host operating system to the virtual machine. Only network adapters that are specific to Hyper-V support this feature.

Dynamic VMQ is enabled by default in Windows Server 2016. You can enable or disable it by using the Windows PowerShell cmdlets **Enable-NetAdapterVmq** and **Disable-NetAdapterVmq**, respectively.

Dynamic VMQ is very similar to RSS, which was mentioned in Lesson 1. On a physical host, RSS processes incoming network traffic so that a single CPU core does not slow it down. RSS does this by spreading the calculations across multiple CPU cores. For a Hyper-V host that has several virtual machines with significant incoming traffic, dynamic VMQ is similar to RSS. Dynamic VMQ hashes the destination MAC address, puts the traffic for a particular virtual machine in a specific queue, and distributes the interrupts to the CPU cores. Dynamic VMQ handles this by offloading these functions to the network adapters. In dynamic VMQ, a rare circumstance can occur when processing that is happening on a CPU core generates a large amount of inbound traffic. This triggers dynamic VMQ to use another, less-busy CPU core, and because the traffic load has not changed, it jumps back to the original or another CPU core. This process continues and is referred to as the *ping-pong effect*. Although dynamic VMQ is more automatic, RSS can better avoid the ping-pong effect in this situation.



## Network adapter advanced features

Windows Server 2016 continues to improve the software-defined network infrastructure. A software-defined network is a primary building block of a software-defined datacenter. You can easily manage many of these features through Microsoft System Center Virtual Machine Manager. However, you can also use Windows PowerShell commands to configure implementations of these features. The default settings are adequate in most small-scale environments. Some of the new or improved features are:

- Network function virtualization
- Network Controller
- SET
- RDMA
- VMQ
- Converged network adapters
- QoS for software-defined networks

- Network function virtualization. In most datacenters, hardware appliances handle some network functions, such as software load balancing and network address translation. However, with software-defined networking, more appliances are becoming virtualized. All three functions are available in Windows Server 2016.



**Note:** To use containers and build out Hyper-V virtualized networks more efficiently, it is important that you have the ability to use network address translation with Windows Server 2016 as a built-in feature of a virtual switch. You can create a virtual switch in a virtual machine container host by running the following command:

```
New-VMSwitch -Name "Virtual Switch Name" -SwitchType NAT
```

- Network Controller. By using Network Controller, you can have a central location to monitor, manage, troubleshoot, and configure both your physical and your virtual environment.
- SET. SET is a new NIC Teaming option that you can use for Hyper-V networks. SET has some integrated functionality with Hyper-V that provides faster performance and better fault tolerance than traditional teaming.
- RDMA with Hyper-V. RDMA services can now use Hyper-V switches. You can enable this feature with or without SET.
- Multiple queues for virtual machines. This feature allocates multiple hardware queues for each virtual machine, thereby improving throughput as compared to Windows Server 2012 R2.
- Converged network adapters. A converged network adapter supports using a single network adapter or a team of network adapters to handle multiple forms of traffic, management, RDMA, and virtual machine traffic. This reduces the number of specialized adapters that are needed on each host.
- QoS for software-defined networks. This feature manages the default class of traffic through the virtual switch within the default class bandwidth.

## Hardware acceleration features

The hardware acceleration features specify network tasks that can be offloaded to a physical network adapter. Many of the hardware acceleration features are enabled by default in a virtual network adapter, but that does not mean the virtual machine actually uses them all. All the hardware acceleration settings require hardware support. To configure the hardware acceleration settings for a virtual machine network adapter:

1. In the **Hyper-V Manager** console, right-click the virtual machine, and then click **Settings**.
2. In the **Settings** window for the virtual machine, select and expand the network adapter that you want to manage.
3. Note two subnodes; **Hardware Acceleration** and **Advanced Features**. Click the **Hardware Acceleration** node.
4. In the **details** pane, note the various settings. Some are already selected. You can enable or disable the various features on this page.

The features that you can enable and disable are:

- VMQ. VMQ requires a physical network adapter that supports this feature.
- IPsec task offloading. This technology supports hardware-equipped network adapters to reduce the CPU load by performing the computationally intensive work of encryption and decryption. You can also specify the maximum number of offloaded security associations in the range 1 through 4096. The default is 512.

## NIC Teaming in virtual machines

When used with virtual machines, NIC Teaming allows the virtual machines to team the virtual network adapters that connect to separate virtual switches. To get the benefit of NIC Teaming, the host must have at least two external virtual switches. When you have multiple virtual network adapters attached to the same switch, if the physical network adapter that the virtual switch is connected to fails, those virtual network adapters will lose connectivity. When configuring NIC Teaming for virtual machines, the network adapters connected to virtual switches can use SR-IOV.

- NIC Teaming in virtual machines:
  - Requires multiple virtual network adapters
  - Requires being enabled on the virtual network adapters
  - Allows you to then implement it in the virtual machine's operating system (if supported)
- SET:
  - Allows you to group from one through eight physical network adapters into one or more virtual network adapters

Enable virtual machine NIC Teaming for virtual machines on the **Advanced Features** page of the virtual network adapter in Hyper-V Manager. You can also enable NIC Teaming for virtual machines by using the **Set-VMNetworkAdapter** Windows PowerShell cmdlet. To enable NIC Teaming within the virtual machine's operating system, you must enable NIC Teaming on the virtual network adapter or configure the virtual network adapter to allow MAC address spoofing. After you enable virtual NIC Teaming on the virtual network adapter or enable MAC address spoofing, you can configure NIC Teaming within the virtual machine.

Dynamic NIC Teaming was first introduced in Windows Server 2012. It allows new traffic to be assigned to a particular network adapter, and the traffic flow remains with that network adapter throughout the session. Dynamic NIC Teaming balances the traffic flow across all the available network adapters in a team.

## SET

SET allows you to use fewer network adapters when you want to use RDMA and SET at the same time. SET is an alternative to NIC Teaming that you can use in environments that include Windows Server 2016 Hyper-V and the Software-Defined Networking stack. SET incorporates some of the NIC Teaming functions into a Hyper-V virtual switch.

SET allows you to group from one through eight physical Ethernet network adapters into one or more virtual network adapters. These virtual network adapters then help to provide faster performance and fault tolerance in the event of a failure of any network adapter. To place the member network adapters in a SET team, you must install them in the same physical Hyper-V host.

## Demonstration: Configuring network adapter advanced features

In this demonstration, you will learn how to implement advanced features for network adapters on virtual machines.

### Demonstration Steps

#### Use Windows PowerShell to enable DHCP guarding

1. Ensure that you have performed the preparation steps.
2. On **LON-CL1**, open the **Network and Sharing Center**, and then note the **Ethernet** hyperlink properties. In the status details, note that **LON-DC1** is the DHCP server.
3. On **LON-HOST1**, open the **Windows PowerShell** window, and then run the following two cmdlets:

```
Set-VMNetworkAdapter -VMName 20741A-LON-DC1-B -DhcpGuard On  
Set-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -DhcpGuard Off
```

4. On **LON-CL1**, open a command prompt as an administrator, and then release and renew the IP address with the **ipconfig** command.
5. Open the **Network and Sharing Center**, and then note the **Ethernet** hyperlink properties. In the status details, note that **LON-SVR1** is now the DHCP server.

#### 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 20741A-LON-DC1-B -DhcpGuard Off
```

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 **20741A-LON-DC1-B**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-SVR1-B** and **20741A-LON-CL1-B**.

**Check Your Knowledge**

Question	
What is the ping-pong effect?"?	
Select the correct 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 generate 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.

# Lab: Configuring advanced Hyper-V networking features

## Scenario

A. Datum Corporation has implemented the Hyper-V virtualization platform in one of their subsidiaries. You have created several test virtual machines and familiarized yourself with many of the configuration options. The next step is to implement and test network connectivity for the virtual machines.

## Objectives

After completing this lab, you will be able to:

- Create and use Hyper-V virtual switches.
- Configure bandwidth management and DHCP guarding.

## Lab Setup

Estimated Time: **30 minutes**

Physical Computer: Restart to **20741A-LON-HOST1**

Virtual machines: **20741A-LON-DC1-B**, **20741A-LON-SVR1-B**, and **20741A-LON-CL1-B**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will need to start **20741A-LON-HOST1**. Restart the physical computer and in the boot menu that appears, select **20741A-LON-HOST1**. Sign into **LON-HOST1** as **Adatum\Administrator** with a password of **Pa\$\$w0rd**. You use the available virtual machine environment. To start the lab, complete the following steps:

1. On the **LON-HOST1**, on the task bar, click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1-B**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for virtual machines **20741A-LON-SVR1-B** and **20741A-LON-CL1-B**.

## Exercise 1: Creating and using Hyper-V virtual switches

### Scenario

A. Datum Corporation has the Hyper-V virtualization platform already installed. Before deploying Hyper-V and virtual machines in the production environment, you need to ensure that you understand the different networking options that you can configure in Hyper-V. First, you will review the current networking configuration of the Hyper-V host. Then you will create new virtual network adapters in the parent partition. You will also create different types of Hyper-V virtual switches and explore the connectivity options that exist when using each of the switches.

The main tasks for this exercise are as follows:

1. Verify the current Hyper-V network configuration.
2. Create virtual switches.

3. Create virtual network adapters.
4. Use the Hyper-V virtual switches.
5. Add NIC Teaming.

► **Task 1: Verify the current Hyper-V network configuration**

1. On **LON-HOST1**, if necessary, open **Hyper-V Manager**.
2. In Hyper-V Manager, open the **Virtual Switch Manager**, and then note the virtual switch. **Private Network** that has been created for **LON-HOST1**.

► **Task 2: Create virtual switches**

1. On **LON-HOST1**, in the **Virtual Switch Manager**, create an external switch named **External Switch**.
2. In the **Virtual Switch Manager**, create an internal switch named **Internal Switch**.

► **Task 3: Create virtual network adapters**

1. Shut down **LON-SVR1**.
2. On **LON-HOST1**, open **Windows PowerShell** and then type the following commands. Press Enter after each line:

```
Add-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -Name "New Network Adapter"  
Connect-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -Name "New Network Adapter" -  
SwitchName "External Switch"
```

► **Task 4: Use the Hyper-V virtual switches**

1. In **Hyper-V Manager**, in the **Virtual Machines** pane, right-click **20741A-LON-SVR1-B**, and then click **Settings**.
2. In the **Settings for 20741A-LON-SVR1-B on LON-HOST1** window, in the console tree, click **New Network Adapter**.
3. Review the **New Network Adapter** settings in the **details** pane.
4. Start and connect to the **20741A-LON-SVR1-B** virtual machine, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
5. If prompted, click **Yes** to add the new network to the private network profile.
6. Open **Server Manager**, click the **Local Server** node, and then review the status details of the **Ethernet 2** network connection.
7. Note the IP address and other settings assigned to the network adapter. They should be external to your virtual machine environment.
8. Close all open windows and leave the **Server Manager** open.

► **Task 5: Add NIC Teaming**

1. On **LON-SVR1**, in **Server Manager**, select the **Local Server** node.
2. In the **Local Server** node, create a NIC team that uses the **Ethernet 2** virtual network adapter, and then name it **LON-SVR1 NIC Team**.



3. In the **NIC Teaming** dialog box, in the **Teams** pane, note the following:
  - o Team: **LON-SVR1 NIC Team**
  - o Status: **OK**
  - o Teaming Mode: **Switch Independent**
  - o Load Balancing: **Address Hash**
  - o Adapters: **1**

**Results:** After completing this exercise, you should have successfully configured the Hyper-V virtual switch.

## Exercise 2: Configuring and using the advanced features of a virtual switch

### Scenario

One of your managers wants to see how the Hyper-V virtual switch can help to protect the network clients from unauthorized DHCP servers. You plan to demonstrate how to configure DHCP guarding and, at the same time, show the manager how simple it is to configure VLANs and bandwidth management.

The main tasks for this exercise are as follows:

1. Configure the network adapters to use DHCP guarding.
2. Configure and use DHCP guard.
3. Configure and use VLANs.
4. Configure and use bandwidth management.
5. Prepare for the next module.

#### ► Task 1: Configure the network adapters to use DHCP guarding

1. On **LON-HOST1**, open **Hyper-V Manager**.
2. In **Hyper-V Manager**, open the settings for the **20741A- SVR1-B** virtual machine.
3. Under **Settings**, in the **Network Adapter** node, open **Advanced Features**.
4. Enable **DHCP guard**.
5. Repeat steps 2–4 for **20741A-LON-CL1-B**.

#### ► Task 2: Configure and use DHCP guard

1. On **LON-CL1**, check the TCP/IP network properties, and then confirm the following:
  - o IP Address: **172.16.0.50**
  - o Subnet Mask: **255.255.255.0**
  - o Default Gateway: **172.16.0.1**
  - o Preferred DNS Server: **172.16.0.10**
2. Change the network connection to automatically get its IP address and preferred DNS server.
3. Verify that **LON-CL1** is now getting an IP address from the DHCP role service on **LON-DC1**.

4. On **LON-SVR1**, open **Server Manager**, and then install and authorize the **DHCP Server** role on **LON-SVR1**.
5. After DHCP is installed, configure it with all default settings, except for the following:
  - o Name of Scope: **Lab 10 Scope**
  - o Address pool: **172.16.0.200** through **172.16.0.210**
  - o Subnet Mask: **255.255.0.0**
  - o Default Gateway: **172.16.0.1**
  - o DNS Server: **172.16.0.10**
  - o Domain name: **Adatum.com**
  - o Activate the scope: **Yes, I want to activate this scope now**
6. On the physical host computer, in the **Windows PowerShell** window, type the following commands, and then press Enter after each line:

```
Set-VMNetworkAdapter -VMName 20741A-LON-DC1-B -DhcpGuard On
Set-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -DhcpGuard Off
```

7. On **LON-CL1**, use the **Ipconfig** command to release and then renew the IP address settings.
8. Verify that **LON-CL1** is now getting an IP address from the DHCP role service on **LON-SVR1**.

### ► Task 3: Configure and use VLANs

1. On **LON-SVR1**, in **Server Manager**, click the **Local Server** node.
2. Delete **LON-SVR1 NIC Team** from the **Ethernet 2** network adapter.
3. On **LON-HOST1**, open **Hyper-V Manager**, and then click **Virtual Switch Manager**.
4. Select the external switch, and then enable VLAN identification for the management operating system.
5. In the settings for the virtual machine **20741A-LON-SVR1-B**, in the **New Network Adapter** settings, enable VLAN identification.

### ► Task 4: Configure and use bandwidth management

1. While still on **LON-HOST1**, in **Hyper-V Manager**, in the **Settings** for the virtual machine **20741A-LON-SVR1-B**, in the **New Network Adapter** settings, click **Enable Bandwidth Management**, and then set the **Maximum Bandwidth** to **100** megabits per second (Mbps).
2. On the **LON-SVR1** virtual machine, open **Task Manager** to display more details, and then click the **Performance** tab. Select the **Ethernet 2** network adapter item.
3. Open **Internet Explorer**, and then navigate to the **www.microsoft.com** page while watching the status of **Ethernet 2** in **Task Manager**.
4. You should not see more than 100 Mbps consumed on the network adapter.

5. On **LON-HOST1**, in the **20741A-LON-SVR1-B** settings, disconnect **External Switch** from **New Network Adapter**.
6. In **Virtual Switch Manager**, remove **External Switch**.

**Results:** After completing this exercise, you should have successfully configured the advanced features of the Hyper-V virtual switch.

#### ► Task 5: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state, and return the physical computer to the default operating system.

1. On **LON-HOST1**, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1-B**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-SVR1-B** and **20741A-LON-CL1-B**.
5. Restart **LON-HOST1** and in the boot menu, select the default training center computer.

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

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

## Module Review and Takeaways

### 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?

### 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 network connectivity will be retained 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 physical 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.

# Module 11

## Implementing Software Defined Networking

### Contents:

Module Overview	11-1
Lesson 1: Overview of Software Defined Networking	11-2
Lesson 2: Implementing network virtualization	11-11
Lesson 3: Implementing Network Controller	11-16
Lab: Deploying Network Controller	11-28
Module Review and Takeaways	11-32

## Module Overview

Software Defined Networking (SDN) bypasses the limitations imposed by physical network devices and allows organizations to dynamically manage their networks. SDN uses an abstraction layer in software to manage your network dynamically. When you implement SDN, you can virtualize your network, define policies to manage network traffic, and manage your virtualized network infrastructure.

### Objectives

After completing this module, you will be able to:

- Describe Software Defined Networking.
- Implement network virtualization.
- Implement Network Controller.

## Lesson 1

# Overview of Software Defined Networking

SDN enables you to centrally configure and manage both the physical and virtual network devices in your datacenter, such as switches, routers, and gateways, so that you can provide an automated means of responding to application and workload requirements. In Windows Server 2016, virtualization features, including Hyper-V Virtual Switch, Hyper-V Network Virtualization (HNV), and Remote Access Service (RAS) Gateway, are integrated into your SDN infrastructure.

### Lesson Objectives

After completing this lesson, you will be able to:

- Describe SDN in Windows Server 2016.
- Explain when to use SDN.
- Plan to implement SDN.
- Describe how to deploy SDN by using scripts.

### What is Software Defined Networking?

Although Software Defined Networking still requires a physical network layer, with SDN, you can:

- Virtualize the network so that you can break the direct connection between the applications and virtual servers and the underlying physical network. To do this, you need to virtualize network management by creating virtual abstractions for network elements such as IP addresses, ports, and switches.
- Define policies that will manage traffic flow across both physical and virtual networks. You define these policies in the management system but apply them at the physical layer.
- Manage the virtualized network infrastructure by providing the tools to configure the virtual network objects and policies.

- Software Defined Networking enables you to:
  - Virtualize the network layer in a datacenter
  - Define policies for the physical and virtual networks
  - Manage the virtualized network infrastructure
- The Microsoft Software Defined Networking solution includes:
  - Network Controller
  - Hyper-V Network Virtualization
  - Hyper-V Virtual Switch
  - RRAS Multitenant Gateway
  - NIC Teaming
  - System Center Operations Manager
  - System Center Virtual Machine Manager
  - Windows Server Gateway

Microsoft has implemented Software Defined Networking in Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Hyper-V by providing the following components:

- Network Controller. Provides centralized management, configuration, monitoring, and troubleshooting of both your virtual and physical network infrastructure.




**Note:** Network Controller is a new feature in Windows Server 2016.

- Hyper-V Network Virtualization (HNV). Helps you abstract your applications and workloads from the underlying physical network by using virtual networks.

- Hyper-V Virtual Switch. Gives you the ability to connect virtual machines to both virtual networks and your physical network. Hyper-V Virtual Switch also provides security, isolation, and service-level policy enforcement.
- RRAS Multitenant Gateway. Gives you the ability to extend your network boundaries to Microsoft Azure or another provider to deliver on-demand hybrid infrastructure.
- NIC Teaming. Gives you the ability to configure multiple network adapters as a team for bandwidth aggregation and traffic failover to guard against loss of connectivity following a network component failure.

You can integrate Microsoft System Center with SDN to extend your SDN capabilities.

 **Note:** System Center is a powerful enterprise datacenter management system that you can use to monitor, provision, configure, automate, and maintain your IT infrastructure.

Microsoft System Center provides a number of SDN technologies in the following components:

- System Center Operations Manager. Provides infrastructure monitoring for your datacenter and both the private and public cloud.
- System Center Virtual Machine Manager. Gives you the ability to provision and manage virtual networks. Provides for central control of virtual network policies that link to your applications or workloads.
- Windows Server Gateway. A virtual software router and gateway that allows you to route datacenter and cloud traffic between your virtual and physical networks.

These components are discussed in more detail throughout this module.

## Benefits of SDN

Many customers with extensive network infrastructure face several common problems, which SDN can help to solve. The four main challenges are:

- Resources are finite. Finding the tools and resources to address the needs of business groups is difficult. This results in the IT department becoming a bottleneck to organizational growth.
- Resources are inflexible. After you address a business need by deploying IT infrastructure components and services, it is difficult to shift it around to address other needs.
- Mistakes are expensive. If the infrastructure fails to deliver, then the cost to the business can be huge.
- Networks are not always secure. The more software and hardware you have to address your business needs, the greater is the security risk. Managing the security of a distributed and disparate network infrastructure can be difficult.

- Challenges faced by many IT departments today include:
  - Resources are finite
  - Resources are inflexible
  - Mistakes are expensive
  - Networks are not always secure
- SDN overcomes these challenges and enables you to be:
  - Flexible
  - Efficient
  - Scalable

SDN enables you to take advantage of a cloud-based infrastructure to overcome the limitations in your on-premises infrastructure, regardless of whether those limitations are short-term or persistent. This facility enables you to be:

- 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 that let you scale up your infrastructure when needed.

## Planning for Software Defined Networking

### Requirements

Before you can deploy a Software Defined Network, you must ensure that your network infrastructure meets the following prerequisites. These prerequisites fall into two categories:

- Physical network. You must be able to access all of your physical networking components. These will include:
  - Virtual LANs (VLANs)
  - Routers
  - Border Gateway Protocol (BGP) devices
  - Data Center Bridging with Enhanced Transmission Selection if using a Remote Direct Memory Access (RDMA) technology
  - Data Center Bridging with Priority-based Flow Control if using an RDMA technology that is based in RDMA over Converged Ethernet (RoCE)
- Physical compute hosts. These computers run the Hyper-V role and host the SDN infrastructure and tenant virtual machines. These hosts must:
  - Have Windows Server 2016 installed.
  - Have the Hyper-V role enabled.
  - Have an external Hyper-V Virtual Switch created with at least one physical adapter.
  - Be reachable with a Management IP address assigned to the Management Host virtual NIC (vNIC).

You must plan the following aspects of your Software Defined Networking configuration:

- Management and HNV Provider logical networks
- Logical networks for gateways and the software load balancer
- Logical networks required for RDMA-based storage
- Routing infrastructure
- Default gateways
- Network hardware

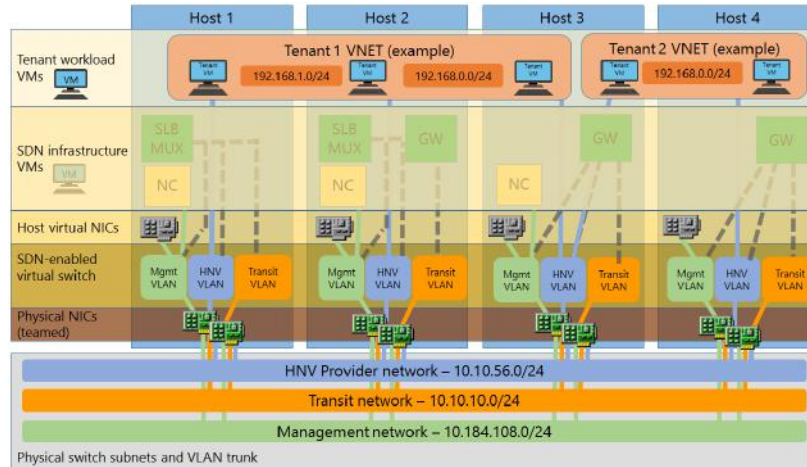




## Software Defined Networking configuration

After you have ensured that your infrastructure meets these requirements, you must plan your SDN configuration. The components of a typical SDN deployment are shown in the following diagram.

A sample Software Defined Network architecture showing four Hyper-V hosts and two tenants:



A typical SDN deployment consists of the following components:

- Management and HNV Provider logical networks. All physical compute hosts must be able to access the Management logical network and the HNV Provider logical network.

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 or else manually assign static IP configurations.

**Note:** The Management logical network is used by compute hosts to communicate with one another. All physical compute hosts need to have access to the Management logical network. All compute hosts must be reachable by using a Management IP address assigned to the Management Host vNIC.

- Logical networks for gateways and the software load balancer. You must create and provision additional logical networks for gateway and Software Load Balancing (SLB) usage. These include:
  - Transit logical network. Used by the RAS Gateway and SLB multiplexer (MUX) to exchange BGP peering information and North/South (external-internal) tenant traffic.

**Note:** Only physical compute hosts that run HNV Gateway or SLB MUX virtual machines must have connectivity to the Transit logical network subnet.

- Public virtual IP address (VIP) logical network. Required to have IP subnet prefixes that are Internet-routable outside of the cloud environment. These are the front-end IP addresses that external clients use to access resources in the virtual networks.

- Private VIP logical network. Used for VIPs that are only accessed from internal cloud clients, such as Generic Route Encapsulation (GRE) gateways or private services, and therefore do not need to be routable outside of the cloud.
- GRE VIP logical network. Exists solely for defining VIPs that are assigned to gateway virtual machines running on your SDN fabric for a server-to-server (S2S) GRE connection type.
- Logical networks required for RDMA-based storage. If you are using RDMA-based storage, then you must define a VLAN and a subnet for each physical adapter in your compute and storage hosts.
- Routing infrastructure. Routing information for the VIP subnets is advertised by the SLB MUX and HNV Gateways into the physical network by using internal BGP peering. You must create a BGP peer on the router that your SDN infrastructure uses to receive routes for the VIP logical networks advertised by the SLB MUXs and HNV Gateways. Typically, you configure BGP peering in a managed switch or router as part of the network infrastructure.
- Default gateways. You must configure only one default gateway on computers that are configured to connect to several networks, such as the physical compute hosts and gateway virtual machines. You usually configure the default gateway on the adapter that is used to reach all the way to the Internet.
- Network hardware. Your network hardware has a number of requirements, including those for network interface cards, switches, link control, availability and redundancy, and monitoring.



**Note:** For more information, refer to: “Plan a Software Defined Network Infrastructure” at: <http://aka.ms/Partnc>

## Deploying Software Defined Networking by using scripts

After you have planned your Software Defined Networking and configured your compute hosts, you can deploy a Software Defined Network. You can do this by using Virtual Machine Manager or by using scripts. This topic describes the process of using scripts to deploy Software Defined Networks.



**Note:** For more information on how to deploy a Software Defined Network by using Virtual Machine Manager, refer to: <http://aka.ms/Y3vm9n>

Use the following high-level procedure to deploy Software Defined Networking:

1. Install host networking and validate the configuration
2. Run SDN Express scripts and validate setup
3. Deploy a sample tenant workload and validate deployment

Use the following high-level procedure to deploy a Software Defined Network:

1. Install host networking and validate the configuration.
2. Run SDN Express scripts and validate setup.
3. Deploy a sample tenant workload and validate deployment.

## Install host networking and validate the configuration

To install host networking, complete the following tasks:

1. On your compute hosts:
  - a. Install the latest network drivers for all NICs.
  - b. Add the Hyper-V role.
  - c. Create the Hyper-V Virtual Switch.
2. Obtain the VLAN ID of your Management VLAN and attach the Management vNIC of the newly created virtual switch to the Management VLAN.



**Note:** The Management VLAN ID is determined during the planning phase.

3. Assign a valid IP configuration to the Management vNIC of the newly created virtual switch.



**Note:** The decision whether to use DHCP or static configuration is made during the planning phase.

4. Deploy a virtual machine to host the Active Directory Domain Services (AD DS) and Domain Name System (DNS) roles and then join your Hyper-V hosts to this AD DS domain.

To validate host networking setup, complete the following tasks:

1. Ensure that the virtual switch was created correctly by using the **Get-VMSwitch "Switch\_name"** cmdlet.
2. Verify that the Management vNIC on the virtual switch is connected to the VLAN by using the **Get-VMNetworkAdapterIsolation -ManagementOS** cmdlet.
3. Verify that all Hyper-V hosts are accessible by testing connectivity to their Management IP address and the fully qualified domain name (FQDN).
4. Ensure that the Kerberos credentials that are used provide access to all servers:
  - o To do this, at a command prompt, run the **winrm id -r:<Hyper-V Host FQDN>** command.

## Run SDN Express scripts and validate setup

To set up Software Defined Networking by using SDN Express scripts, complete the following tasks:

1. Download the required scripts.



**Note:** You can download the scripts from the Microsoft SDN GitHub Repository at: <http://aka.ms/lu57tt>

2. Set up your deployment computer:
  - a. Install Windows Server 2016 on the deployment computer.
  - b. Extract the scripts and copy the **SDNExpress** folder from the extract to the root of drive C on the deployment computer.
  - c. Verify that the **SDNExpress** folder contains the following subfolders:
    - **AgentConf**. This subfolder stores copies of schemas used by the SDN Host Agent on each Windows Server 2016 Hyper-V host to program network policy.
    - **Certs**. This subfolder is the temporary location for certificate files.
    - **Images**. You use this subfolder to store your Windows Server 2016 vhd image file.
    - **Tools**. This subfolder includes utilities and tools for troubleshooting.
    - **TenantApps**. This subfolder is used to deploy tenant workloads.
    - **Scripts**:
      - **SDNExpress.ps1**. This script deploys and configures the SDN fabric, including the Network Controller virtual machines, SLB/MUX virtual machines, gateway pools, and the HNV gateway virtual machines corresponding to the pools.
      - **FabricConfig.psd1**. This script is a configuration file template for the SDNExpress script. You customize this for your environment.
      - **SDNExpressTenant.ps1**. This script deploys a sample tenant workload on a virtual network with a load-balanced VIP. You can use this script with an **Undo** option to delete the corresponding configuration.
      - **TenantConfig.psd1**. This script is a template configuration file for tenant workload and S2S gateway configuration.
      - **SDNExpressUndo.ps1**. This script cleans up the fabric environment and resets it to a starting state.
      - **SDNExpressEnterpriseExample.ps1**. This script provisions one or more enterprise site environments. You can use this script with an **Undo** option to delete the corresponding configuration.
      - **EnterpriseConfig.psd1**. This script is a template configuration file.
3. Share the **C:\SDNExpress** folder.
4. Edit and configure the **SDNExpress\scripts\FabricConfig.psd1** script file by changing the **<< Replace >>** tags with specific values to fit your infrastructure including:
  - Host names
  - Domain names
  - Usernames and passwords
  - Network information for your networks
5. In DNS, create a Host A record for:
  - The NetworkControllerRestName (FQDN)
  - The NetworkControllerRestIP
6. Run the following script as a Domain Admin:

```
SDNExpress\scripts\SDNExpress.ps1 -ConfigurationDataFile FabricConfig.psd1 -Verbose
```



**Note:** If you have to roll back the configuration, run the following command:

```
SDNExpress\scripts\SDNExpressUndo.ps1 -ConfigurationDataFile FabricConfig.psd1 -
Verbose
```

If the script ran without errors, you can proceed to validate the setup. Complete the following procedure to validate your Software Defined Networking setup:

1. Ensure that the Network Controller Host Agent and SLB Host Agent are running on all Hyper-V hosts by using the **Get-Service NCHostAgent** and **Get-Service SlbHostAgent** cmdlets.
2. Verify network connectivity on the Management logical network between all Network Controller node virtual machines and Hyper-V hosts.
3. Use **Netstat.exe** to check that the Network Controller Host Agent is connected to the Network Controller on TCP:6640.
4. Verify that the dynamic IPs associated with all Hyper-V hosts that are hosting load-balanced tenant workload virtual machines have Layer-3 IP connectivity to the SLB Manager VIP address.
5. Use diagnostic tools to ensure that there are no errors on any fabric resources in the Network Controller. For example, use the **Debug-NetworkControllerConfigurationState** cmdlet.
6. Verify the BGP peering state to ensure that the SLB MUX is peered to the Top-of-Rack switch or RRAS virtual machine (the BGP peer). Run the following cmdlet from a Network Controller node virtual machine: **Debug-SlbConfigState**.

### Deploy a sample tenant workload and validate deployment

After you have deployed SDN and verified the configuration, you can deploy a sample tenant workload.



**Note:** This sample tenant workload consists of two virtual subnets (a web tier and a database tier) that are protected with access control list rules by using the SDN distributed firewall. The web tier's virtual subnet is accessible through the SLB MUX by using a VIP address. The script automatically deploys two web tier virtual machines and one database tier virtual machine and connects these to the virtual subnets.

Validate your SDN deployment by performing the following steps:

1. Edit and configure the **SDNExpress\scripts\TenantConfig.psd1** file by changing the << **Replace** >> tags with specific values, including the:
  - o VHD image name
  - o Network controller representational state transfer (REST) name
  - o vSwitch Name
2. Run the following script:

```
SDNExpress\scripts\SDNExpressTenant.ps1 -ConfigurationDataFile TenantConfig.psd1 -
Verbose
```



**Note:** If you have to roll back the configuration, run the following command:

```
SDNExpress\scripts\SDNExpressTenant.ps1 -Undo -ConfigurationDataFile
TenantConfig.psd1 -Verbose
```

3. Validate the tenant deployment by performing the following steps:
  - a. Sign in to the database tier virtual machine and verify network connectivity to the IP address of one of the web tier virtual machines.
  - b. Check the Network Controller tenant resources for any errors by running the following cmdlet from any Hyper-V host with Layer-3 connectivity to the Network Controller: **Get-NetworkControllerConfigurationState -NCIP <FQDN of Network Controller REST Name>**.
  - c. Validate that the policy has been received and persisted in the Network Controller Host Agent by running the following cmdlet: **ovsdb-client.exe dump tcp:127.0.0.1:6641 ms\_vtep**.
  - d. Check that an IP address has been assigned for a provider address (PA) Host vNIC and the Ethernet adapters for the PA Host vNIC by using the **ipconfig /allcompartments /all** command.
  - e. Check PA connectivity between two hosts with a ping command. Obtain the compartment ID from the output of the previous command: **ping -c <compartment Id> <Remote Hyper-V Host PA IP Address>**.

Verify the correctness of the statement by placing a mark in the column to the right.

Statement	Answer
In Software Defined Networking, 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 Software Defined Networking?

## Lesson 2

# Implementing network virtualization

Network virtualization is a part of Software Defined Networking in Windows Server 2016 with which you can create virtual networks that are isolated logically on the same physical network infrastructure. This lesson explores the features and technologies in network virtualization.

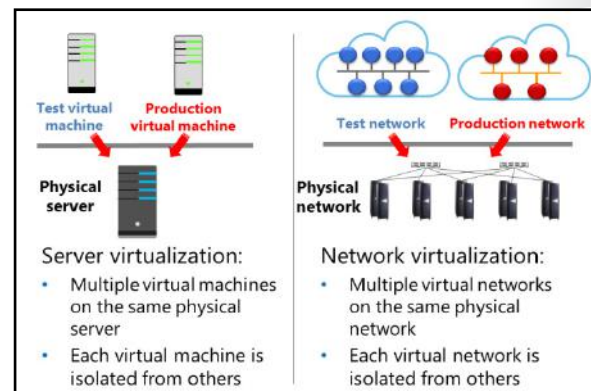
### Lesson Objectives

After completing this lesson, you will be able to:

- Explain network virtualization.
- Identify the benefits of network virtualization.
- Describe Network Virtualization Generic Route Encapsulation (NVGRE).
- Explain network virtualization policies.

### What is network virtualization?

Network virtualization provides functionality for managing network traffic that is similar to what server virtualization does for managing virtual machines. You can use server virtualization to run multiple virtual machines on the same physical server. The same is true for network virtualization. You can have multiple virtual networks, which are logically isolated, on the same physical network infrastructure. From each virtual network, it seems that only the virtual network is using the physical network infrastructure, even though multiple virtual networks could be using the same physical infrastructure at the same time.



*Network virtualization* is an implementation of SDN and provides a layer of abstraction over the physical network. To achieve this abstraction, the virtualization platform has to support it. The Hyper-V Virtual Switch in Windows Server 2016 supports network virtualization by using two IP addresses for each virtual machine. By using the two IP addresses, you can use network virtualization to keep the logical network topology, which is virtualized and separated from the actual underlying physical network topology, and addresses used on the physical network. Thus, you can run virtual machines and provide them with the same network access without any modification on any Hyper-V host, assuming that Hyper-V hosts are configured to map between both IP addresses.

## Benefits of network virtualization

Network virtualization provides a layer of abstraction between the physical network and network traffic and thereby provides the following benefits:

- Flexible virtual machine placement. Network virtualization provides abstraction and separates IP addresses used in virtual machines from the IP addresses used on the physical network. This way, you can place a virtual machine on any Hyper-V host in the datacenter, and the IP address assignment or VLAN isolation restrictions of the physical network no longer restricts the placement.
- Multitenant network isolation without VLANs. You can define and enforce network traffic isolation without the use of VLANs or the need to reconfigure physical network switches. Because network virtualization uses a 24-bit identifier for virtual networks compared to a 12-bit identifier for VLANs, you are also not limited to 4094 VLAN IDs. Also, with network virtualization, no manual reconfiguration of physical hardware is required when you move existing virtual machines or create new ones.
- IP address reuse. Virtual machines in different virtual networks can use the same or overlapping IP address space, even when deploying those virtual machines on the same physical network. Virtual networks are isolated, and they can use the same address space without any conflict or issue.
- Live migration across subnets. Without network virtualization, virtual machine live migration is limited to the same IP subnet or VLAN, because when a virtual machine moves to different subnets, its IP address has to change to match the new network. With network virtualization, you can move virtual machines by using live migration between two Hyper-V hosts in different subnets without having to change the virtual machine IP address. With the use of network virtualization, the virtual machine location change updates and synchronizes among computers that have ongoing communication with the migrated virtual machine.
- Compatibility with existing network infrastructure. Network virtualization is compatible with existing network infrastructure, and you can deploy it in an existing datacenter. You do not need to redesign the physical network layer to implement network virtualization.
- Transparent moving of virtual machines to a shared infrastructure as a service (IaaS) cloud. With IaaS, the physical platform where the virtual machines run is hosted in a separate datacenter, usually accessible through the Internet. When network virtualization is used, IP addresses, IP policies, and virtual machine configurations remain unchanged, regardless of which Hyper-V host the virtual machine is running on. As a result, you can move virtual machines between Hyper-V hosts in your datacenter, between Hyper-V hosts in different datacenters, and between a Hyper-V host in your datacenter and the shared IaaS cloud.
- Support for resource metering. With Hyper-V in Windows Server 2016, you can enable resource metering. Resource metering provides information about the usage of host and network resources for individual virtual machines. You can use this information to charge the tenants for actual resource usage. You can enable network resource metering for virtual machines that use network virtualization.

- Flexible virtual machine placement
- Multitenant network isolation without VLANs
- IP address reuse
- Live migration across subnets
- Compatibility with existing network infrastructure
- Transparent moving of virtual machines to a shared IaaS cloud
- Support for resource metering
- Configuration by using Windows PowerShell or by using System Center Virtual Machine Manager

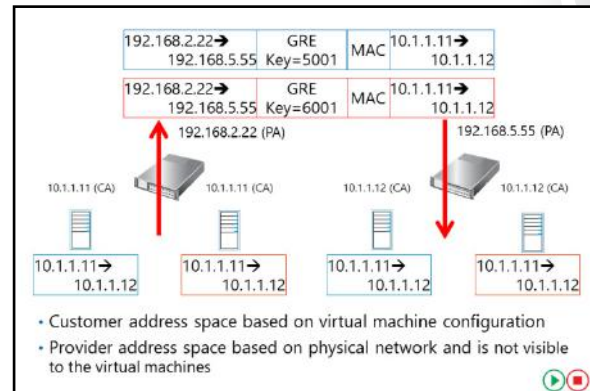


- Configuration by Windows PowerShell. Network virtualization supports Windows PowerShell for configuring the network virtualization and isolation policies. The Hyper-V module includes cmdlets that you can use to configure, monitor, and troubleshoot network virtualization. Configuring network virtualization in Windows PowerShell is complex, so we strongly recommend that you use the Virtual Machine Manager to configure and manage network virtualization.

## What is Generic Route Encapsulation?

Windows Server 2016 Hyper-V use *Network Virtualization Generic Route Encapsulation* (NVGRE) to implement network virtualization. When network virtualization is used, each virtual network adapter is associated with two IP addresses. Those two addresses are:

- Customer address (CA). This is the IP address that is configured and used by the virtual machine. This address is configured in the properties of the virtual network adapter in the virtual machine guest operating system, regardless of whether network virtualization is used. A virtual machine uses the CA when communicating with another system, and if you migrate a virtual machine to a different Hyper-V host, the CA can remain the same.
- Provider address (PA). This is the IP address that the virtualization platform assigns to the Hyper-V host and is dependent on the physical network infrastructure where the Hyper-V host is connected. When network virtualization is used and the virtual machine sends network traffic, the Hyper-V host encapsulates the packets and includes the PA as the source address from where packets were sent. The PA is visible on the physical network but not visible to the virtual machine. If you migrate a virtual machine to a different Hyper-V host, the PA changes.



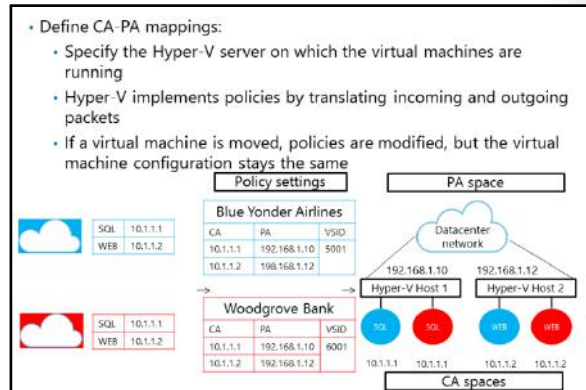
## Using NVGRE

When a virtual machine has to communicate over a network and you have configured network virtualization, NVGRE is used to encapsulate its packets. For example, assume that one virtual machine is configured with IP address 10.1.1.11 (CA 1) and is running on a Hyper-V host that uses IP address 192.168.2.22 (PA 1). The second virtual machine is configured with IP address 10.1.1.12 (CA 2) and is running on Hyper-V host with IP address 192.168.5.55 (PA 2). If network virtualization is used, the first Hyper-V host will use NVGRE to encapsulate the virtual machine packets, which contain the source (CA 1) and the destination IP address (CA 2), into the envelope. This envelope uses its own IP address (PA 1) as the source address and the IP address of the Hyper-V host on which the second virtual machine is running (PA 2) as the destination address. Encapsulated packages will be sent on the physical network between the two Hyper-V hosts. The destination Hyper-V host (PA 2) will extract the envelope from the encapsulated packet and pass it to the destination virtual machine (CA 2), which is running on that Hyper-V host.

With NVGRE, you can configure virtual machines with the same IP addresses and deploy them on the same or different host machines. To address this scenario, the GRE envelope header includes a field named Key, which represents a Virtual Subnet ID. When implementing network virtualization, you define a Virtual Subnet ID on the Hyper-V host for each network used by the hosted virtual machines. The Virtual Subnet ID is used to separate and isolate traffic between different virtual networks and enables Hyper-V host to pass the traffic only to virtual machines on the same virtual network.

## What are network virtualization policies?

If you configure network virtualization and if two virtual machines have to communicate, the Hyper-V host that the first virtual machine is running on must be aware which Hyper-V host the second virtual machine is running on before the host can encapsulate network packets into GRE envelopes. If both virtual machines are running on the same Hyper-V host, Hyper-V already has this information. But virtual machines usually run on different Hyper-V hosts, so you must configure network virtualization to ensure the virtual machines can communicate. You configure network virtualization by deploying network virtualization policies. Network virtualization policies define the mappings between IP address spaces used by the virtual machines (CA spaces) and the IP addresses of the Hyper-V hosts that those virtual machines are running on (PA spaces). Before sending traffic on the physical network, the Hyper-V hosts consult the network virtualization policies to determine on which Hyper-V host the target virtual machine is running and encapsulate the traffic with a GRE envelope. The encapsulated traffic is sent on the physical network only after that determination.



For example, assume that you are hosting two companies, Blue Yonder Airlines and Woodgrove Bank, with the following configuration:

- Blue Yonder Airlines is running Microsoft SQL Server data management software in a virtual machine with the IP address 10.1.1.1 and a web server in a virtual machine with the IP address 10.1.1.2. The web server is using SQL Server as a database for storing transactions.
- Woodgrove Bank is running SQL Server in a virtual machine configured with the same IP address 10.1.1.1 and a web server in a virtual machine with the IP address 10.1.1.2. The web server is using SQL Server as a database for storing transactions.
- The computers running SQL Server for both companies are running on Hyper-V Host 1, which has the IP address 192.168.1.10. Web servers for both companies are running on Hyper-V Host 2, which has the IP address 192.168.1.12.

This means that the virtual machines have the following CAs and PAs.

Organization	CAs	PAs
Blue Yonder Airlines	SQL is 10.1.1.1; WEB is 10.1.1.2	SQL is 192.168.1.10; WEB is 192.168.1.12
Woodgrove Bank	SQL is 10.1.1.1; WEB is 10.1.1.2	SQL is 192.168.1.10; WEB is 192.168.1.12

To enable communication between the virtual machines, you need to configure a virtual network. For example, you could configure a virtual network for Blue Yonder Airlines with the Virtual Subnet ID 5001 and configure a virtual network for Woodgrove Bank with the Virtual Subnet ID 6001. You also create network virtualization policies for both companies and apply policies to Hyper-V Host 1 and Hyper-V Host 2.

When the Blue Yonder Airlines WEB virtual machine on Hyper-V Host 2 queries its SQL Server at 10.1.1.11, the following process happens:

1. Hyper-V Host 2, based on its policy settings, translates the addresses in the packet from the following:
  - o Source: 10.1.1.2 (the CA of Blue Yonder Airlines WEB)
  - o Destination: 10.1.1.1 (the CA of Blue Yonder Airlines SQL)
2. The addresses are translated into the encapsulated packet that contains the following:
  - o GRE header with Virtual Subnet ID: 5001
  - o Source: 192.168.2.12 (the PA for Blue Yonder Airlines WEB)
  - o Destination: 192.168.1.10 (the PA for Blue Yonder Airlines SQL)



**Note:** The encapsulated packet also contains the original packet.

When Hyper-V Host 1 receives the packet, based on its policy settings, it will decapsulate the NVGRE packet, determine that it is for the Blue Yonder Airlines virtual network (Virtual Subnet ID 5001), and pass it to the virtual machine with IP 10.1.1.1, as specified in the original (encapsulated) packet.



**Note:** You can configure network virtualization policies by using Windows PowerShell. It is easier to configure network virtualization policies with tools such as System Center Virtual Machine Manager.

You can use network virtualization and network virtualization policies to move virtual machines between Hyper-V hosts and preserve their network configuration. When you move a virtual machine, you need to update only the network virtualization policies to reflect the new Hyper-V host on which the virtual machine is running; the virtual machine network configuration stays the same and is still connected to the same virtual network.

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

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

## Lesson 3

# Implementing Network Controller

Network Controller, a new feature of Windows Server 2016, gives you the ability to manage, configure, monitor, and troubleshoot virtual and physical network infrastructure in your datacenter by using a centralized, programmable point of automation. Using Network Controller, you can automate the configuration of your network infrastructure without needing to perform manual configuration of network devices and services.


### Lesson Objectives

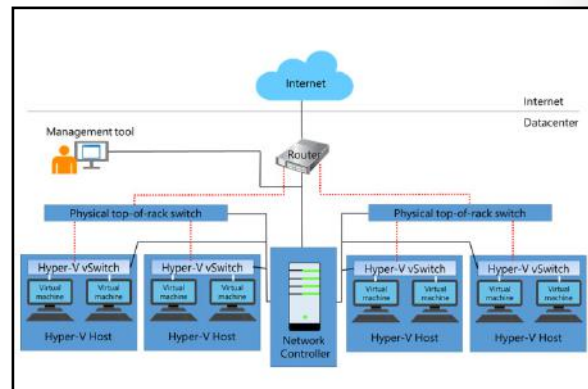
After completing this lesson, you will be able to:

- Describe Network Controller.
- List the requirements for installing Network Controller.
- Prepare to deploy Network Controller.
- Describe the procedure for deploying Network Controller.
- Describe the role of Network Controller in Datacenter Firewall.
- Describe the role of Network Controller in SLB.
- Describe the role of Network Controller in RAS Gateway.
- Deploy Network Controller.

### What is Network Controller?

Network Controller is a Windows Server 2016 server role. It provides two application programming interfaces (APIs): the Southbound API and the Northbound API. The first of these enables Network Controller to communicate with the network, while the second API gives you the ability to communicate with Network Controller.

 **Note:** You can deploy Network Controller in AD DS domain and non-domain environments. In AD DS domain environments, Network Controller authenticates users and devices with Kerberos, while in non-domain environments, you must deploy digital certificates to provide authentication.



### Southbound API

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 of the information you need about the network.
- Send information to the network infrastructure, for example, configuration changes that you have made.

### **Northbound API**

The Network Controller Northbound API provides you with the ability to gather network information from Network Controller with which you can monitor and configure the network. The Network Controller Northbound API enables you to configure, monitor, troubleshoot, and deploy new devices on the network by using:

- Windows PowerShell
- REST API
- A management application with a graphical user interface, for example, System Center Virtual Machine Manager or System Center Operations Manager

### **Management with Network Controller**

You can use Network Controller to manage the following physical and virtual network infrastructure:

- Hyper-V virtual machines and virtual switches
- Datacenter Firewall
- RAS Multitenant Gateways, Virtual Gateways, and gateway pools
- Load balancers

Network Controller provides a number of features with which you can configure and manage both virtual and physical network devices and services. These are:

- Firewall management. You can configure and manage firewall Access Control rules for your workload virtual machines.
- SLB management. You can configure multiple servers to host the same workload, helping to provide high availability and scalability.
- Virtual network management. You can deploy and configure HNV, including Hyper-V Virtual Switch, virtual network adapters on individual virtual machines, and virtual network policies storage and distribution.
- RAS gateway management. You can provide gateway services to your tenants by deploying, configuring, and managing Hyper-V hosts and virtual machines that are members of a RAS gateway pool.

## Requirements for deploying Network Controller

You can deploy Network Controller on one or more computers, one or more virtual machines, or a combination of both. Because Network Controller is a Windows Server 2016 server role, the requirements are not complex. They are as follows:


- You can only deploy Network Controller to the Windows Server 2016 Datacenter edition.
- The management client you use must be installed on a computer or virtual machine running Windows 10, Windows 8.1, or Windows 8.
- You must configure dynamic DNS registration to enable registration of required DNS records for Network Controller.
- If the computers or virtual machines 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 that 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.

- You can deploy Network Controller only to the Windows Server 2016 Datacenter edition
- The management client must be running Windows 10, Windows 8.1, or Windows 8
- You must configure dynamic DNS registration for Network Controller
- If virtual machines running Network Controller are joined to a domain, you must create appropriate AD DS security groups
- If virtual machines running Network Controller are not joined to a domain, you must configure certificate-based authentication




**Note:** In both these instances, all users added to either of these groups must also belong to the Domain Users group.

- If the computers or virtual machines running Network Controller or the management client for Network Controller are not joined to a domain, 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. The certificate must meet the following requirements:
    - The certificate subject name must match the DNS name of the computer or virtual machine holding the Network Controller role.
    - The server authentication purpose is present in enhanced key usage (EKU) extensions.
    - The certificate subject name should resolve to one of the following addresses:
      - The IP address of the Network Controller, if Network Controller is deployed on a single computer or virtual machine.
      - The REST IP address, if Network Controller is deployed on multiple computers, multiple virtual machines, or both.
    - The certificate must be trusted by all the REST clients.
    - The certificate must be trusted by the SLB MUX and the southbound host computers that Network Controller manages.

 **Note:** A certification authority can enroll the certificate, or the certificate can be self-signed. We do not recommend self-signed certificates for production deployments, but they are acceptable for test lab environments.

- Enrolling this certificate on the Network Controller.

 **Note:** The same certificate must be provisioned on all the Network Controller nodes. After creating the certificate on one node, you can export the certificate (with private key) and import it on the other nodes.

## Demonstration: Preparing to deploy Network Controller

In this demonstration, you will see how to:

- Create AD DS security groups.
- Request a certificate.

### Demonstration Steps

#### Create AD DS security groups

1. On **LON-DC1**, open **Active Directory Users and Computers**.
2. Create the following global security groups:
  - **Network Controller Admins**
  - **Network Controller Ops**
3. Add **Beth Burke** and **Administrator** to both these groups.

These security groups are required for users that will administer Network Controller and for users that will use Network Controller to administer the network devices and services.

#### Request a certificate

1. On **LON-SVR2**, open the management console, and then add the **Certificates** snap-in with the focus on the local computer.
2. Request a **Computer** certificate.
3. Close the management console without saving changes.

This certificate is required for encryption of communication between the Network Controller and the management clients.

## The procedure for deploying Network Controller

You can deploy the Network Controller role by using Windows PowerShell by following these high-level steps:

1. Install the Network Controller server role.
2. Configure the Network Controller cluster.
3. Configure the Network Controller application.
4. Validate the Network Controller deployment.

1. Install the Network Controller server role
2. Configure the Network Controller cluster
3. Configure the Network Controller application
4. Validate the Network Controller deployment

### Install the Network Controller server role


To install the Network Controller server role, on the server computer or virtual machine that will host the role, open Windows PowerShell (Admin) and then run the following cmdlet:

```
Install-WindowsFeature -Name NetworkController -IncludeManagementTools
```

After performing this task, restart your computer or virtual machine.

### Configure the Network Controller cluster

The Network Controller cluster provides scalability and high-availability for the Network Controller application. To configure the cluster, sign in as a local administrator on the computer or virtual machine where you want to configure the cluster.

 **Note:** If the computer or virtual machine on which you deployed the Network Controller role is a domain member, the user account you use to sign in with must also belong to Domain Users.


To configure the cluster, complete the following steps:

1. Create a node object. You must create a node object for each computer or virtual machine that is a member of the Network Controller cluster. Use the **New-NetworkControllerNodeObject** cmdlet to complete this step. For example, the following command creates a Network Controller node object named Node1. The FQDN of the computer is NCNode1.Adatum.com, and Ethernet is the name of the interface on the computer listening to REST requests.

```
New-NetworkControllerNodeObject -Name "Node1" -Server "NCNode1.Adatum.com" -FaultDomain "fd:/rack1/host1" -RestInterface "Ethernet"
```

2. Configure the cluster. After you have created the node(s) for the cluster, use the **Install-NetworkControllerCluster** cmdlet to configure the cluster. For example, the following commands install a Network Controller cluster in a test lab. High-availability support is not available because a single node is used. Kerberos authentication is used between the cluster nodes.

```
$NodeObject = New-NetworkControllerNodeObject -Name "Node1" -Server "NCNode1.Adatum.com" -FaultDomain "fd:/rack1/host1" -RestInterface "Ethernet"
Install-NetworkControllerCluster -Node $NodeObject -ClusterAuthentication Kerberos
```

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



## Configure the Network Controller application

The last deployment step involves the configuration of the Network Controller application. Use the **Install-NetworkController** cmdlet to complete this procedure. For example, the following code creates a Network Controller node object, and then stores it in the \$NodeObject variable.

```
$NodeObject = New-NetworkControllerNodeObject -Name "Node01" -Server "NCNode11" -
FaultDomain "fd:/rack1/host1" -RestInterface Ethernet
```

The following command gets a certificate named NCEncryption, and then stores it in the \$Certificate variable.

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

The following command creates a Network Controller cluster by using the **Install-NetworkControllerCluster** cmdlet.

```
Install-NetworkControllerCluster -Node $NodeObject -ClusterAuthentication None
```

The following command deploys the Network Controller in a test environment. Because a single node is used in the deployment, there is no high-availability support. This Network Controller employs no authentication between the cluster nodes, nor between the REST clients and Network Controller. The command specifies the \$Certificate to encrypt the traffic between the REST clients and Network Controller.

```
Install-NetworkController -Node $NodeObject -ClientAuthentication None -RestIpAddress
"10.0.0.1/24" -ServerCertificate $Certificate
```



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

## Validate the Network Controller deployment

After you have deployed the Network Controller, you can validate the deployment by adding a credential to the Network Controller and then retrieving the credential.



**Note:** If you are using Kerberos as the ClientAuthentication mechanism—that is, if the computers or virtual machines are members of a domain—then membership in the ClientSecurityGroup that you created is the minimum required to perform this procedure. You define the ClientSecurityGroup when you use the **Install-NetworkController** cmdlet.

Complete this task by performing the following steps:

1. Open Windows PowerShell (Admin), and then run the following commands:

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
$cred.type="usernamepassword"
$cred.username="admin"
$cred.value="abcd"
New-NetworkControllerCredential -ConnectionUri https://networkcontroller -Properties
$cred -ResourceId cred1
```

2. To retrieve the credential that you added to Network Controller, run the following command:

```
Get-NetworkControllerCredential -ConnectionUri https://networkcontroller -ResourceId cred1
```


3. If everything works, you should receive output similar to the following:

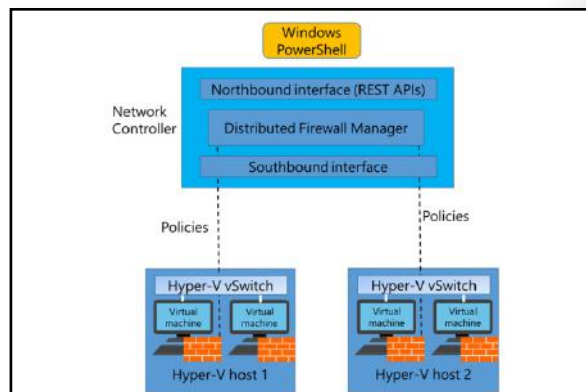
```
Tags :
ResourceRef : /credentials/cred1
CreatedTime : 1/1/0001 12:00:00 AM
InstanceId : e16ffe62-a701-4d31-915e-7234d4bc5a18
Etag : W/"1ec59631-607f-4d3e-ac78-94b0822f3a9d"
ResourceMetadata :
ResourceId : cred1
Properties : Microsoft.Windows.NetworkController.CredentialProperties
```

You have successfully verified the deployment.

## Datacenter Firewall

Datacenter Firewall in Windows Server 2016 helps you install and configure firewall policies to protect your virtual networks from unwanted network traffic. You manage the Datacenter Firewall policies by using Network Controller Northbound APIs.

 **Note:** Both the cloud service provider admin and the tenant admin can manage Datacenter Firewall policies by using the Network Controller.



### Benefits for cloud provider

For cloud service providers, the Datacenter Firewall provides these benefits:

- A software-based firewall solution that is highly scalable and manageable and that can easily be offered to tenants.
- The ability to easily move tenant virtual machines to different compute hosts without disrupting tenant firewall configuration because:
  - It is deployed as a vSwitch port host agent firewall.
  - Tenant virtual machines get the policies assigned to their vSwitch host agent firewall.
  - Firewall rules are configured in each vSwitch port, independent of the host that runs the virtual machine.
- Protection to tenant virtual machines regardless of the tenant guest operating system.

## Benefits for tenants

For tenants, the Datacenter Firewall provides the ability to:

- Define firewall rules that can help protect Internet-facing workloads on their virtual networks.
- Define firewall rules that can help protect traffic between virtual machines on the same L2 virtual subnet and also between virtual machines on different L2 virtual subnets.
- Define firewall rules that can help protect and isolate network traffic between tenant on-premises networks and their virtual networks at the service provider.

## Software Load Balancing


You can use Software Load Balancing (SLB) in SDN to distribute network traffic across available network resources. Windows Server SLB provides the following features:

- Layer 4 load balancing for both "North-South" and "East-West" Transmission Control Protocol/User Datagram Protocol (TCP/UDP) traffic
- Public and internal network traffic load balancing
- Support for dynamic IP addresses on VLANs and on Hyper-V virtual networks
- Support for health probe

Windows Server SLB provides the following features:

- Layer 4 load balancing for both "North-South" and "East-West" TCP/UDP traffic
- Public and internal network traffic load balancing
- Support for dynamic IP addresses on VLANs and on Hyper-V virtual networks
- Support for health probe


SLB maps VIPs to dynamic IP addresses that are part of a set of resources in the cloud. In this scenario, VIPs are single IP addresses that map to a pool of available virtual machines. Dynamic IP addresses are assigned to tenant resources within the cloud infrastructure.

 **Note:** VIPs are IP addresses available on the Internet for tenants and tenant customers to connect to tenant resources in the cloud datacenter. Dynamic IP addresses are the IP addresses of the virtual machines that are members of a load-balanced pool.


## SLB infrastructure

The SLB infrastructure consists of the following components:


- Virtual Machine Manager. You use Virtual Machine Manager to configure Network Controller, including Health Monitor and SLB Manager.

 **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>

- Network Controller. Before you can deploy SLB in Windows Server 2016, you must first deploy Network Controller. Network Controller performs the following functions in SLB:
  - Processes SLB commands that arrive via the Northbound API from Virtual Machine Manager, Windows PowerShell, or other network management application.
  - Calculates policy for distribution to Hyper-V hosts and SLB MUXs.
  - Provides the health status of the SLB infrastructure.
  - Provides each MUX with each VIP.
  - Configures and controls the behavior of the VIP to dynamic IP mapping in the MUX.

 **Note:** Specifically, you define load balancing policies by using Network Controller, and the MUX maps VIPs to the correct dynamic IP addresses by using these policies. These load balancing policies include Protocol, Front-end port, Back-end port, and distribution algorithm (5-, 3-, or 2-tuples).

- SLB MUX. When network inbound Internet traffic arrives, the SLB MUX maps and rewrites the traffic so that it will arrive at an individual dynamic IP. This is based on an examination of the traffic by the MUX for the destination VIP. Within the SLB infrastructure, the MUX:
  - Holds the VIPs.
  - Uses BGP to advertise each of the VIPs to routers on the physical network.
  - Consists of one or more virtual machines.
- Hosts that run Hyper-V. You use SLB with computers that are running Windows Server 2016 and Hyper-V.
- SLB Host Agent. The SLB Host Agent:
  - Listens for SLB policy updates from Network Controller.
  - Programs rules for SLB into the Software Defined Networking–enabled Hyper-V virtual switches that are configured on the local computer.

 **Note:** When you deploy SLB, you must deploy the SLB Host Agent on every Hyper-V host computer. You can install this agent on all versions of Windows Server 2016 that support the Hyper-V role, including Nano Server.

- Software Defined Networking–enabled Hyper-V Virtual Switch. For a virtual switch to be compatible with SLB, you must use Hyper-V Virtual Switch Manager or Windows PowerShell commands to create the switch, and then you must enable Virtual Filtering Platform for the virtual switch. The virtual switch performs the following actions for SLB:
  - Processes the data path for SLB.
  - Receives inbound network traffic from the MUX.
  - Bypasses the MUX for outbound network traffic, sending it to the router by using direct server return (DSR).
  - Runs on Nano Server instances of Hyper-V.

- BGP-enabled router. BGP allows the routers to:
  - Route inbound traffic to the MUX by using equal-cost multi-path routing (ECMP).
  - For outbound network traffic, use the route provided by the host.
  - Listen for route updates for VIPs from SLB MUX.
  - Remove SLB MUXs from the SLB rotation if Keep Alive fails.

## RAS Gateway

When you implement network virtualization by using the Hyper-V Virtual Switch, the switch operates as a router between different Hyper-V hosts in the same infrastructure. The network virtualization policies define how packets will be routed from one host to another. However, a virtual switch cannot route to networks outside the Hyper-V server infrastructure when using network virtualization. If you were not using network virtualization, you would just connect the virtual machine to an external switch, and the virtual machine could connect to the same networks as the host machine.

RAS Gateway provides the following features:

- Site-to-site VPN
- Point-to-site VPN
- GRE tunneling
- Dynamic routing with BGP

Use RAS Gateway in the following scenarios:

- Multitenant-aware VPN gateway
- Multitenant-aware NAT gateway
- Forwarding gateway for internal physical network access



But in a network virtualization scenario, you might have multiple virtual machines running on a Hyper-V host that share the same IP addresses. You might also want to move the virtual machine to any host in the network without disrupting network connectivity. You must be able to connect the virtualized networks to the Internet by using a mechanism that is multitenant-aware so that traffic to external networks is correctly routed to the internal addresses that the virtual machines use. Windows Server 2016 provides the RAS Gateway to address these issues.



**Note:** RAS Gateway is referred to as Windows Server Gateway in System Center.

### Overview of RAS Gateway

RAS Gateway is a software-based, multitenant, BGP-capable router. It is designed for cloud service providers and large organizations that host multiple tenant virtual networks using Hyper-V Network Virtualization (HNV). RAS Gateway provides the following features:

- Site-to-site VPN. Gives you the ability to connect two networks at different physical locations across the Internet with a site-to-site VPN connection.
- Point-to-site VPN. Gives organization employees or administrators the ability to connect to your organization's network from remote locations.
- GRE tunneling. Enables connectivity between tenant virtual networks and external networks.
- Dynamic routing with BGP. Reduces the need for manual route configuration on routers because it is a dynamic routing protocol, and automatically learns routes between sites that are connected by using site-to-site VPN connections.

## Scenarios for use

You can implement RAS Gateway in several different configurations:

- Multitenant-aware VPN gateway. In this configuration, RAS Gateway is configured as a VPN gateway that is aware of the virtual networks deployed on the Hyper-V hosts. Deploying RAS Gateway with this configuration means that you can connect to the RAS Gateway by using a site-to-site VPN from a remote location or that you can configure individual users with VPN access to the RAS Gateway. The RAS Gateway operates like any other VPN gateway, where it allows the remote users to connect directly to the virtual networks on the Hyper-V servers. The main difference is that the RAS Gateway is multitenant-aware, so you can have multiple virtual networks with overlapping address spaces located on the same virtual infrastructure. This configuration is useful for organizations that have multiple locations or multiple business groups that share the same address spaces and must be able to route traffic to the virtual networks. Hosting providers also can use this configuration to provide remote clients direct network access between their on-premises network and the hosted networks.
- Multitenant-aware network address translation (NAT) gateway for Internet access. In this configuration, RAS Gateway provides access to the Internet for virtual machines on virtual networks. The RAS Gateway is configured as a NAT device, which translates addresses that can connect to the Internet to addresses used on the virtual networks. In this configuration, RAS Gateway is also multitenant-aware, so all virtual networks behind the RAS Gateway can connect to the Internet, even if they use overlapping address spaces.
- Forwarding gateway for internal physical network access. In this configuration, RAS Gateway provides access to internal network resources that are located on physical networks. For example, an organization may have some servers that are still deployed on physical hosts. When configured as a forwarding gateway, RAS Gateway enables computers on the virtual networks to connect to those physical hosts.

## Network Controller with RAS Gateway

By using Network Controller you can deploy, configure, and manage Hyper-V hosts and virtual machines that are members of a RAS Gateway pool, so you can provide RAS Gateway services to your tenants. You can use Network Controller to automatically deploy virtual machines running RAS Gateway to support the following features:

- Ability to add and remove gateway virtual machines from the RAS Gateway pool and specify the level of backup required.
- Site-to-site VPN gateway connectivity between remote tenant networks and your datacenter using Internet Protocol security (IPsec).
- Site-to-site VPN gateway connectivity between remote tenant networks and your datacenter using GRE.
- Point-to-site VPN gateway connectivity so that your tenants' administrators can access their resources on your datacenter from anywhere.
- Layer 3 forwarding capability.
- BGP routing, so you can manage the routing of network traffic between your tenants' virtual machine networks and their remote sites.

## Demonstration: Deploying Network Controller

In this demonstration, you will see how to:

- Add the Network Controller role.
- Configure the Network Controller cluster.
- Configure the Network Controller application.
- Validate the deployment.

### Demonstration Steps

#### Add the Network Controller role

1. Use **Server Manager** to add the **Network Controller** server role.
2. Restart the computer after the role installation is complete.

#### Configure the Network Controller cluster

1. Create a new Network Controller node. At a Windows PowerShell (Admin) command prompt, run the following command:

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

2. Retrieve details about a certificate in the local computer store for use in client encryption. At the Windows PowerShell (Admin) command prompt, run the following command:

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

3. Install the Network Controller cluster. At the Windows PowerShell (Admin) command prompt, run the following command:

```
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, run the following command:

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

#### Validate the deployment

- Run the following commands in sequence to validate the deployment:

```
$cred=New-Object Microsoft.Windows.Networkcontroller.credentialproperties
$cred.type="usernamepassword"
$cred.username="admin"
$cred.value="abcd"
New-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
Properties $cred -ResourceId cred1
Get-NetworkControllerCredential -ConnectionUri https://LON-SVR2.Adatum.com -
ResourceId cred1
```

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

## Lab: Deploying Network Controller

### Scenario

A Datum Corporation intends to deploy and use Network Controller to manage network services and devices. You should set up a trial of the technology in a test lab.

### Objectives

After completing this lab, you will be able to:

- Prepare to deploy Network Controller.
- Deploy Network Controller.

### Lab Setup

Estimated Time: 30 minutes

Virtual machines: **20741A-LON-DC1** and **20741A-LON-SVR2**

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20741A-LON-DC1**, and in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20741A-LON-SVR2**.

## Exercise 1: Preparing to deploy Network Controller

### Scenario

You decide to deploy Network Controller on a single virtual machine called **LON-SVR2** by using Server Manager. Beth Burke and the domain administrator account will be responsible for managing Network Controller and for managing the network using Network Controller. The first stage in your test deployment is to configure the required security groups in AD DS and to obtain a certificate for encryption on the Network Controller server.

The main tasks for this exercise are as follows:

1. Create the required AD DS security groups.
2. Request a certificate for authenticating Network Controller.



► **Task 1: Create the required AD DS security groups**

1. On **LON-DC1**, from **Server Manager**, open **Active Directory Users and Computers**.
2. Create the following global security groups:
  - **Network Controller Admins**
  - **Network Controller Ops**
3. Add **Beth Burke** and **Administrator** to both these groups.
4. Close **Active Directory Users and Computers**.

► **Task 2: Request a certificate for authenticating Network Controller**

1. On **LON-SVR2**, open the management console, and then add the **Certificates** snap-in with the focus on the local computer.
2. Request a **Computer** certificate.
3. Close the management console without saving changes.

**Results:** After completing this exercise, you should have successfully prepared your environment for Network Controller.

## Exercise 2: Deploying Network Controller

### Scenario

After creating the required groups and obtaining the relevant certificate on LON-SVR2, you must now use Windows PowerShell to deploy Network Controller.

The main tasks for this exercise are as follows:

1. Add the Network Controller role.
2. Configure the Network Controller cluster.
3. Configure the Network Controller application.
4. Verify the deployment.
5. Prepare for course completion.

► **Task 1: Add the Network Controller role**

1. On **LON-SVR2**, use **Server Manager** to add the **Network Controller** server role.
2. Restart the computer after the role installation is complete.
3. Sign in as **Adatum\administrator** with the password as **Pa\$\$w0rd**.

## ► Task 2: Configure the Network Controller cluster



**Note:** These steps are duplicated in the detailed steps for this lab due to the complexity of the Windows PowerShell cmdlets.

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 "Ethernet"
```

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
```

## ► Task 3: Configure the Network Controller application



**Note:** This step is duplicated in the detailed steps for this lab due to the complexity of the Windows PowerShell cmdlets.

- 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
```

## ► Task 4: Verify the deployment



**Note:** These steps are duplicated in the detailed steps for this lab due to the complexity of the Windows PowerShell cmdlets.

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

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

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

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

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

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

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

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

- 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
```

- Press **Y**, and then press Enter when prompted.
- 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
```

- You should receive output that looks similar to the output below:

```
Tags                :
ResourceRef         : /credentials/cred1
CreatedTime         : 1/1/0001 12:00:00 AM
InstanceId          : e16ffe62-a701-4d31-915e-7234d4bc5a18
Etag                : W/"1ec59631-607f-4d3e-ac78-94b0822f3a9d"
ResourceMetadata   :
ResourceId          : cred1
Properties          : Microsoft.Windows.NetworkController.CredentialProperties
```

**Results:** After completing this exercise, you should have successfully deployed Network Controller.

### ► Task 5: Prepare for course completion

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

- On the host computer, start **Hyper-V Manager**.
- In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
- In the **Revert Virtual Machine** dialog box, click **Revert**.
- Repeat steps 2 and 3 for **20741A-LON-SVR2**.

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

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

## 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?

**Question:** What are the reasons to consider implementing Software Defined Networking with Windows Server 2016?

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

## Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 1: Planning and implementing an IPv4 network

## Lab A: Planning an IPv4 network

### Exercise 1: Planning the IPv4 address assignments

#### ► Task 1: Plan the IPv4 implementation

1. How will you determine the number of IP addresses required for each location?

**Answer:** The key factors for this exercise are the number of systems per location and the requirements.

2. How do the laptops that have both wired and wireless network adapters affect the number of IP addresses required?

**Answer:** There is a requirement for all potential wired and wireless clients to have addresses. Having clients that could be either will increase the number of required addresses.

3. What is the simplest subnet class to use when planning an IP addressing scheme for each of the North America branch locations?

**Answer:** The starting point for each location would be to use /24 subnets.

4. In the Houston office, what is the number of potential wired and wireless clients?

**Answer:** 400 potential wired clients (300 desktops and 100 laptops) and 150 potential wireless clients (100 laptops and 50 tablets).

5. In the Houston office, how many /24 subnets are required for wired connections? How many are required for wireless?

**Answer:** Two /24 subnets would be the minimum required for wired connections (each /24 supports a maximum of 253 clients + 1 gateway). One /24 subnet would suffice for the potential wireless clients.

6. In the Mexico City office, what is the number of potential wired and wireless clients?

**Answer:** 150 potential wired connections (100 desktops and 50 laptops) and 70 potential wireless connections (70 laptops and 20 tablets).

7. In the Mexico City office, how many /24 subnets are required for wired connections? How many for wireless?

**Answer:** One /24 subnet for the potential wired connections and one /24 subnet for the potential wireless connections.

8. In the Portland office, what is the number of potential wired and wireless clients?

**Answer:** 175 potential wired connections (100 desktops and 75 laptops) and 225 potential wireless connections (75 laptops and 150 tablets).

9. In the Portland office, how many /24 subnets are required for wired connections? How many for wireless?

**Answer:** One /24 subnet for the potential wired connections and one /24 subnet for the potential wireless connections.

10. Given the assigned IP range of 172.16.20.0/24 – 172.16.52.0/24 for wired clients, which subnets will you use for the Houston, Mexico City, and Portland offices?

**Answer:** Answers will vary. One possible option is:

Houston: 172.16.30.0/24

172.16.31.0/24

Mexico City: 172.16.35.0/24

Portland: 172.16.40.0/24

11. Given the assigned IP range of 172.16.53.0/24 – 172.16.60.0/24 for wireless clients, which subnets will you use for the Houston, Mexico City, and Portland offices?

**Answer:** Answers will vary. One possible option is:

Houston: 172.16.55.0/24

Mexico City: 172.16.56.0/24

Portland: 172.16.57.0/24

**Results:** You will have planned an IPv4 network.



# Lab B: Implementing and troubleshooting an IPv4 network

## Exercise 1: Verify IPv4 communication

### ► Task 1: Verify IPv4 traffic

#### Verify that the LON-DC1 server can communicate with the default gateway

1. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**, type the following command, and then press Enter.

```
Test-NetConnection 172.16.0.1
```

2. Review the results.

#### Verify that LON-DC1 can communicate with TOR-SVR1

1. On **LON-DC1**, in the Windows PowerShell window, type the following command, and then press Enter.

```
Test-NetConnection -TraceRoute TOR-SVR1.adatum.com
```

2. Review the results.

### ► Task 2: Prepare LON-CL1 for troubleshooting

1. On **LON-CL1**, open a **File Explorer** window, and then browse to **\\LON-DC1\Labfiles\Mod01**.
2. Copy **LON-CL1.ps1** from **\\LON-DC1\Labfiles\Mod01** to the **LON-CL1** desktop.



**Note:** Do not open the file. This script creates the problem that you will troubleshoot and repair in the next exercise. Opening the file can cause issues with the lab tasks.

3. Close **File Explorer**.
4. Right-click the **LON-CL1.ps1** file, and then click **Run with PowerShell**.
5. If prompted to confirm, type **y**, and then press Enter.

### ► Task 3: Prepare LON-CL2 for troubleshooting

1. On **LON-CL2**, open a **File Explorer** window, and then browse to **\\LON-DC1\Labfiles\Mod01**.
2. Copy **LON-CL2.ps1** from **\\LON-DC1\Labfiles\Mod01** to the **LON-CL2** desktop.



**Note:** Do not open the file. This script creates the problem that you will troubleshoot and repair in the next exercise. Opening the file can cause issues with the lab tasks.

3. Close **File Explorer**.
4. Right-click the **LON-CL2.ps1** file, and then click **Run with PowerShell**.
5. If prompted to confirm, type **y**, and then press Enter.

**Results:** After completing this exercise, you will have verified that the London computers can communicate with the Toronto server.

## Exercise 2: Troubleshooting IPv4

### ► Task 1: Troubleshoot IPv4 connectivity between the London clients and the Toronto server

#### Troubleshooting LON-CL1

1. On **LON-CL1**, click **start**, type **PowerShell** and then click **Windows PowerShell**. At the Windows PowerShell prompt, type the following, and then press Enter:

```
Test-NetConnection LON-DC1
```

2. Verify that the results contain **PingSucceeded:False** from **LON-DC1**.
3. Verify the **LON-CL1 IP** address, and at the Windows PowerShell prompt, type the following, and then press Enter:

```
Get-NetIPAddress
```

Notice that the IPv4 address is 169.254.x.x. This indicates that the client is configured for DHCP and has not received an address.

4. Configure the **LON-CL1 IP** address, and at the Windows PowerShell prompt, type the following, and then press Enter:

```
New-NetIPAddress -InterfaceAlias "London_Network" -IPAddress 172.16.0.50 -  
PrefixLength 24
```

5. Verify the communications have been fixed, and at the Windows PowerShell prompt, type the following, and then press Enter:

```
Test-NetConnection TOR-SVR1
```

6. Confirm that the **TOR-SVR1** server is reachable by verifying that you receive a reply from **172.16.18.20** that contains **PingSucceeded:True**.

#### Troubleshooting LON-CL2

1. On **LON-CL2**, open a Windows PowerShell prompt, type the following, and then press Enter:

```
Test-NetConnection LON-DC1
```

2. Confirm that the **LON-DC1** server is reachable by verifying that you receive a reply from **172.16.0.10** that contains **PingSucceeded:True**.
3. At the Windows PowerShell prompt, type the following, and then press Enter:

```
Test-NetConnection TOR-SVR1
```

4. Verify that the results contain **PingSucceeded:False** from **TOR-SVR1**. Also note the yellow message, "WARNING: Ping to TOR-SVR1 failed – Status: DestinationHostUnreachable."

5. Verify the Router is accessible, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Test-NetConnection 172.16.0.1
```

6. Confirm that the router is reachable by verifying that you receive a reply from **172.16.0.1** that contains **PingSucceeded:True**.
7. Verify the traffic is being routed correctly, at the Windows PowerShell prompt, type the following, and then press Enter:

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

8. Notice that none of the TraceRoute packets left the 172.16.0.51 interface.
9. Verify the IP Configuration, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-NetIpConfiguration
```

10. Notice the IPv4DefaultGateway is set incorrectly to 172.16.0.2.
11. Fix the IPv4DefaultGateway by running the following commands:

```
Remove-NetIPAddress -InterfaceAlias " London_Network " -IPAddress 172.16.0.51 -  
PrefixLength 24 -DefaultGateway 172.16.0.2 -Confirm:$false  
New-NetIPAddress -InterfaceAlias " London_Network " -IPAddress 172.16.0.51 -  
PrefixLength 24 -DefaultGateway 172.16.0.1 -Confirm:$false
```

12. Verify the communications have been fixed, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Test-NetConnection TOR-SVR1
```

13. Confirm that the **TOR-SVR1** server is reachable by verifying that you receive a reply from **172.16.18.20** that contains **PingSucceeded:True**.

**Results:** After completing this lab, you should have resolved all IPv4 connectivity issues.

### ► Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-CL1**, **20741A-LON-CL2**, **20741A-EU-RTR**, and **20741A-TOR-SVR1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 2: Implementing DHCP

# Lab: Implementing DHCP

### Exercise 1: Planning the DHCP server implementation

#### ► Task 1: Plan the Dynamic Host Configuration Protocol (DHCP) server implementation

Based on your answers to the following questions, you will develop a plan for implementing the DHCP server infrastructure.

1. What scopes do you need to create to enable the IP addressing scheme from module 1?

**Answer:** Subnet assignments will vary, but possibilities are:

- Houston: Has 400 potential wired connections and 150 potential wireless connections. Houston will need two /24 subnets supernetted for the wired connections, and one /24 subnet for the wireless connections.

Houston will use 172.16.30.0/24 and 172.16.31.0/24 supernetted for wired connections, and 172.16.55.0/24 for wireless connections.

- Mexico City: Has 150 potential wired connections and 70 potential wireless connections. Mexico City will use 172.16.35.0/24 for wired connections, and 172.16.56.0/24 for wireless connections.
- Portland: Has 175 potential wired connections and 225 potential wireless connections. Portland will use 172.16.40.0/24 for wired connections, and 172.16.57.0/24 for wireless connections.

Wireless scopes will have a short duration of 1 day, and wired scopes will have a duration of 8 days.

2. Where will DNS service come from?

**Answer:** LON-DC1 will be the Domain Name System (DNS) server for all scopes.

3. How will you get DHCP messages from TOR-SVR1 to the clients in the Houston, Mexico City, and Portland locations?

**Answer:** You will configure DHCP relay agents in the branches.

4. What configuration changes do you need to make to NA-RTR to enable the IP addressing scheme through the DHCP relay?

**Answer:** You will need to assign the interfaces IP addresses from their respective branch subnets and configured as DHCP relay agents.

5. How will you assign different IP ranges to the clients in each location? How will you assign different IP addresses for wired and wireless clients?

**Answer:** You will create multiple scopes on the DHCP server. You will need a separate scope for each wired and wireless network.

To distinguish between wired and wireless requests you will configure the router as a DHCP relay agent for the wired connections, and configure the wireless access points as relay agents for wireless requests.

6. What IP addresses will you assign to the network interfaces on NA-RTR that are connected to the Houston, Mexico City, and Portland networks?

**Answer:** You will assign the Houston interface 172.16.30.1. You will assign the Mexico City interface 172.16.35.1. You will assign the Portland interface 172.16.40.1

7. How will you provide for DHCP Failover for **TOR-SVR1**?

**Answer:** You will configure a failover relationship with **LON-SVR1** as a hot standby DHCP server.

**Results:** At the completion of this exercise you should have planned the DHCP implementation.

## Exercise 2: Implementing the DHCP configuration

### ► Task 1: Install and configure the DHCP server role on TOR-SVR1

#### Install the DHCP server role

1. On **TOR-SVR1**, click **Start**, and then click the **Server Manager** tile.
2. On the **Server Manager** dashboard, 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, select **DHCP Server**.
7. In the **Add Roles and Features Wizard**, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.



**Note:** The installation will take a few minutes to complete.

11. After the installation succeeds, click **Close**.

#### Perform the post-installation tasks

1. On the top menu bar, click the (orange triangle) **Notifications** icon, 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 Microsoft Management Console (MMC)**.

## ► Task 2: Configure DHCP scopes for Houston, Mexico City, and Portland

### Create the Houston scopes

1. On **TOR-SVR1**, in **Server Manager**, click **Tools**, and then click **DHCP**.
2. In the left pane, click to select **TOR-SVR1.adatum.com**. This will open the **IPv4** node.
3. Click to select the **IPv4** node.
4. In the **Actions** pane, click **More Actions**, and then click **New Scope**.
5. In the **New Scope Wizard**, click **Next**.
6. On the **Scope Name** page, in the **Name** text box, type **Houston-wired1**, and then click **Next**.
7. On the **IP Address Range** page, in the **Start IP address** text box, type **172.16.30.2**, and in the **End IP address** text box, type **172.16.30.254**.



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

8. Change the value of the subnet mask to **255.255.255.0**, and then click **Next**.
9. On the **Add Exclusions and Delay** page, click **Next**.
10. On the **Lease Duration** page, click **Next**.
11. On the **Configure DHCP Options** page, click **Next**.
12. On the **Router (Default Gateway)** page, in the **IP address** text box, type **172.16.30.1**, click **Add**, and then click **Next**.
13. On the **Domain Name and DNS Servers** page, click **Next**.
14. On the **WINS Servers** page, click **Next**.
15. On the **Activate Scope** page, click **Next**, and then click **Finish**.
16. Repeat steps 4–15 to create a second scope with the following settings:
  - Name: **Houston –wired2**
  - Start IP address: **172.16.31.1**
  - End IP address: **172.16.31.254**
17. Repeat steps 4–15 to create a third scope with the following settings:
  - Name: **Houston-wireless**
  - Start IP address: **172.16.55.2**
  - End IP address: **172.16.55.254**
  - Lease duration: **1 day**
  - Router (Default Gateway): **172.16.55.1**

### Create a superscope for Houston wired scopes

1. Right-click the **IPv4** node, and then click **New Superscope**.
2. In the **New Superscope Wizard**, click **Next**.
3. On the **Superscope Name** page, in the **Name** text box, type **Houston-wired**, and then click **Next**.

4. On the **Select Scopes** page, press and hold the Ctrl key, click to select **[172.16.30.0] Houston-wired1** and **[172.16.31.0] Houston-wired2**, and then click **Next**.
5. On the **Completing the New Superscope Wizard** page, click **Finish**.

### Create the Mexico City scopes

1. Click to select the **IPv4** node.
2. In the **Actions** pane, click **More Actions**, and then click **New Scope**.
3. In the **New Scope Wizard**, click **Next**.
4. On the **Scope Name** page, in the **Name** text box, type **MexicoCity-wired**, and then click **Next**.
5. On the **IP Address Range** page, in the **Start IP address** text box, type **172.16.35.2**, and then in the **End IP address** text box type, **172.16.35.254**.
6. Change the value of the subnet mask to **255.255.255.0**, and then click **Next**.
7. On the **Add Exclusions and Delay** page, click **Next**.
8. On the **Lease Duration** page, click **Next**.
9. On the **Configure DHCP Options** page, click **Next**.
10. On the **Router (Default Gateway)** page, in the **IP address** text box, type **172.16.35.1**, click **Add**, and then click **Next**.
11. On the **Domain Name and DNS Servers** page, click **Next**.
12. On the **WINS Servers** page, click **Next**.
13. On the **Activate Scope** page, click **Next**, and then click **Finish**.
14. Repeat steps 1–13 to create a scope with the following parameters:
  - o Name: **MexicoCity-wireless**
  - o Start IP address: **172.16.56.2**
  - o End IP address: **172.16.56.254**
  - o Lease duration: **1 day**
  - o Router (Default Gateway): **172.16.56.1**

### Create the Portland scopes

1. Click to select the **IPv4** node.
2. In the **Actions** pane, click **More Actions**, and then click **New Scope**.
3. In the **New Scope Wizard**, click **Next**.
4. On the **Scope Name** page, in the **Name** text box, type **Portland-wired**, and then click **Next**.
5. On the **IP Address Range** page, in the **Start IP address** text box, type **172.16.40.2**, and then in the **End IP address** text box, type **172.16.40.254**.
6. Change the value of the subnet mask to **255.255.255.0**, and then click **Next**.
7. On the **Add Exclusions and Delay** page, click **Next**.
8. On the **Lease Duration** page, click **Next**.
9. On the **Configure DHCP Options** page, click **Next**.



10. On the **Router (Default Gateway)** page, in the **IP address** text box, type **172.16.40.1**, click **Add**, and then click **Next**.
11. On the **Domain Name and DNS Servers** page, click **Next**.
12. On the **WINS Servers** page, click **Next**.
13. On the **Activate Scope** page, click **Next**, and then click **Finish**.
14. Repeat steps 1–13 to create a scope with the following parameters:
  - o Name: **Portland-wireless**
  - o Start IP address: **172.16.57.2**
  - o End IP address: **172.16.57.254**
  - o Lease duration: **1 day**
  - o Router (Default Gateway): **172.16.57.1**

► **Task 3: Configure network adapters on NA-RTR**

1. Switch to **NA-RTR**.
2. Right-click **Start**, and then click **Network Connections**.
3. Right-click the **HOU\_WAN** adapter, and then click **Properties**.
4. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Use the following IP address**.
6. In the **IP address** text box, type **172.16.30.1**, in the **Subnet mask** text box, type **255.255.255.0**, and then click **OK**.
7. Click **Close**.
8. Right-click the **MEX\_WAN** adapter, and then click **Properties**.
9. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
10. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Use the following IP address**.
11. In the **IP address** text box, type **172.16.35.1**, in the **Subnet mask** text box, type **255.255.255.0**.
12. Click **OK**, and then click **Close**.
13. Right-click the **POR\_WAN** adapter, and then click **Properties**.
14. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
15. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Use the following IP address**.
16. In the **IP address** text box, type **172.16.40.1**, in the **Subnet mask** text box, type **255.255.255.0**.
17. Click **OK**, and then click **Close**.

► **Task 4: Install the DHCP server role on LON-SVR1**

**Install the DHCP server role**

1. On **LON-SVR1**, click **Start**, and then click the **Server Manager** tile.
2. On the **Server Manager** dashboard, 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, select **DHCP Server**.
7. In the **Add Roles and Features Wizard**, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.



**Note:** The installation will take a few minutes to complete.

11. After the installation succeeds, click **Close**.

### Perform the post-installation tasks

1. On the top menu bar, click the (orange triangle) **Notifications** icon, 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 MMC**.

### ► Task 5: Configure DHCP failover between TOR-SVR1 and LON-SVR1

1. Switch to **TOR-SVR1**.
2. In the DHCP management console, right-click the **IPv4** node, and then click **Configure Failover**.
3. On the **Introduction to DHCP Failover** page, ensure that all scopes are selected, and then click **Next**.
4. On the **Specify the partner server to use for failover** page, click **Add Server**. In the **This server** text box, type **172.16.0.11**, click **OK**, and then click **Next**.
5. On the **Create a new failover relationship** page, click the **Mode** drop-down list box, click **Hot standby**, and then set the **Maximum Client Lead Time** to **1** minute.



**Note:** This low value is for the purposes of the lab.

6. In the **Shared Secret** text box, type **Pa\$\$w0rd**, click **Next**, and then click **Finish**.
7. In the **Configure Failover** message box, click **Close**.
8. Switch to **LON-SVR1**. In **Server Manager**, click **Tools**, and then click **DHCP**.
9. In the **DHCP** management console, expand the **IPv4** node, and then note that all of the scopes now display.

► **Task 6: Configure DHCP relay on NA-RTR for Houston, Mexico City, and Portland**

1. On **NA-RTR**, click **Start**, and then click the **Server Manager** tile.
2. In **Server Manager**, click **Tools**, and then click **Routing and Remote Access**.
3. Expand **NA-RTR**, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.
4. In the **New Routing Protocol** dialog box, select **DHCP Relay Agent**, and then click **OK**.
5. Right-click **DHCP Relay Agent**, and then click **Properties**.
6. In the **DHCP Relay Agent Properties** dialog box, in the **Server address** box, type **172.16.18.20**, and then click **Add**. Then type **172.16.0.11**, in the **Server address** box and then click **Add** and then click **OK**.
7. Right-click **DHCP Relay Agent**, and then click **New Interface**.
8. In the **New Interface for DHCP Relay Agent**, dialog box, click **HOU\_WAN**, and then click **OK**.
9. In the **DHCP Relay Properties – HOU\_WAN Properties** dialog box, click **OK**.
10. Repeat steps 7-9 for both **MEX\_WAN** and **POR\_WAN**.


**Results:** After completing this exercise, you should have you should have implemented your plan for the DHCP configuration.

### Exercise 3: Validating the DHCP implementation

► **Task 1: Test DHCP allocation to the correct subnets**


1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **Network Connections**.
3. Right-click the **London\_Network** adapter, and then click **Properties**.
4. In the **London\_Network Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Obtain an IP address automatically**, click **OK**, and then click **Close**.
6. On the virtual machine menu bar, click the **File** menu, and then click **Settings**.
7. In the left pane, click the **Network Adapter** connected to **London\_Network**.
8. In the right pane, click the **Virtual switch** drop-down list box, click **HOU\_WAN**, and then click **OK**.
9. Right-click **Start**, and then click **Command Prompt**.
10. In the **Administrator: Command Prompt** window, type the following command, and then press Enter:

```
Ipconfig /All
```

 **Note:** Note that the IP address will be 172.16.30.2. The IP address of the DHCP server will be 172.16.18.20.


11. On the virtual machine menu bar, click the **File** menu, and then click **Settings**.
12. In the left pane, click the **Network Adapter** connected to **HOU\_WAN**.
13. In the right pane, click the **Virtual switch** drop-down list box, click **MEX\_WAN**, and then click **OK**. Wait a few seconds for the change to take effect.
14. In the **Administrator: Command Prompt** window, type the following command, and then press Enter.

```
Ipconfig /All
```

 **Note:** Note that the IP address will be 172.16.35.2. The IP address of the DHCP server will be 172.16.18.20.

15. On the virtual machine menu bar, click the **File** menu, and then click **Settings**.
16. In the left pane, click the **Network Adapter** connected to **MEX\_WAN**.
17. In the right pane, click the **Virtual switch** drop-down list box, click **POR\_WAN**, and then click **OK**. Wait a few seconds for the change to take effect.
18. In the **Administrator: Command Prompt** window, type the following command, and then press Enter.

```
Ipconfig /All
```

 **Note:** Note that the IP address will be 172.16.40.2. The IP address of the DHCP server will be 172.16.18.20.

### ► Task 2: Test DHCP failover

1. Switch to **TOR-SVR1**.
2. In **Server Manager**, click **Tools**, and click **Services**.
3. Click the **DHCP Server** service, and then click **Stop**.
4. Switch to **LON-CL1**.
5. In the **Command Prompt** window, type **ipconfig /release**, and then press Enter.
6. In the **Command Prompt** window, type **ipconfig /renew**, and then press Enter.
7. Type **ipconfig /All** and press Enter

 **Note:** Note that the IP DHCP server will now be 172.16.0.11.

**Results:** After completing this exercise, you should have tested DHCP IP address allocation to the correct subnets, and tested DHCP failover.

► **Task 3: Prepare for the next module**

When you finish the lab, revert all the virtual machines to their initial state by performing the following steps:

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

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 3: Implementing IPv6

# Lab: Configuring and evaluating IPv6 transition technologies

### Exercise 1: Reviewing the default IPv6 configuration

#### ► Task 1: Identify the default IPv6 configuration

1. On **LON-DC1**, in **Server Manager**, on the menu in the upper-right corner, click **Tools**, and then click **DNS**.
2. In the DNS console tree, expand **DNS\LON-DC1\Forward Lookup Zones**, and then click **Adatum.com**.

Notice that **LON-DC1** has one IPv6 address preconfigured for the lab. Notice that there are no AAAA records registered for any other computer.

3. On **LON-DC1**, click **Start**, and then click **Windows PowerShell**.
4. At the Windows PowerShell command prompt, type **ipconfig**, and then press Enter.

Notice that this command returns a link-local IPv6 address. Note this address.

5. Type **Get-NetIPAddress**, and then press Enter. Notice that this command also returns a link-local IPv6 address.
6. Repeat steps 3 to 5 on **LON-SVR1** and **TOR-SVR1**.



**Note:** Windows client and server operating systems do not register link-local IPv6 addresses in DNS.

#### ► Task 2: Test link-local address connectivity

1. Switch to **LON-DC1**.
2. At the Windows PowerShell command prompt, type **ping**, followed by the **LON-SVR1** link-local IPv6 address, and then press Enter.



**Note:** The **LON-SVR1** link-local IPv6 address was displayed in step 5 of the previous task. When typing the IPv6 address, do not type the percent sign (%) and do not type the numbers after the %.

Four successful replies should be displayed.

3. At the Windows PowerShell command prompt, type the **Test-NetConnection** cmdlet followed by the **LON-SVR1** link-local IPv6 address, and then press Enter.



**Note:** The **LON-SVR1** link-local IPv6 address was displayed in step 5 of the previous task. When typing the IPv6 address, do not type the percentage symbol (%) and do not type the numbers after the %.

**Ping Succeeded: True** from the **LON-SVR1** link-local IPv6 address should be displayed. The **Test-NetConnection** cmdlet performs diagnostics for a network connection and displays the results. The results also include a diagnostic message to notify you of whether the **ping** command was successful.

4. At the Windows PowerShell command prompt, type the **Test-NetConnection** cmdlet followed by the **TOR-SVR1** link-local IPv6 address.



**Note:** The **TOR-SVR1** link-local IPv6 address was displayed in the previous task. When typing the IPv6 address, do not type the percentage sign (%) and do not type the numbers after the %.

5. The following should be displayed: The warning message "DestinationHostUnreachable," and the result of the diagnostics that displays the message "Ping Succeeded: False." This is because the link-local IPv6 addresses are not routable and can be used for communication only on local subnet.

**Results:** After completing the exercise, you should have reviewed the default IPv6 configuration and test how computers communicate by using link-local IPv6 addresses.

## Exercise 2: Implementing DHCPv6

### ► Task 1: Create and configure DHCPv6 scopes

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** text box, type **Headquarters IPv6**, and then click **Next**.
5. On the **Scope Prefix** page, in the **Prefix** text 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**.

### ► Task 2: Verify configuration by testing allocation of IPv6 addresses

1. Switch to **LON-CL1**.
2. On the **Start** screen, type **PowerShell**, and then press Enter.
3. In the **Windows PowerShell** window, type the **Ipconfig /renew6** command, and then press Enter.
4. Verify that the IPv6 address is in the IP range **FD00:0000:0000:0000::/64**.



**Results:** After completing the exercise, you should have configured DHCP to assign IPv6 addresses, and verified that the addresses are assigned correctly.

### Exercise 3: Configuring network integration by using ISATAP

#### ► Task 1: Configure an ISATAP router

1. On **LON-DC1**, in the **Windows PowerShell** window, type the following command, and then press Enter.

```
dnscmd /config /globalqueryblocklist wpad
```

This step removes the name **ISATAP** from the default global query block list.

2. In the **DNS** console tree, right-click **LON-DC1**, point to **All Tasks**, and then click **Restart**.
3. In the **DNS** console tree, expand **DNS\LON-DC1**, and then click to expand **Forward Lookup Zones**.
4. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
5. In the **New Host** dialog box, in the **Name** box, type **isatap**; in the **IP address** box, type **172.16.0.1**; click **Add Host**; click **OK**, and then click **Done**.
6. Switch to **EU-RTR**.
7. From the **Start** menu, click **Windows PowerShell**.
8. In the **Windows PowerShell** window, type the following command, and then press Enter to configure the IP address of London\_Network as the ISATAP router:

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

9. Type the following command, and then press Enter:

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address
```

10. Record the **InterfaceIndex** of the ISATAP interface that has an IPv6 address that includes 172.16.0.1.

Record the interface index here:



**Note:** As an optional step, you might consider modifying the preceding cmdlet so that the output of the cmdlet will be stored in a text file. This will make it easier for you to search for the InterfaceIndex value.

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address > C:\Results.txt
```

This cmdlet will create the **Results.txt** file on drive C of **EU-RTR**. The file contains the results from running the cmdlet. Search the **Results.txt** file for the interface that has an IPv6 address, which includes 172.16.0.1.

11. Type the following command, and then press Enter.

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore | Format-List
```

12. Verify that forwarding is enabled for the interface and that advertising is disabled.
13. The ISATAP interface for an ISATAP router must have forwarding enabled and advertising enabled. Type the following command, and then press Enter.

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

14. Create a new IPv6 network that will be used for the ISATAP network. Type the following command, and then press Enter.

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64 -Publish Yes
```

15. View the IP address configuration for the ISATAP interface. Type the following command, and then press Enter.

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

16. Verify that an IPv6 address is listed on the 2001:db8:0:2::/64 network, and then close the **Windows PowerShell** window.

### ► Task 2: Verify the ISATAP configuration on the client

1. Restart **TOR-SVR1** and **LON-SVR1**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On **TOR-SVR1**, from the **Start** menu, click **Windows PowerShell**.
3. In the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Verify that the Tunnel adapter has received an IPv6 address starting with 2001.
4. On **LON-SVR1**, from the **Start** menu, click **Windows PowerShell**.
5. In the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Verify that the Tunnel adapter has received an IPv6 address starting with 2001.
6. On **LON-DC1**, switch to the DNS management console.
7. In the **DNS** management console tree, expand **DNS\LON-DC1**, then expand **Forward Lookup Zones**.
8. Click **Adatum.com**, and then click **Refresh** button to verify that there are new AAAA records registered.

### ► Task 3: Verify network connectivity to other subnets

- On **TOR-SVR1**, open the Windows PowerShell command prompt, and then verify the connection with the **LON-SVR1** tunnel ISATAP adapter's IPv6 address by typing the following cmdlet and pressing Enter:

```
Test-NetConnection 2001:db8:0:2:0:5efe:172.16.0.11
```

Notice that the message "Ping Succeeded: True" is received from **LON-SVR1** tunnel ISATAP adapter's IPv6 address.

**Results:** After completing this exercise, you should have configured an ISATAP router to allow communication between an IPv6-only network and an IPv4-only network.

## Exercise 4: Configuring native IPv6 connectivity

### ► Task 1: Configure native IPv6 connectivity

Before configuring native IPv6 connectivity, you have to perform steps 1 to 12 to remove the ISATAP that you configured in the previous exercise. This is because ISATAP is not required in the native IPv6 environment.

1. On **EU-RTR**, click **Start** and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter. In the cmdlet, replace **IndexYouRecorded** with the value you recorded in Exercise 3, Task 1, Step 10.

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Disabled
```

3. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
Remove-NetRoute -InterfaceIndex IndexYouRecorded -Publish Yes
```

4. Type **Y**, and then press Enter each time when asked.
5. On **LON-DC1**, in the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones** \Adatum.com, right-click **isatap**, click **Delete**, and then in the **DNS** dialog box, click **Yes**.
6. Open the **Windows PowerShell** window, and restart the **IP Helper** service by typing the following cmdlet, and then press Enter.

```
Restart-Service iphlpsvc
```

7. Switch to **EU-RTR**.
8. Repeat step 5 on **EU-RTR**.
9. Switch to **TOR-SVR1**.
10. Repeat step 5 on **TOR-SVR1**.
11. Switch to **LON-SVR1**.
12. Repeat step 5 on **LON-SVR1**.
13. Switch to **LON-DC1**.
14. In the **DNS** console tree, expand **DNS\LON-DC1\Forward Lookup Zones**, right-click **adatum.com**, and then click **Refresh** to verify that no AAAA records are registered. If there are still AAAA records registered, repeat steps 4 through 12.

In the following steps, you will configure **EU-RTR** as an advertising and forwarding IPv6 router that advertises native IPv6 prefixes to the London and Toronto subnets.

1. On **EU-RTR**, click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
Set-NetIPInterface -AddressFamily ipv6 -InterfaceAlias "London_Network" -Advertising enabled -AdvertiseDefaultRoute enabled
```

3. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
Set-NetIPInterface -AddressFamily ipv6 -InterfaceAlias "NA_WAN" -Advertising enabled -AdvertiseDefaultRoute enabled
```

- In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
New-NetRoute -InterfaceAlias "London_Network" -DestinationPrefix 2001:db8::/64 -Publish Yes
```

- In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
New-NetRoute -InterfaceAlias "NA_WAN" -DestinationPrefix 2001:db8:0:2::/64 -Publish Yes
```

- In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.

```
Get-NetIPAddress
```

- In the **Windows PowerShell** window, document the link-local IPv6 address of "**London\_Network**" adapter. This IPv6 address will be used in the next step.
- In the **Windows PowerShell** window, type the following command, and then press Enter. When typing the command, replace **link-local address of EU-RTR "London\_Network" interface** with the IPv6 address you documented in previous step. When typing the IPv6 address, do not type the percent sign (%) and do not type the numbers after the %.

```
New-NetRoute -InterfaceAlias "London_Network" -DestinationPrefix ::/0 -NextHop link-local address of EU-RTR "London_Network" interface -Publish yes
```

### ► Task 2: Verify the native IPv6 configuration

- Switch to **EU-RTR**.
- In the **Windows PowerShell** window, type the following, and then press Enter.

```
Get-NetIPAddress
```

- Notice the new IPv6 address starting with **2001:db8::** assigned to the **London\_Network** interface, and the address starting with **2001:db8:0:2** assigned to the **NA\_Network** interface. Notice the link-local address of the **London\_Network** interface.
- Switch to **LON-SVR1**.
- On **LON-SVR1**, in the **Windows PowerShell** window, type the following, and then press Enter.

```
Get-NetIPAddress
```

- Notice the new IPv6 address starting with **2001:db8::** and the default gateway of **EU-RTR** link-local address.
- Switch to **LON-DC1**.
- In the **DNS** console tree, expand **DNS\LON-DC1**, and then expand **Forward Lookup Zones**.
- Right-click **Adatum.com**, and then click **Refresh** to verify that there are new AAAA records registered.

### ► Task 3: Verify network connectivity to other subnets

- On **TOR-SVR1**, open **Windows PowerShell**.
- In the **Windows PowerShell** window, type **ipconfig /flushdns**, and then press Enter.

3. In the **Windows PowerShell** window, type **Test-NetConnection LON-DC1**, and then press Enter. The successful name resolution to the **LON-DC1** IPv6 address and the **PingSucceeded:True** reply is displayed.
4. On the Start screen, click **Start**, click **All Apps**, click **Windows Accessories**, and then click **Internet Explorer**.
5. In the address bar, type **http://LON-SVR1.adatum.com**, and then press Enter. You should see the default Microsoft Internet Information Services (IIS) webpage for **LON-SVR1**.
6. Switch to **LON-SVR1**.
7. On **LON-SVR1**, in the **Windows PowerShell** window, type **ipconfig /flushdns**, and then press Enter.
8. In the **Windows PowerShell** window, type **Test-NetConnection EU-RTR**, and then press Enter. A successful name resolution to the **EU-RTR** IPv6 address and the "PingSucceeded:True" reply is displayed.
9. In the Windows PowerShell window, type **Test-NetConnection TOR-SVR1.adatum.com**, and then press Enter. A successful name resolution to the **TOR-SVR1** IPv6 address and the "PingSucceeded:True" reply is displayed. Notice that **LON-SVR1** is using the **TOR-SVR1** IPv6 address, rather than the IPv4 address.

**Results:** After completing this exercise, you should have configured native IPv6 connectivity and tested whether the computers can communicate by using IPv6 addresses.

## Exercise 5: Configuring 6to4 Connectivity

### ► Task 1: Configure 6to4 connectivity

1. On **EU-RTR**, on the taskbar, click the **Windows PowerShell** icon.
2. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.
 

```
Set-Net6to4Configuration -State enabled
```
3. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.
 

```
Set-NetIPInterface -InterfaceAlias "6to4 Adapter" -Forwarding enabled
```
4. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter.
 

```
Set-NetIPInterface -InterfaceAlias "London_Network" -Forwarding enabled
```
5. Switch to **INET1**, and then start **Server Manager**.
6. In **Server Manager**, in the menu on the upper-right corner, click **Tools**, and then click **DNS**.
7. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
8. On the **Zone Type** page, click **Next**.
9. On the **Zone Name** page, in the **Zone name** box, type **ipv6.microsoft.com**, and then click **Next**.
10. On the **Zone File** page, click **Next**.

11. On the **Dynamic Update** page, click **Do not allow dynamic updates**, click **Next**, and then click **Finish**.
12. In the DNS console, in the console tree, click and then right-click the **ipv6.microsoft.com** zone, and then click **New Host (A or AAAA)**.
13. In the **New Host** dialog box, in the **Name** box, type **6to4**; in the **IP address** box, type **131.107.0.10**; click **Add Host**; click **OK**; and then click **Done**.

► **Task 2: Verify 6to4 configuration**

1. On **EU-RTR**, in the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Notice the **2002:836b:a::836b:a** IPv6 address assigned to the **6TO4 Adapter**.

This is a 6to4 address that **EU-RTR** automatically assigns based on the public IPv4 address **131.107.0.10**, which is assigned to the **Internet** interface.



**Note:** Note the IPv6 address of the **6to4** adapter where, **836b:a** in the hexadecimal system corresponds to **131.107.0.10**. That is:

**83** hexadecimal = **131** decimal

**6b** hexadecimal = **107** decimal

**0** hexadecimal = **0** decimal (preceding zero is skipped)

**a** hexadecimal = **10** decimal

2. Switch to **LON-CL1**.
3. To move the client from the intranet to the public network, on **LON-CL1**, to open **Control Panel**, at the **Windows PowerShell** command window, type **control**, and then press Enter.
4. In Control Panel, click **Network and Internet**, and then click **Network and Sharing Center**.
5. In the **Network and Sharing Center** window, click **Change adapter settings**.
6. Right-click **London\_Network**, and then click **Disable**.
7. Right-click **Internet**, and then click **Enable**.
8. Close the **Network Connections** window. In the **Networks** pane, click **Yes**.
9. On **LON-CL1**, in the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Notice the address starting with **2002:836b:** assigned to the **6TO4 Adapter**. This is a 6to4 address corresponding to its public IPv4 address. Also notice that the default gateway for the **6TO4 Adapter** is set to **2002:836b:a::836b:a**, a 6to4 address assigned to **EU-RTR**.
10. On **EU-RTR**, in the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Notice and document the address starting with **2001:db8::** assigned to the **London\_Network** interface, because it will be used in the next task.
11. On **LON-DC1**, in the **Windows PowerShell** window, type **Get-NetIPAddress**, and then press Enter. Notice and document the address starting with **2001:db8::** assigned to the **Ethernet** interface, because it will be used in the next task.

### ► Task 3: Verify network connectivity to other subnets

1. Switch to **LON-CL1**.
2. In the **Windows PowerShell** window, type the following command, and then press Enter to test communication.

```
Test-NetConnection EU-RTR IPv6 address
```



**Note:** Use the IPv6 address for **EU-RTR** on the London\_Network adapter you documented in the previous task.

3. A message "Ping Succeeded: True" should be displayed in the reply.
4. In the **Windows PowerShell** window, type the following command, and then press Enter to test communication.

```
Test-NetConnection LON-DC1 IPv6 address
```



**Note:** Use the IPv6 address for **LON-DC1** on the Ethernet adapter you documented in the previous task.

5. A message "Ping Succeeded: True" should be displayed in the reply.

**Results:** After completing this exercise, you should have configured 6to4 transition technology and verified the connectivity when using the 6to4 transition technology.

### ► Task 4: Prepare for the next module

After you finish the lab, revert the virtual machines back to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-EU-RTR**, **20741A-LON-SVR1**, **20741A-LON-CL1**, **20741A-TOR-SVR1**, and **20741A-INET1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**



## Module 4: Implementing DNS

# Lab A: Planning and implementing name resolution by using DNS

### Exercise 1: Planning DNS name resolution

#### ► Task 1: Plan the DNS infrastructure to support name resolution

Read the scenario and answer the following:

1. What is the first step in implementing your new DNS plan for the Sydney office?  
**Answer:** Install the DNS Server role on **SYD-SVR1**.
2. How will you configure **SYD-SVR1** to resolve DNS queries for Internet-based addresses?  
**Answer:** Set forwarding to INET (131.107.0.100).
3. How will you configure **SYD-SVR1** to resolve DNS queries for the internal web server?  
**Answer:** Set conditional forwarding for Contoso.com to **LON-SVR1**.
4. How will you configure **SYD-SVR1** to resolve queries for the Treyresearch.net DNS namespace?  
**Answer:** Create a Secondary zone for TreyResearch.net on **SYD-SVR1**.
5. How will you configure **SYD-SVR1** to resolve queries for the Adatum.com domain?  
**Answer:** Set conditional forwarding for Adatum.com to **LON-DC1**.

**Results:** After completing this exercise, you should have created a plan for implementing DNS name resolution successfully.

### Exercise 2: Implementing DNS servers and zones

#### ► Task 1: Install the DNS server role

1. On **SYD-SVR1**, click **Start** and then click **Server Manager**.
2. In **Server Manager**, 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, ensure that **SYD-SVR1.Adatum.com** is selected, and then click **Next**.
6. On the **Select server roles** page, select **DNS Server**.
7. When the **Add Roles and Features Wizard** displays, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DNS Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, when the "Installation succeeded" message appears, click **Close**.

**► Task 2: Configure DNS forwarding**

1. On **SYD-SVR1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, expand **SYD-SVR1**, select and right-click **SYD-SVR1**, and then click **Properties**.
3. In the **SYD-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 **131.107.0.100**, and then press Enter. In a few moments, the IP address will resolve to **INET1** and you will see a green check mark beside the address. Click **OK**.
5. In the **SYD-SVR1 Properties** window, click **OK**.

**► Task 3: Configure DNS conditional forwarding**

1. On **SYD-SVR1**, with the **SYD-SVR1** node still expanded in the **DNS Manager** console tree, select **Conditional Forwarders**.
2. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** window, in the **DNS Domain** text box, type **Adatum.com**, and then, in the **<Click here to add IP address or DNS domain name>** text area, type **172.16.0.10**, press Enter, and then click **OK**.



**Note:** You might see a red **X** icon beside the IP address after you press Enter. This is normal. Continue by selecting OK in the window. The red **X** icon will resolve after this. You can return to the **Conditional Forwarder** dialog box, and click **Edit**, which will now show a green **Check Mark** icon in place of the red **X** icon.

4. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
5. In the **New Conditional Forwarder** window, in the **DNS Domain** text box, type **Contoso.com**, and then, in the **<Click here to add IP address or DNS domain name>** text area, type **131.107.0.100**, press Enter, and then click **OK**.

**► Task 4: Configure zones and resource records**

1. On **SYD-SVR1**, in the **DNS Manager** console, select and then right-click **Forward Lookup Zones**, and then click **New Zone**.
2. In the **New Zone Wizard**, click **Next**.
3. On the **Zone Type** page, select **Secondary zone**, and then click **Next**.
4. On the **Zone Name** page, in the **Zone name** text box, type **TreyResearch.net**, and then click **Next**.
5. On the **Master DNS Servers** page, in the **<Click here to add IP address or DNS domain name>** text area, type **172.16.0.11**, press Enter, and then click **Next**.
6. On the **Completing the New Zone Wizard** page, click **Finish**.
7. Switch to **LON-SVR1**.
8. Click **Start** and then click **Server Manager**.
9. In **Server Manager**, click **Tools**, and then click **DNS**.
10. In the console tree, select **LON-SVR1**, and then select and expand **Forward Lookup Zones**.
11. Select and right-click **TreyResearch.net**, and then click **Properties**.
12. In the **TreyResearch.net Properties** page, click the **Zone Transfers** tab.

13. Under the **Allow zone transfers** area, select **Only to the following servers**, and then click **Edit**.
14. In the **<Click here to add IP address or DNS domain name>** text area, type **172.16.19.20**, press Enter, and then click **OK**.
15. In the **TreyResearch.net Properties** dialog box, while still in the **Zone Transfers** tab, click **Notify**.
16. In the **Notify** window, under the **Automatically notify** area, select **The following servers**. In the **<Click here to add IP address or DNS domain name>** text area, type **172.16.19.20**, press Enter, and then click **OK**.
17. In the **TreyResearch.net Properties** page, click **OK**.
18. Switch to **SYD-SVR1**, and then in the DNS console, in the console tree, select the **TreyResearch.net** zone.
19. In the details pane, you should see the **Start of Authority (SOA)** and **Name Server (NS)** resource records for LON-SVR1.Adatum.com.

► **Task 5: Configure name resolution between zones**

1. Switch to **LON-SVR1**, and then in the DNS console, in the console tree, select the **TreyResearch.net** zone.
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 **ATL-SVR1**, in the **IP address** text box, type **172.16.18.125**, and then select **Add Host**.
4. In the **DNS** pop-up window, select **OK**, and then in the **New Host** window, click **Done**.
5. Switch to **SYD-SVR1**, and then in the DNS console, in the console tree, select the **TreyResearch.net** zone.
6. Right-click **TreyResearch.net**, and then click **Refresh**. In the details pane, you should now see the **ATL-SVR1** host record, along with the **Start of Authority (SOA)** and **Name Server (NS)** resource records for LON-SVR1.Adatum.com.

**Results:** After completing this exercise, you should have installed and configured DNS on **20741A-SYD-SVR1** successfully.

► **Task 6: Prepare for the next lab**

- After you finish this lab, Leave the virtual machine running for the next lab.

# Lab B: Integrating DNS with AD DS

## Exercise 1: Integrating DNS with AD DS

### ► Task 1: View resource records for the Sydney location

1. On **SYD-SVR1**, in the **DNS Manager** console, in the console tree, expand **SYD-SVR1**, and then select and expand **Forward Lookup Zones**.
2. Note that **Adatum.com** does not appear.
3. Click the **Conditional Forwarders** node in the console tree, right-click **Adatum.com**, and then click **Delete**.
4. In the **DNS** pop-up window, click **Yes**.
5. Close the **DNS Manager** console.
6. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **DNS**.
7. In the console tree, expand **LON-DC1**, select and expand **Forward Lookup Zones**, and then select **Adatum.com**.
8. Note the resource records in the details pane. You will compare these to the resource records on **SYD-SVR1** after it is promoted to be a domain controller.
9. Do not close the **DNS Manager** console on **LON-DC1**.

### ► Task 2: Install AD DS on SYD-SVR1

1. On **SYD-SVR1**, in the **Server Manager** console, click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **SYD-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** 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, *do not* close it. Instead, click the hyperlink **Promote this server to a domain controller**.
11. 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**.
12. On the **Domain Controller Options** page, ensure that **Domain Name System (DNS) server** and the **Global Catalog (GC)** are selected, type **Pa\$\$w0rd** in both text boxes, and then click **Next**.
13. On the **DNS Options** page, click **Next**.
14. On the **Additional Options** page, click **Next**.
15. On the **Paths** page, click **Next**.
16. On the **Review Options** page, click **Next**.

17. On the **Prerequisites Check** page, click **Install**.



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

18. After **SYD-SVR1** restarts, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
19. On the **Taskbar**, right-click the **Network** icon, and then click **Open Network and Sharing Center**.
20. In the **Network and Sharing Center** window, click the **Ethernet** hyperlink.
21. In the **Ethernet Status** window, click **Properties**.
22. In the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IP4)**, and then click **Properties**.
23. In the **Internet Protocol Version 4 (TCP/IP4) Properties** dialog box, in the **Preferred DNS server** text box, type **172.16.19.20**, and in the **Alternate DNS server** text box, type **172.16.0.10**, and then click **OK**.
24. Click **Close** two times.
25. Close the **Network and Sharing Center** window.

► **Task 3: Review resource records on SYD-SVR1**

1. On **SYD-SVR1**, open **Server Manager**, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, in the console tree, expand **SYD-SVR1**, expand **Forward Lookup Zones**, and then click the **Adatum.com** zone.
3. Right-click **Adatum.com**, and then click **Properties**.
4. In the **Adatum.com Properties** dialog box, click the **Start of Authority** tab. Ensure that **SYD-SVR1** shows as the **Primary server**.
5. Click **Cancel**.
6. With the **Adatum.com** zone still selected, review the resource records in the details pane. All the resource records that appeared in the **LON-DC1** zone **Adatum.com** will appear here on **SYD-SVR1**.
7. In the console tree, right-click the **Adatum.com** zone, and then click **New Host (A or AAAA)...**
8. In the **New Host** window, in the **Name** text box, type **SYD-CL1**, in the **IP address** text box, type **172.16.19.150**, and then click **Add Host**.
9. In the **DNS** pop-up window, click **OK**, and then in the **New Host** window, click **Done**.
10. Switch to **LON-DC1**, in the **DNS Manager** console, click the **Adatum.com** zone in the console tree, right-click **Adatum.com**, and then click **Refresh**. In the details pane, you should now see the **SYD-CL1** host record.
11. If the **SYD-CL1** record does not appear, perform the following actions on **LON-DC1**:
  - a. In **Server Manager**, in the **Tools** drop-down list, click **Active Directory Sites and Services**.
  - b. In the **Active Directory Sites and Services** window, in the console tree, expand **Sites**, expand **Default-First-Site-Name**, and then expand **Servers**.
  - c. Expand **LON-DC1**, and then click **NTDS Settings**.
  - d. In the details pane, right-click the **<automatically generated>** replication link, and then click **Replicate Now**.

- e. In the **Replicate Now** pop-up window, click **OK**.
  - f. Repeat step 10 above. The **SYD-CL1** resource record should display in the **Adatum.com** zone.
12. Close all open windows.

**Results:** After completing this exercise, you should have integrated DNS with AD DS successfully.

► **Task 4: Prepare for the next lab**

- After you finish this lab, leave the virtual machines running for the next lab.

# Lab C: Configuring advanced DNS settings

## Exercise 1: Configuring DNS policies

### ► Task 1: Verify DNS name resolution before configuring DNS policies

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 **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**, 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**.
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 last command returns the IP address **172.16.0.10**.

### ► Task 2: Configure DNS policies

1. On **LON-DC1**, in the **Windows PowerShell** window, type the following command, and then press Enter:

```
Import-Module DnsServer
```



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

- At the Windows PowerShell command prompt, type the following cmdlets, and 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
```

### ► Task 3: Check DNS name resolution after configuring DNS policies

- Switch to **LON-CL1**.
- While still on **LON-CL1**, In the **Administrator: Command Prompt** window, type the following two commands, and press Enter after each command:

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

- You should get the result **172.16.0.41**.
- Switch to **TOR-SVR1**, click **Start**, and then click **Windows PowerShell**.
- In the **Windows PowerShell** console, type the following two commands, and press Enter after each command:

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

- You should get the result **172.16.18.17**.

**Results:** After completing this exercise, you should have configured DNS policies, and then tested that the policies work successfully.

## Exercise 2: Validating the DNS implementation

### ► Task 1: Connect the client to the appropriate virtual LAN

- On the student host computer, open **Hyper-V Manager**, and then in the **20741A-LON-CL1 <hostname> - Virtual Machine Connection** window, in the **File** menu, click **Settings**.
- In the **Settings for 20741A-LON-CL1 on <hostname>** window, in the console tree, select **Network Adapter** for the **London\_Network**.
- In the details pane, in the **Virtual switch** drop-down list, select **PAC-WAN**, and then click **OK**.
- Switch back to **LON-CL1**.
- On the **Taskbar**, in the **Search** text box, type **PowerShell**, and then in the list that is returned, click **Windows PowerShell**.



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

```
Get-DnsClientServerAddress
```

Note that the DNS server address assigned to London\_Network IPv4 is **172.16.0.10**. This is **LON-DC1**.

- Right-click **Start**, and then then click **Control Panel**.
- In the **Control Panel**, click **Network and Internet**.
- In the **Network and Internet** dialog box, click **Network and Sharing Center**.
- In **Network and Sharing Center**, click **London\_Network**.
- In the **London\_Network Status** dialog box, click **Properties**.
- Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
- In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, in the **IP address** text box, change the third octet from **0** to **19**.
- In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, in the **Default gateway** text box, change the third octet from **0** to **19**.
- In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, in the **Preferred DNS server** box, type **172.16.19.20**, and then click **OK**.
- In the **London\_Network Properties** dialog box, click **Close**.
- In the **London\_Network Status** dialog box, click **Close**. If a **Networks** window appears that states, **"Do you want to allow your PC to be discoverable by other PCs and devices on this network?"**, click **No**.

► **Task 2: Use DNS tools to confirm proper client configuration**

- On **LON-CL1**, in **Windows PowerShell**, type the following cmdlet, and press Enter after each line:

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

Note that the DNS server address assigned to Ethernet IPv4 is **172.16.19.20**. This is **SYD-SVR1**.

- On **SYD-SVR1**, in **Server Manager**, click **Tools**, and then click **DNS**.
- In **DNS Manager**, expand **SYD-SVR1**, expand **Forward Lookup Zones**, and then select **Adatum.com**.
- In the details pane, examine the **LON-CL1** host record. The IP address should be **172.16.19.50**.
- If the address still shows as **172.16.0.50**, perform the following:
  - Switch to **LON-CL1**.
  - On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
Register-DnsClient
```

- Switch to **SYD-SVR1**. In the console tree, right-click **Adatum.com**, and then click **Refresh**. The host record for **LON-CL1** should have an IP address of **172.16.19.50**.
- In the console tree, right-click **SYD-SVR1**, and then click **Clear Cache**.

**► Task 3: Test DNS name resolution to external and internal hosts**

1. On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlets, and press Enter after each line:

```
Clear-DnsClientCache  
Nslookup mail.contoso.com
```

You should get a non-authoritative reply of **10.10.0.50**.

2. On **LON-CL1**, in the **Windows PowerShell** console, type the following cmdlet, and then press Enter:

```
Nslookup treyresearch.net
```

You should get a reply of **172.16.19.20**.

**Results:** After completing this exercise, you should have validated the implementation of a global DNS infrastructure successfully.

**Exercise 3: Troubleshooting DNS****► Task 1: Review the scenario**

- Read the help desk Incident Record 723101 in the Student Handbook Exercise Scenario.

**► Task 2: Simulate the problem**

1. Switch to **LON-CL1**.
2. From the Taskbar, click **File Explorer**.
3. In **File Explorer**, in the address bar, type **\\LON-DC1\Labfiles\Mod04**, and then press Enter.
4. In the details pane, right-click **Scenario.vbs** and then select **Copy**.
5. In the console tree of **File Explorer**, click the **Documents** library, and then, in the empty space of the details pane, right-click and select **Paste**. Close **File Explorer**.
6. In the taskbar, in the **Search** area, type **cmd**, and then, in the **Best match** list that appears, right click **cmd**, and then select **Run as administrator**.
7. In the **Command Prompt** window, type **cd documents** and then press the Enter key.
8. Type **Scenario.vbs**, and then press the Enter key. Close the **Command Prompt** window.

**► Task 3: Resolve the problem**

1. On **LON-CL1**, while still in Windows PowerShell, type the following command, and then press Enter:

```
Get-DnsClientCache
```

2. Notice the records that are returned.
3. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Clear-DnsClientCache
```

- At the Windows PowerShell command prompt, type the following command, and then press Enter. Notice that the address returned is the default gateway:

```
test-connection lon-dc1
```

- At the Windows PowerShell command prompt, type the following command, and then press Enter. Notice that the wrong IP address is returned for **LON-DC1**:

```
Get-DnsClientCache | fl
```

- At the Windows PowerShell command prompt, type the following command, and then press Enter. Notice that the correct record is returned from the Domain Name System (DNS) server:

```
nslookup LON-DC1
```

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

```
notepad C:\windows\system32\drivers\etc\hosts
```

- Scroll to the end of the file, delete **172.16.0.1 lon-dc1.adatum.com**, and then press Enter.

- Click **File**, and then click **Save**.

- Close Notepad.

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

```
Clear-DnsClientCache
```

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

```
test-connection lon-dc1
```

- At the Windows PowerShell command prompt, type the following command, and then press Enter. You can now see the correct record for LON-DC1 in the cache:

```
Get-DnsClientCache | fl
```

- At the Windows PowerShell command prompt, type the following command, and then press Enter. Note that the command runs successfully:

```
Resolve-Dnsname LON-DC1 | fl
```

- Click **File Explorer**.

- In the **File Explorer** address bar, type **\\LON-DC1\Labfiles**, and then press Enter. The folder opens.

- Close **File Explorer**.

- Update the **Resolution** section of the Incident Record with the following comments:

- The client had an incorrect entry in the hosts file. Because this entry is used to populate the DNS resolver cache, the client could not resolve the host name **LON-DC1**.
- Removed the entry, and the client was able to connect to resources.

**Results:** After completing this exercise, you should have resolved the name resolution problems successfully.

► **Task 4: Prepare for the next module**

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


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

## Module 5: Implementing and managing IPAM

# Lab: Implementing IPAM

### Exercise 1: Installing the IPAM Server feature

#### ► Task 1: Prepare the lab environment

 **Note:** Running the following scripts will return several warnings regarding Windows updates. You can ignore these warnings.

1. Switch to **LON-SVR1**.
2. On **LON-SVR1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. At the command prompt in the Windows PowerShell command-line interface, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\LON-SVR1_Mod05_Setup.ps1
```

4. Switch to **TOR-SVR1**.
5. On **TOR-SVR1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
6. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\TOR-SVR1_Mod05_Setup.ps1
```

7. Switch to **SYD-SVR1**.
8. On **SYD-SVR1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
9. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
C:\Labfiles\Mod05\SYD-SVR1_Mod05_Setup.ps1
```

**SYD-SVR1** will restart when the script completes. After it restarts, sign in as **Adatum\Administrator** with the password of **Pa\$\$w0rd**.

#### ► Task 2: Install the IPAM Server feature on LON-SVR2

1. If necessary, sign in to **LON-SVR2** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Click **Start** and then click **Server Manager**. In the results pane, click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, select the **IP Address Management (IPAM) Server** check box.
8. In the **Add features that are required for IP Address Management (IPAM) Server?** dialog box, click **Add Features**, and then click **Next**.

9. On the **Confirm installation selections** page, click **Install**.
10. When the **Add Roles and Features Wizard** completes, close the wizard.

**Results:** After completing this exercise, you should have successfully installed the IPAM Server feature.


## Exercise 2: Provisioning the IPAM server

### ► Task 1: Configure the IPAM server for GPO deployment

1. On **LON-SVR2**, 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, ensure that **Windows Internal Database (WID)** is selected, and then click **Next**.
6. On the **Select provisioning method** page, ensure that **Group Policy Based** is selected.
7. In the **GPO name prefix** text box, type **IPAM**, and then click **Next**.
8. On the **Confirm the Settings** page, click **Apply**. Provisioning will take a few moments to complete.
9. When provisioning completes, click **Close**.

### ► Task 2: Perform discovery on Adatum.com

1. In the **IPAM Overview** pane, click **Configure server discovery**.
2. In the **Configure Server Discovery** dialog box, click **Get forests**, and then in the **Configure Server Discovery** dialog box, click **OK**.
3. Click **OK** again, and then click **Configure server discovery**.
4. In the **Configure Server Discovery** dialog box, click **Add** to add the **Adatum.com** domain, and then click **OK**.
5. In the **IPAM Overview** pane, click **Start server discovery**. Discovery might take 5-10 minutes to run. The yellow bar indicates when discovery is complete.
6. 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 the servers. Scroll down to the **Details** view, and then note the status report.


 **Note:** You have not yet granted the IPAM server permission to manage servers in the Adatum.com domain by using Group Policy.

► **Task 3: Provision IPAM server to manage DC, DNS, and DHCP servers**


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

```
Invoke-IPAMGpoProvisioning -Domain Adatum.com -DomainController lon-dc1.adatum.com -
GpoPrefixName IPAM -IpamServerFqdn LON-SVR2.adatum.com -DelegatedGpoUser
Administrator
```

3. When you are prompted to confirm the action, type **Y**, and then press Enter.  
The command will take a few moments to complete.
4. Close Windows PowerShell.
5. Switch to **LON-DC1**.
6. In **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
7. In the **Active Directory Administrative Center** window, in the navigation pane, click **Global Search**.
8. In the **Search** box, type **IPAMUG**, and then press Enter.
9. Double-click the **IPAMUG** group.
10. In the **IPAMUG** dialog box, under **Group scope**, click **Global**.
11. Scroll down to the **Member Of** section, and then click **Add**.
12. In the **Select Groups** window, type **Domain Admins**, click **Check Names**, and then click **OK**.
13. Click **OK** to close the **IPAMUG** dialog box.
14. Close **Active Directory Administrative Center**.
15. Switch to **LON-SVR2**.
16. Restart **LON-SVR2**.
17. On **LON-SVR2**, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
18. Click **Start**, and then click **Server Manager**. Click **IPAM**, and then click **SERVER INVENTORY**.
19. In the **IPv4 details** pane, right-click **lon-dc1**, and then click **Edit Server**.
20. In the **Add or Edit Server** dialog box, set the **Manageability status** field to **Managed**, and then click **OK**.

 **Note:** If a Group Policy Object (GPO) error appears, switch the server back to **Unspecified**, and then restart **LON-DC1**, **LON-SVR1**, **LON-SVR2**, **TOR-SVR1**, and **SYD-SVR1**. Sign back into all servers as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

21. In the **IPv4 details** pane, right-click **lon-svr1**, and then click **Edit Server**.
22. In the **Add or Edit Server** dialog box, set the **Manageability status** field to **Managed**, and then click **OK**.
23. In the **IPv4 details** pane, right-click **tor-svr1**, and then click **Edit Server**.
24. In the **Add or Edit Server** dialog box, set the **Manageability status** field to **Managed**, and then click **OK**.
25. In the **IPv4 details** pane, right-click **SYD-SVR1**, and then click **Edit Server**.

26. In the **Add or Edit Server** dialog box, set the **Manageability status** field to **Managed**, and then click **OK**.
  27. Switch to **LON-DC1**.
  28. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
  29. At the Windows PowerShell command prompt, type **Gpupdate /force**, and then press Enter.
  30. Close the **Windows PowerShell** window.
  31. Switch to **LON-SVR1**.
  32. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
  33. At the Windows PowerShell command prompt, type **Gpupdate /force**, and then press Enter.
  34. Close the **Windows PowerShell** window.
  35. Switch to **TOR-SVR1**.
  36. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
  37. At the Windows PowerShell command prompt, type **Gpupdate /force**, and then press Enter.
  38. Close the **Windows PowerShell** window.
  39. Switch to **SYD-SVR1**.
  40. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
  41. At the Windows PowerShell command prompt, type **Gpupdate /force**, and then press Enter.
  42. Close the **Windows PowerShell** window.
  43. Switch back to **LON-SVR2**.
  44. In **Server Manager**, right-click **LON-DC1**, and then click **Refresh Server Access Status**. Repeat this step for **LON-SVR1**, **TOR\_SVR1**, and **SYD\_SVR1**.
  45. When completed, refresh IPv4 by clicking **Refresh**.
-  **Note:** It might take up to five minutes for the status to change. If the status does not change, restart **LON-DC1**, **LON-SVR1**, **LON-SVR2**, **TOR\_SVR1**, and **SYD\_SVR1**, and then repeat step 43-45. Ensure that you restart **LON-DC1** before restarting the other virtual machines.
46. In the **IPAM Overview** pane, click **Retrieve data from managed servers**. This action will take a few moments to complete.

**Results:** After completing this exercise, you should have successfully provisioned the IPAM server.

### Exercise 3: Managing IP address spaces by using IPAM

#### ► Task 1: Add an IP address block

1. On **LON-SVR2**, in **Server Manager**, in the navigation pane, click **IP Address Blocks**.
2. In the **IPv4** pane, next to the **current view**, click **IP Address Ranges**.





**Note:** Note the three IP address ranges displayed from **TOR-SVR1**.

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** window, type the following in the text boxes, and then click **OK**:
  - o Network ID: **172.16.18.0**
  - o Prefix length: **24**
  - o Start IP address: **172.16.18.0**
  - o End IP address: **172.16.18.255**
  - o Description: **Toronto subnet**
5. In the **IPv4** pane, next to the **current view**, click **IP Address Blocks**.



**Note:** Note the newly created address block for Toronto.

#### ► Task 2: 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 either of the IP address ranges with a **Network** value of **172.16.20.0/23**, and then click **Edit IP Address Range**.
4. In the **Edit IP Address Range** window, click **Reservations**.
5. In the **Reservations** text box, type **172.16.20.200**, click **Add**, and then click **OK**.

#### ► Task 3: Deactivate the Portland Wired scope

1. Click the **DHCP Scopes** node, in the details pane, right-click the first scope listed with a **Scope ID** of **172.16.23.0**, and then click **Deactivate DHCP Scope**.
2. Repeat step 1 for the second scope with a listed **Scope ID** of **172.16.23.0**.



**Note:** This scope is duplicated as a result of Dynamic Host Configuration Protocol (DHCP) failover configuration between **TOR-SVR1** and **LON-SVR1**. The preceding steps deactivate the scopes on both servers.

**Results:** After completing this exercise, you should have successfully managed IP address spaces by using IPAM.

#### ► Task 4: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.

3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-EU-RTR**, **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-SYD-SVR1**, and **20741A-TOR-SVR1**.

## Module 6: Remote access in Windows Server 2016

# Lab: Implementing Web Application Proxy

### Exercise 1: Implementing Web Application Proxy

#### ► Task 1: Prepare environment

##### Disable Routing and Remote Access on EU-RTR

1. Switch to **EU-RTR**.
2. Click the **Start** button, and then click the **Server Manager** tile.
3. In **Server Manager**, on the upper-right side, click **Tools**, and then click **Routing and Remote Access**.
4. In the **Routing and Remote Access** console, in the left pane, right-click **EU-RTR (local)**, and then click **Disable Routing and Remote Access**.
5. In the **Routing and Remote Access** dialog box, click **Yes**, and then close the **Routing and Remote Access** window.



**Note:** Routing and Remote Access is preconfigured on the virtual machine for other labs in this course. The Web Application Proxy configuration in this lab will not work properly if you leave Routing and Remote Access enabled on the virtual machine.

#### ► Task 2: Remove the client computer from a domain

1. Switch to **LON-CL1**.
2. Right-click the **Start** button, and then click **System**.
3. In the **System** window, click **Advanced system settings**, and then click the **Computer Name** tab.
4. On the **Computer Name** tab, click the **Change** button.
5. In the **Computer Name/Domain Changes** dialog box, click **Workgroup**, in the **Workgroup** box, type **WORKGROUP**, and then click **OK**.
6. In the **Computer Name/Domain Changes** dialog box, click **OK**.
7. In the **Welcome to the WORKGROUP workgroup** dialog box, click **OK**.
8. To restart the computer, click **OK**.
9. To close **System Properties** dialog box, click **Close**.
10. Click **Restart Now**, and then wait for the computer to restart.

##### Import Root CA certificate on client

1. When the **LON-CL1** computer restarts, sign in with the user name **Admin** and the password **Pa\$\$w0rd**.
2. When prompted by **Networks**, click **Yes**.
3. On the desktop, on the taskbar, click the **File Explorer** icon.
4. In the **This PC** window, in the address bar, type **\\172.16.0.10\C\$**, and then press Enter.

5. When prompted for the username, type **Adatum\Administrator**, for the password, type **Pa\$\$w0rd**, and then press Enter.
6. In the **File Explorer** window, right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
7. In the **Open File – Security Warning** dialog box, click **Open**.
8. On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
9. In the **User Account Control** dialog box, click **Yes**.
10. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
11. On the **Certificate Store** page, click **Next**, and then click **Finish**.
12. In the **Certificate Import Wizard**, click **OK**.
13. Right-click the **Start** button, and click **Command Prompt**.
14. In the **Command Prompt** window, type **mmc**, and then press Enter.
15. In the **User Account Control** dialog box, click **Yes**.
16. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
17. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
18. In the **Certificates snap-in** dialog box, click **Computer** account, click **Next**, click **Finish**, and then click **OK**.
19. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
20. Verify that **AdatumCA** exists.



**Note:** You perform the above steps to import the AdatumCA certificate into Trusted Root Certification Authorities of **LON-CL1**, and then to verify that the AdatumCA certificate is imported into Trusted Root Certification Authorities of **LON-CL1**. This enables the client to trust the certificates issued by the Adatum Certification Authority.

### Move the computer 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** field, type **https://lon-svr1.adatum.com**, and then press Enter. Notice that a "Network Error" message displays.
6. Right-click the **Start** button and click **Run**. In the **Run** dialog box type **mstsc**, and then press Enter.

7. In the **Remote Desktop Connection** app, in the **Computer** field, 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 web site running on lon-svr1 and connect to **lon-dc1** using Remote Desktop because the client cannot access the internal network.

### ► Task 3: Install the Web Application Proxy role service

#### 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**, on the **Select installation type** page, click **Next**, and then on the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **Remote Access**, click **Web Application Proxy**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

### ► Task 4: Configure access to an internal website


#### Obtain a certificate for the ADFS WAP farm

1. On **EU-RTR**, right-click the **Start** button, and 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 Certificate**, 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, under the **Type** field, click the drop-down list, and select **Common name**, in the **Value** box, type **adfs wap.adatum.com**, and then click **Add**.
11. In the **Alternative name** list, under the **Type** field, click the drop-down list, and select **DNS**. In the **Value** box, type **adfs wap.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 **Pa\$\$w0rd**, and then click **Next**.
6. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, click **adfswap.adatum.com**, and then click **Next**.
7. On the **Confirmation** page, review the settings. If necessary, 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 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 the **Backend server URL** is entered automatically 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.

### ► Task 5: Configure access to Remote Desktop Gateway

#### Install Remote Desktop Gateway

1. Switch to **LON-SVR2**.
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**, on the **Select installation type** page, click **Next**, and then, on the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, click **Remote Desktop Services**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Remote Desktop Services** page, click **Next**.
8. On the **Select role services** page, click **Remote Desktop Gateway**. When you receive a prompt, click **Add Features**, and then click **Next**.
9. On the **Network Policy and Access Services** page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.
13. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

#### Obtain certificate for Remote Desktop Gateway server

1. On **LON-SVR2**, 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 Certificate**, 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, under the **Type** field, click the drop-down list and select **Common name**, in the **Value** box, type **rdgw.adatum.com**, and then click **Add**.
11. Click **OK** to close the **Certificate Properties** dialog box.
12. Click **Enroll** to proceed with Certificate Enrollment.
13. Click **Finish** to close the **Certificate Enrollment** dialog box.

### Configure Remote Desktop Gateway server

1. In **Server Manager**, on the **Tools** menu, select **Remote Desktop Services**, and then click **Remote Desktop Gateway Manager**.
2. In the **RD Gateway Manager**, click **LON-SVR2 (Local)**.
3. In the details pane, under **RD Gateway Server Status: LON-SVR2**, click the **View or modify certificate properties** link.
4. On the **SSL Certificate** tab in the **LON-SVR2 Properties** dialog box, click **Import Certificate**.
5. In the **Import Certificate** dialog box, click the **rdgw.adatum.com** certificate, and then click **Import**. Verify that information about the certificate is now listed on the **SSL Certificate** tab.
6. Click the **SSL Bridging** tab, and then click **Use SSL Bridging**. Verify that **HTTPS – HTTPS bridging (terminate SSL requests and initiate new HTTPS requests)** is selected. Click **OK**, and then, when prompted by RD Gateway, click **Yes**.
7. In the **RD Gateway Manager**, expand **LON-SVR2 (Local)**, right-click **Policies**, and then click **Create New Authorization Policies**.
8. On the **Create Authorization Policies for RD Gateway** page, verify that **Create a RD CAP and a RD RAP (recommended)** is selected, and then click **Next**.



**Note:** An RD CAP allows you to select the users that can connect to a remote computer using the RD Gateway server.

9. On the **Create an RD CAP** page, type **Adatum Admins**, and then click **Next**.
10. On the **Select Requirements** page, in the **User group membership (required)** section, click **Add Group**.
11. In the **Select Groups**, type **Domain admins**, click **Check Names**, and then click **OK**. On the **Select Requirements** page, click **Next**.
12. On the **Enable or Disable Device Redirection** page, click **Disable device redirection for the following client device types**, and then click **Next**.



13. On the **Set Session Timeout** page, click **Enable idle timeout**, in the value field, type **15**, and then click **Next**.
14. On the **RD CAP Settings Summary** page, verify your selections, and then click **Next**.



**Note:** An RD RAP allows you to select the network resources that users can connect to remotely using the RD Gateway server.

15. On the **Create an RD RAP** page, type **Adatum admins – allow access to all computers**, and then click **Next**.
16. On the **Select User Groups** page, verify that **ADATUM\Domain Admins** displays under **User group membership (required)**, and then click **Next**.
17. On the **Select Network Resources** page, click **Allow users to connect to any network resource (computer)**, and then click **Next**.
18. On the **Select Allowed Ports**, click **Next**.
19. On the **RD RAP Settings Summary** page, verify your selection, and then click **Finish**.
20. On the **Confirm Creation of Authorization Policies**, click **Close**.

### **Publish the Remote Desktop Gateway Server**

1. Switch to **EU-RTR**.
2. 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**.
3. In the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
4. On the **Preauthentication** page, click **Pass-through**, and then click **Next**.
5. 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://rdgw.adatum.com**.
  - c. In the **External certificate** list, click **adfsweb.adatum.com**.
  - d. In the **Backend server URL** box, ensure that **https://rdgw.adatum.com** is listed, and then click **Next**.



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

6. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the Windows PowerShell command to set up additional published applications.
7. On the **Results** page, ensure that the application published successfully, and then click **Close**.

**Results:** After completing this exercise, you should have successfully implemented Web Application Proxy.

## Exercise 2: Validating the Web Application Proxy deployment

### ► Task 1: Verify access to the internal website from the client computer

1. Switch to **LON-CL1**.
2. On the taskbar, click the **Microsoft Edge** icon.
3. In the **Search or enter web address** field, type **https://lon-svr1.adatum.com** and then press Enter.
4. When you receive a prompt, in the **Microsoft Edge** dialog box, type **adatum\logan** for the username, and **Pa\$\$w0rd** for the password, and then click **OK**.
5. Verify that the default IIS 9.0 webpage for **LON-SVR1** opens.

### ► Task 2: Verify access to the internal Remote Desktop Gateway Server and remote desktop access to LON-DC1

1. Right-click the **Start** button and click **Run**. In the **Run** dialog box, type **mstsc**, and then press Enter.
2. In the **Remote Desktop Connection** app, click **Show Options**, and then click the **Advanced** tab.
3. On the **Advanced** tab, in the drop-down box under **If server authentication fails**, click **Connect and don't warn me**.



**Note:** In real life, you would leave this setting at **Warn me**. However, because the certificate revocation list distribution point (CDP) is not reachable to **LON-CL1** in this lab, you change it.

4. Click **Settings**, and in the **RD Gateway Server Settings** dialog box, click **Use these RD Gateway server settings**. In the **Server name** box, type **rdgw.adatum.com**. In the **Logon settings** section, click **Use my RD Gateway credentials for the remote computer**. Click **OK**.



**Note:** If you have not chosen the **Use my RD Gateway credentials for the remote computer** setting, you would have to validate twice—once for the Remote Desktop Gateway server and once for the server you are connecting to.

5. Click the **General** tab, and in the **Computer** field, type **lon-dc1**, and then click **Connect**.
6. In the **Windows Security** dialog box, type **adatum\administrator** for the username and **Pa\$\$w0rd** for the password, and then click **OK**.
7. Verify that you can connect to **LON-DC1** using Remote Desktop.



**Note:** It will take approximately 20 seconds to connect to **LON-DC1**.

**Results:** After completing this exercise, you will have verified that external users are able to access the internal application through the Web Application Proxy.

► **Task 3: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-SVR1**, **20741A-LON-SVR2**, **20741A-EU-RTR**, **20741A-INET1**, and **20741A-LON-CL1**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 7: Implementing DirectAccess

# Lab A: Implementing DirectAccess by using the Getting Started Wizard

### Exercise 1: Verifying readiness for a DirectAccess deployment

#### ► Task 1: Document the network configuration

##### Verify the IP address on LON-DC1

1. Switch to **LON-DC1**.
2. Right-click **Start**, and then click **Network Connections**.
3. In the **Network Connections** window, right-click the **Ethernet** icon, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. Document the current IP address, subnet mask, default gateway, and DNS configuration.
6. Click **Cancel** twice, and then close the **Network Connections** window.

##### Verify the network configuration on EU-RTR

1. Switch to **EU-RTR**.
2. Click **Start**, and then click the **Server Manager** tile.
3. In **Server Manager**, on the upper right side, click **Tools**, and then click **Routing and Remote Access**.
4. In the **Routing and Remote Access** console, in the left pane, right-click **EU-RTR (local)**, and then click **Disable Routing and Remote Access**.
5. In the **Routing and Remote Access** dialog box, click **Yes**.
6. Close the **Routing and Remote Access** window.



**Note:** Routing and Remote Access is preconfigured on the virtual machine for other labs in this course. The DirectAccess configuration in this lab will not work properly if you leave Routing and Remote Access enabled on the virtual machine.

7. Right-click **Start**, and then click **Network Connections**.
8. In the **Network Connections** window, verify that the following four network adapters display: **Internet**, **London\_Network**, **NA\_WAN**, and **PAC\_WAN**.



**Note:** For this module, you will use only London Network, which is connected to both the internal network and the Internet.

9. In the **Network Connections** window, right-click the **London\_Network** adapter, and then click **Disable**.
10. In the **Network Connections** window, right-click the **London\_Network** adapter, and then click **Enable**.
11. Repeat steps 9 and 10 for the following network connections: **Internet**, **NA\_WAN**, and **PAC\_WAN**.

12. Verify that **London\_Network** adapter is connected to the domain network **Adatum.com**.
13. Right-click the **London\_Network** adapter, and then click **Properties**.
14. In the **London\_Network Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
15. Verify that the IP address corresponds with the subnet used in the domain network (the IP address should be 172.16.0.1.), and then click **Cancel** twice.
16. Right-click the Internet adapter, and then click **Properties**.
17. In the **Internet Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
18. Verify that the IP address corresponds with the subnet used to simulate internet connectivity. (The IP address should be 131.107.0.10).
19. Click **Cancel** twice, and then close the **Network Connections** window.



**Note:** If you notice that the Internet network adapter is connected to Adatum.com, disable Microsoft Routing and Remote Access Service (RRAS). This is because for DirectAccess, you will need at least one adapter to be on the external network.

### Verify the network configuration on LON-CL1

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **Network Connections**.
3. In the **Network Connections** window, verify that the **London\_Network** adapter is connected to the domain network **Adatum.com**.
4. Right-click the **London\_Network** adapter, and then click **Properties**.
5. In the **London\_Network Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration, and then click **Cancel** twice.
7. Close the **Network Connections** window.

### Verify the network configuration on LON-SVR1

1. Switch to **LON-SVR1**.
2. Right-click **Start**, and then click **Network Connections**.
3. In **Network Connections**, verify that the **Ethernet** adapter is connected to the domain network **Adatum.com**.
4. Right-click the **Ethernet** adapter, and then click **Properties**.
5. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration.
7. Click **Cancel** twice, and then click **Close**.

## Verify the network configuration on INET1

1. Switch to **INET1**.
2. Right-click **Start**, and then click **Control Panel**.
3. In **Control Panel**, under the **Network and Internet** section, click **View network status and tasks**.
4. In the **Network and Sharing Center** window, verify that **Public network** displays under **View your active networks**.
5. Still in the **Network and Sharing Center** window, from the menu on the left, click **Change adapter settings**.
6. Right-click the **Ethernet** adapter, and then click **Properties**.
7. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
8. Document the current IP address, subnet mask, default gateway, and DNS configuration, and then click **Cancel** twice.
9. Close both the **Network Connections** and **Network and Sharing Center** windows.



**Note:** The **INET1** server will have the IP address of 131.107.0.100, which simulates the Internet DNS server.

## ► Task 2: Verify the server readiness for DirectAccess

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.

**Results:** After completing this exercise, you should have successfully verified the readiness for DirectAccess deployment.

## Exercise 2: Configuring DirectAccess

### ► Task 1: Configure DirectAccess by using the Getting Started Wizard

1. Switch to **EU-RTR**.
2. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
3. In the **Remote Access Management** console, under **Configuration**, click **DirectAccess and VPN**.
4. Click **Run the Getting Started Wizard**.
5. In the **Getting Started Wizard**, on the **Configure Remote Access** page, click **Deploy DirectAccess only**.
6. Verify that **Edge** is selected. In the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** 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 to display an additional window for configuring 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 listed: **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**.
12. Verify that **DirectAccessClients** displays, and then click **OK**.
13. Clear the **Enable DirectAccess for mobile computers only** check box, and then click **Next**.
14. On the **DirectAccess Client Setup** page, fill out the following information, and then click **Finish**:
  - o Helpdesk email address: **DAHelp@adatum.com**
  - o DirectAccess connection name: **A. Datum DirectAccess**
15. On the **Remote Access Review** page, click **OK**.
16. On the **Configure Remote Access** page, click **Finish** and wait for the configuration to complete.
17. In the **Applying Getting Started Wizard Settings** dialog box, verify that the configuration was applied successfully, and then click **Close**.

**Results:** After completing this exercise, you should have successfully configured DirectAccess by using the Getting Started Wizard.



## Exercise 3: Validating the DirectAccess deployment

### ► Task 1: Verify the GPO deployment

1. Switch to **LON-CL1**.
2. Right-click **Start**, select **Shut down or sign out**, and then click **Restart**.



**Note:** You must restart the **LON-CL1** machine because you added the machine account to the DirectAccessClients security while the machine was running. In order to update the machine's security token, you must restart it.

3. When **LON-CL1** restarts, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.
4. Right-click **Start**, and then click **Command Prompt**.
5. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpresult /R
```

6. In the **Command Prompt** window, review the displayed output of the command that you executed in the previous step.
7. Under the **COMPUTER SETTINGS** section, verify that the **DirectAccess Client Settings** GPO is applied.



**Note:** If the DirectAccess Client Settings GPO is not applied, restart **LON-CL1**, and then sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.

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

```
netsh name show effectivepolicy
```

9. Verify that following message displays: **DNS Effective Name Resolution Policy Table Settings**



**Note:** DirectAccess settings are inactive when this computer is inside a corporate network.

10. Close the **Command Prompt** window.

### ► Task 2: Test DirectAccess connectivity from an internal and external client



**Note:** You may not be able to connect to the internal file share or the internal Web site since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

### Verify connectivity to internal network resources

1. On **LON-CL1**, on the taskbar, click the **Internet Explorer** icon.
2. In the Microsoft Internet Explorer Address bar, type **http://lon-svr1.adatum.com**, and then press Enter.
3. Leave the default IIS 9.0 webpage for **LON-SVR1** open.

4. Right-click **Start**, and then click **Run**. In the **Open** text box, type `\\LON-SVR1\Corpdata`, and then press Enter. Note that you are able to access the folder content.
5. Close all open windows.
6. Right-click **Start**, and then click **Command Prompt**.
7. In the **Command Prompt** window, type `ipconfig`, and then press Enter.



**Note:** Notice that you have information about the Ethernet adapter and Tunnel adapter isatap. This is because the **LON-CL1** connects directly to the internal network and is not using DirectAccess.

### Verify connectivity to internal resources from an external client

1. To move the client from the internal network to the Internet, on **LON-CL1**, right-click **Start**, 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. Right-click **Internet**, and then click **Properties**.
5. In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
6. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, ensure that the following settings display, and then click **OK**:
  - o IP address: **131.107.0.20**
  - o Subnet mask: **255.255.255.0**
  - o Preferred DNS server: **131.107.0.100**
7. In the **Internet Properties** dialog box, click **Cancel**.
8. Close all open windows.
9. On **LON-CL1**, on the taskbar, click the **Internet Explorer** icon.
10. In the Internet Explorer Address bar, type `http://lon-svr1.adatum.com`, and then press Enter.
11. Right-click **Start**, click **Run**, type `\\LON-SVR1\Corpdata`, and then press Enter. Note that you are able to access the folder content.
12. Close all open windows.
13. Right-click **Start**, and then click **Command Prompt**.
14. In the **Command Prompt** window, type `ipconfig`, and then press Enter.

Notice that you now have information about the Tunnel adapter iphtttpsinterface. You should see three IPv6 addresses, with two of them starting with **2002**. This is because the **LON-CL1** client is connected to the internal network using DirectAccess.

### Verify connectivity to the DirectAccess server

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

```
Netsh name show effectivepolicy
```

2. Verify that **DNS Effective Name Resolution Policy Table Settings** displays two entries: **.Adatum.com**, and **DirectAccess-NLS.Adatum.com**.

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

```
Powershell
```

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

```
Get-DAClientExperienceConfiguration
```

5. Review the DirectAccess client settings.

### Verify client connectivity on the DirectAccess server

1. Switch to **EU-RTR**.
2. Switch to the **Remote Access Management** console.
3. In the console tree, click **Remote Client Status**.
4. Notice that the client is connected via **IPHttps**.
5. In the **Connection Details** pane, in the bottom-right corner of the screen, note the use of Kerberos for the Machine and the User.
6. Close all open windows.



**Note:** Do not revert the virtual machines after completing this lab. You will need them for subsequent labs.

**Results:** After completing this exercise, you should have successfully validated the DirectAccess deployment.

# Lab B: Deploying an advanced DirectAccess solution

## Exercise 1: Preparing the environment for DirectAccess

► **Task 1: Configure the Active Directory Domain Services (AD DS) and Domain Name System (DNS) requirements**

### Modify the security group for DirectAccess client computers

1. Switch to **LON-DC1**.
2. In **Server Manager**, in the upper-right corner, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** console tree, expand **Special Accounts**, and then in the details pane, double-click **DirectAccessClients** group.
4. In the **DirectAccessClients Properties** dialog box, click the **Members** tab, and then click **Add**.
5. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.
6. In the **Enter the object names to select (examples)** text box, type **LON-CL2**, click **Check Names**, and then click **OK**.
7. Verify that both **LON-CL2** and **LON-CL1** display below the **Members** list, and then click **OK**.



**Note:** The DirectAccessClients security group will control which computer will be able to connect to the internal resources by using DirectAccess.

8. Close the **Active Directory Users and Computers** console.

### Create the required DNS records

1. In **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, in the console tree, expand **LON-DC1**, and then expand **Forward Lookup Zones\Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **Name** text box, type **nls**. In the **IP address** text box, type **172.16.0.11**, click **Add Host**, and then click **OK**.



**Note:** The client will use the NLS record to determine the network location.

5. In the **New Host** dialog box, in the **Name** text box, type **cr1**. In the **IP address** text box, type **172.16.0.1**, and then click **Add Host**.
6. In the **DNS** dialog box, click **OK**.

- In the **New Host** dialog box, click **Done**.



**Note:** The **crl** record will be used by the internal clients to check the revocation status on the certificates that are used in DirectAccess.

- Close the **DNS Manager** console.

### Configure the DNS suffix on EU-RTR

- Switch to **EU-RTR**.
- Right-click **Start**, and then click **Network Connections**.
- In the **Network Connection** window, right-click **Internet**, and then click **Properties**.
- In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
- In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Advanced**.
- On the **DNS** tab, in the **DNS suffix for this connection** text box, type **adatum.com**, and then click **OK**.
- In the **Internet Protocol Version 4 (TCP/IPv4)** dialog box, click **OK**.
- In the **Internet Properties** dialog box, click **OK**.
- Close the **Network Connections** window.



**Note:** The Internet client needs the DNS suffix to resolve names for internal resources.

## ► Task 2: Configure certificate revocation list (CRL) distribution

### Configure certificate requirements

- On **LON-DC1**, in **Server Manager**, on the **Tools** menu, click **Certification Authority**.
- In the details pane, right-click **AdatumCA**, and then click **Properties**.
- In the **AdatumCA Properties** dialog box, click the **Extensions** tab.
- On the **Extensions** tab, click **Add**.
- In the **Location** box, type **http://crl.adatum.com/crld/**.
- Under **Variable**, click **<CaName>**, and then click **Insert**.
- Under **Variable**, click **<CRLNameSuffix>**, and then click **Insert**.
- Under **Variable**, click **<DeltaCRLAllowed>**, and then click **Insert**.
- In the **Location** text box, at the end of the Location string, type **.crl**, and then click **OK**.
- Select check boxes for both **Include in CRLs. Clients use this to find Delta CRL locations**, and **Include in the CDP extension of issued certificates**, and then click **Apply**.
- In the pop-up dialog box that displays prompting you to restart Active Directory Certificate Services, click **No**.
- On the **Extensions** tab, click **Add**.
- In the **Location** text box, type **\\EU-RTR\crldist\$**.
- Under **Variable**, click **<CaName>**, and then click **Insert**.

15. Under **Variable**, click **<CRLNameSuffix>**, and then click **Insert**.
16. Under **Variable**, click **<DeltaCRLAllowed>**, and then click **Insert**.
17. In the **Location** text box, type **.crl** at the end of the string, and then click **OK**.
18. Click **Publish CRLs to this location**, click **Publish Delta CRLs to this location**, and then click **OK**.
19. In the pop-up dialog box that displays prompting you to restart Active Directory Certificate Services, click **Yes**.



**Note:** You perform these steps to prepare the certification authority (CA) with proper extensions for the CRL distribution point, which will be included in the future certificates that the CA will use.

### ► Task 3: Configure client certificate distribution

#### Configure computer certificate auto-enrollment

1. On **LON-DC1**, switch to **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management Console**, in the console tree, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Right-click **Default Domain Policy**, and then click **Edit**.
5. In the **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click **Public Key Policies**.
6. In the details pane, right-click **Automatic Certificate Request Settings**, point to **New**, and then click **Automatic Certificate Request**.
7. In the **Automatic Certificate Request Setup Wizard**, click **Next**.
8. On the **Certificate Template** page, click **Computer**, click **Next**, and then click **Finish**.
9. Close both the **Group Policy Management Editor** and the **Group Policy Management Console**.

### ► Task 4: Configure the network location server and DirectAccess server certificates

#### Request a certificate for LON-SVR1

1. On **LON-SVR1**, right-click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
mmc
```

4. In the console window, click **File**, and then click **Add/Remove Snap-in**.
5. In the **Available snap-ins** list, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, click **Local computer**, click **Finish**, and then click **OK**.

8. In the **Certificates snap-in** window, in the console tree of the Certificates snap-in, expand **Certificates (Local Computer)**, expand **Personal**, and then expand **Certificates**.
9. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
10. On the **Before you begin** page, click **Next**.
11. On the **Select Certificate Enrollment Policy** page, click **Next**.
12. On the **Request Certificates** page, click **Adatum Web Certificate**, and then click **More information is required to enroll for this certificate. Click here to configure settings**.
13. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, select **Common name as Type**.
14. In the **Value** text box, type **nls.adatum.com**, and then click **Add**.
15. Click **OK**, click **Enroll**, and then click **Finish**.
16. In the **Certificates snap-in** window, in the details pane, verify that a new certificate with the name **nls.adatum.com** is enrolled with **Intended Purposes** of **Server Authentication**.
17. Close the window, and when prompted to save the settings, click **No**.

### Change the HTTPS bindings

1. Open **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager** message box, expand **LON-SVR1 (ADATUM\Administrator)**.
3. In **Internet Information Services (IIS) Manager**, expand **Sites**, and then click **Default Web site**.
4. In the **Actions** pane, click **Bindings**.
5. In the **Site Bindings** dialog box, under **Type**, select **https** and then click **Edit**. In the **Host name** text box, type **nls.adatum.com**. In the **SSL Certificate** list, click the **nls.adatum.com** certificate, click **OK**, and then click **Close**.
6. Close the **Internet Information Services (IIS) Manager** console.



**Note:** The client will use the HTTPS bindings that you configure for the host name **nls.adatum.com**, to determine the network location in the DirectAccess scenario.

### Configure the DirectAccess server with the appropriate certificate

1. Switch to **EU-RTR**.
2. Right-click **Start**, and then click **Windows PowerShell**.
3. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
mmc
```

5. In the **MMC**, click **File**, and then click **Add/Remove Snap-in**.
6. In the **Available snap-ins** list, click **Certificates**, and then click **Add**.
7. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.

8. In the **Select Computer** dialog box, click **Local computer**, click **Finish**, and then click **OK**.
9. In the Certificates snap-in, in the console tree, expand **Certificates (Local Computer)**, expand **Personal**, and then expand **Certificates**.
10. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
11. Click **Next** twice.
12. On the **Request Certificates** page, click **Adatum Web Certificate**, and then click **More information is required to enroll for this certificate**.
13. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, select **Common name** as **Type**.
14. In the **Value** text box, type **131.107.0.10**, and then click **Add**.
15. Click **OK**, click **Enroll**, and then click **Finish**.
16. In the Certificates snap-in, in the details pane, verify that a new certificate with the name **131.107.0.10** is issued with **Intended Purposes** of **Server Authentication**.
17. Right-click the certificate, and then click **Properties**.
18. In the **Properties** dialog box, in the **Friendly name** text box, type **IP-HTTPS Certificate**, and then click **OK**.
19. Close the window, and If prompted to save the settings, click **No**.



**Note:** Instead of issuing a certificate with the IP address in the subject name, in a real environment you will use the fully qualified domain name (FQDN) of the Internet-facing server that will be reachable by the external client.

### Create a CRL distribution point on EU-RTR

1. Open **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In the **Internet Information Services (IIS) Manager** console, in the left pane, click **EU-RTR (Adatum\Administrator)**.
4. In the console tree, expand **EU-RTR**, expand **Sites**, and then expand **Default Web Site**.
5. Right-click **Default Web Site**, and then click **Add Virtual Directory**.
6. In the **Add Virtual Directory** dialog box, in the **Alias** text box, type **CRLD**.
7. Next to **Physical path**, click the **ellipsis** button.
8. In the **Browse for Folder** dialog box, click **Local Disk (C:)**, and then click **Make New Folder**.
9. In the **Name** text box, type **CRLDist**, and then press Enter.
10. In the **Browse for Folder** dialog box, click **OK**.
11. In the **Add Virtual Directory** dialog box, click **OK**.
12. In the middle pane of the console, double-click **Directory Browsing**, and then in the **Actions** pane, click **Enable**.
13. In the left pane, click the **CRLD** folder.
14. In the **Internet Information Services (IIS) Manager** console, in the middle pane, under the **Management** section, double-click the **Configuration Editor** icon.



15. Click the **Section** drop-down list box, and navigate to **system.webServer\security\RequestFiltering**.
16. In the middle pane of the console, double-click the **allowDoubleEscaping** entry to change the value from **False** to **True**.
17. In the **Actions** pane, click **Apply**.
18. Close **Internet Information Services (IIS) Manager**.




**Note:** You need to modify the value of **allowDoubleEscaping** to allow clients to access CRL deltas that will have a plus (+) sign appended to the filename.


### Share and secure the CRL distribution point

1. On the taskbar, click the **File Explorer** icon.
2. In **File Explorer**, expand **This PC** and then click **Local Disk (C:)**.
3. In the details pane, right-click the **CRLDist** folder, and then click **Properties**.
4. In the **CRLDist Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
5. In the **Advanced Sharing** dialog box, click **Share this folder**.
6. In the **Share name** text box, type a dollar sign (\$) at the end so that the share name is **CRLDist\$**.
7. In the **Advanced Sharing** dialog box, click **Permissions**.
8. In the **Permissions for CRLDist\$** dialog box, click **Add**.
9. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
10. In the **Object Types** dialog box, click **Computers**, and then click **OK**.
11. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **LON-DC1**, click **Check Names**, and then click **OK**.
12. In the **Permissions for CRLDist\$** dialog box, in the **Group or user names** list, click **LON-DC1 (ADATUM\LON-DC1\$)**.
13. In the **Permissions for LON-DC1** area, under **Full control**, click **Allow**, and then click **OK**.
14. In the **Advanced Sharing** dialog box, click **OK**.
15. In the **CRLDist Properties** dialog box, click the **Security** tab.
16. On the **Security** tab, click **Edit**.
17. In the **Permissions for CRLDist** dialog box, click **Add**.
18. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
19. In the **Object Types** dialog box, click **Computers**, and then click **OK**.
20. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **LON-DC1**, click **Check Names**, and then click **OK**.
21. In the **Permissions for CRLDist** dialog box, in the **Group or user names** list, click **LON-DC1 (ADATUM\LON-DC1\$)**.
22. In the **Permissions for LON-DC1** area, under **Full control**, click **Allow**, and then click **OK**.


23. In the **CRLDist Properties** dialog box, click **Close**.
24. Close the **File Explorer** window.

 **Note:** The following steps will make the CRL distribution point available for external clients. Internal clients will still have the option to connect to the CRL either by using a Lightweight Directory Access Protocol (LDAP) query to AD DS, or by accessing the file share from the internal network adapter on **EU-RTR**.

### Publish the CRL to EU-RTR

 **Note:** These steps make the CRL available on the edge server for Internet-based DirectAccess clients.

1. Switch to **LON-DC1**.
2. In **Server Manager**, click **Tools**, and then click **Certification Authority**.
3. In the **Certification Authority** console tree, expand **AdatumCA**, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.
4. In the **Publish CRL** dialog box, click **New CRL**, and then click **OK**.
5. On the taskbar, click the **File Explorer** icon.
6. In **File Explorer**, in the address bar, type **\\EU-RTR\CRLDist\$**, and then press Enter.
7. In the **File Explorer** window, notice the **AdatumCA** files.
8. Close the **File Explorer** window.


 **Note:** If you receive an error while publishing the certificate, it is because either you did not enter the extensions for CRL in the CA properly, or you did not grant appropriate permission for **LON-DC1** computer account on the **\\EU-RTR\CRLDIST\$** share.

**Results:** After completing this exercise, you should have prepared the environment for implementing advanced DirectAccess infrastructure.

## Exercise 2: Implementing the advanced DirectAccess infrastructure

### ► Task 1: Modify the DirectAccess deployment

#### Reset the DirectAccess configuration

 **Note:** The steps in this section is only required because Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

1. On **EU-RTR**, in **Server Manager**, click **Tools**, and then click **Remote Access Management**.

2. In the **Remote Access Management Console**, click **DirectAccess and VPN**, and then under **Tasks**, click **Remove Configuration Settings**. When prompted by the **Confirm Remove Configuration**, click **OK**.
3. Wait for the **Removing Configuration Settings Wizard** to complete and then click **Close**.
4. In the **Remote Access Management** console, click **Run the Getting Started Wizard**.
5. In the **Getting Started Wizard**, on the **Configure Remote Access** page, click **Deploy DirectAccess only**.
6. Verify that **Edge** is selected and that **131.107.0.10** is listed in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** text box. Then click **Next**.
7. On the **Configure Remote Access** page, click the **here** link.



**Note:** Ensure that you click the here link to display an additional window for configuring 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 listed: **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**.
12. Verify that **DirectAccessClients** displays, and then click **OK**.
13. Clear the **Enable DirectAccess for mobile computers only** check box, and then click **Next**.
14. On the **DirectAccess Client Setup** page, fill out the following information, and then click **Finish**:
  - o Helpdesk email address: **DAHelp@adatum.com**
  - o DirectAccess connection name: **A. Datum DirectAccess**
15. On the **Remote Access Review** page, click **OK**.
16. On the **Configure Remote Access** page, click **Finish** and wait for the configuration to complete.
17. In the **Applying Getting Started Wizard Settings** dialog box, verify that the configuration was applied successfully with warnings, and then click **Close**.



**Note:** You might receive the following warning, **"To deploy a network load balancing cluster or multisite deployment, obtain a certificate for the network location server with a subject name that is different from the internal name of the Remote Access server."** This warning can be safely ignored.

### Configure the Remote Access server role

1. On **EU-RTR**, in **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. In the **Remote Access Management Console**, click **DirectAccess and VPN**.
3. To select which clients will use DirectAccess, in the central pane, under **Step 1**, click **Edit**.
4. On the **Deployment Scenario** page, click **Next**.

5. On the **Select Groups** page, verify that the DirectAccessClients (ADATUM\DirectAccessClients) group is listed, and then click **Next**.
6. On the **Network Connectivity Assistant** page, under the **Resource** column, delete the existing record by right-clicking on the arrow and then clicking **Delete**.
7. Under the **Resource** column, double-click the empty row.
8. On the **Configure Corporate Resources for NCA** page, verify that **HTTP** is selected, and then in the box next to **HTTP**, type **https://nls.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 then click **Next**.
13. On the **Network Adapters** page, verify that **Use a self-signed certificate created automatically by DirectAccess** is not selected, and that **CN=131.107.0.10** is listed. Then click **Next**.
14. On the **Authentication** page, click **Use computer certificates**.
15. Click **Browse**, click **AdatumCA**, and then click **OK**.
16. On the **Authentication** page, click **Enable Windows 7 client computers to connect via DirectAccess**, and then click **Finish**.



**Note:** You need to enable certificate authentication with the certificates issued from a trusted CA to support Windows 7 clients.

17. In the **Remote Access Setup** pane, under **Step 3**, click **Edit**.
18. On the **Network Location Server** page, click **The network location server is deployed on a remote web server (recommended)**.
19. In the **Type in the URL of the network location server** text box, type **https://nls.adatum.com**, and then click **Validate**.
20. Ensure that the URL is validated, and then click **Next**.
21. On the **DNS** page, double-click an empty row below **nls.adatum.com**.
22. In the **DNS suffix** box, type **crl.adatum.com**, click **Apply** to add an entry in the Name Resolution Policy Table (NRPT), and then click **Next**.
23. On the **DNS Suffix Search List** page, click **Next**.
24. On the **Management** page, click **Finish**.
25. Under **Step 4**, click **Edit**.
26. On the **DirectAccess Application Server Setup** page, click **Finish**.
27. In the central pane, click **Finish** to apply the changes.
28. In the **Remote Access Review** window, click **Apply**.
29. In the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

### ► Task 2: Verify the server and GPO configuration

1. On **EU-RTR**, right-click **Start**, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type the following commands, pressing Enter at the end of each line:

```
gpupdate /force
Ipconfig
```

3. Verify that **EU-RTR** has an IPv6 address for **Tunnel adapter IPHTTPSInterface** that starts with **2002**.

**Results:** After completing this exercise, you should have implemented the advanced DirectAccess infrastructure.

## Exercise 3: Validating the DirectAccess deployment

### ► Task 1: Verify Windows 10 client connectivity

#### Verify DirectAccess Group Policy configuration settings for Windows 10 clients

1. Switch to **LON-CL2**.
2. Right-click the **Start** button, click **Shut down or sign out**, and then click **Restart**.



**Note:** You must restart the **LON-CL2** machine because you added the machine account to the DirectAccess Clients security while the machine was running. In order to update the machine's security token, it must restart.

3. After **LON-CL2** has restarted, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.
4. Right-click **Start**, and then click **Run**.
5. In the **Run** box, type **cmd** and then press Enter.
6. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpresult /R
```

7. Review the output of the command.
8. Under the **COMPUTER SETTINGS** section, verify that the DirectAccess Client Settings GPO is applied.



**Note:** If the DirectAccess Client Settings GPO is not applied, restart **LON-CL2**, and then sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.

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

```
Netsh name show effectivepolicy
```

10. Verify that following message displays: "DNS Effective Name Resolution Policy Table Settings. Note: DirectAccess settings are inactive when this computer is inside a corporate network."

### Verify client computer certificate distribution

1. On **LON-CL2**, at a command prompt, type the following command, and then press Enter:

```
mmc
```

2. In the **MMC**, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Available snap-ins** list, click **Certificates**, and then click **Add**.
4. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, click **Local computer**, click **Finish**, and then click **OK**.
6. In the Certificates snap-in, in the console tree, navigate to **Certificates (Local Computer) \Personal\Certificates**.
7. In the details pane, verify that a certificate with the name **LON-CL2.adatum.com** displays with the **Intended Purposes** of **Client Authentication** and **Server Authentication**.
8. Close the console window.
9. When you are prompted to save the settings, click **No**.

### Verify internal network access

1. On **LON-CL2**, on the taskbar, click the **Internet Explorer** icon.
2. In the Internet Explorer Address bar, type **http://lon-svr1.adatum.com**, and then press Enter.
3. Verify that the default IIS 9.0 webpage for **LON-SVR1** displays.
4. Right-click **Start**, and then click **Run**.
5. In the **Run** box, type **\\LON-SVR1\Corpdata**, and then press Enter.



**Note:** Note that you are able to access the folder content.

6. Close all open windows.
7. Right-click **Start**, and then click **Run**.
8. In the **Run** box, type **cmd**, and then press Enter.
9. In the **Command Prompt** window, type **ipconfig**, and then press Enter.



**Note:** Notice that you receive information about the Ethernet adapter and Tunnel adapter isatap. This is because **LON-CL2** is connected directly to the internal network and is not using DirectAccess.


### Move the client computer to the Internet virtual network

1. To move the client from the internal network to the Internet, on **LON-CL2**, right-click **Start**, 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**.


## Verify connectivity to the DirectAccess server

1. On **LON-CL2**, open a **Command Prompt** window, type the following command, and then press Enter:

```
ipconfig
```

 **Note:** Notice the IPv6 address that starts with 2002. This is an IP-HTTPS address. If there is no IP address for iphttpsinterface, type the following commands, restart the computer, and then repeat step 1:

```
Netsh interface teredo set state disabled  
Netsh interface 6to4 set state disabled
```

 **Note:** In this lab setup, IP-HTTPS connectivity on the firewall is enabled and other connectivity methods from the client—such as the Teredo or 6to4 tunneling protocol—are disabled. If you are planning to use the Teredo or 6to4 tunneling protocol in the production environment, you should not disable them.

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

```
Netsh name show effectivepolicy
```

3. Verify that DNS Effective Name Resolution Policy Table Settings displays three entries for **adatum.com**, **crl.adatum.com**, and **nls.adatum.com**.
4. At the command prompt, type the following command, and then press Enter:


```
powershell
```

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

```
Get-DAClientExperienceConfiguration
```

6. Review the DirectAccess client settings that are returned.
7. On **LON-CL2**, click **Start**, and then click **Settings**.
8. In **Settings**, select **Network & Internet**, and then click **DirectAccess**.
9. Under **Location**, verify that **Your PC is set up correctly for single-site DirectAccess** displays.
10. Notice the **Collect** button under **Troubleshooting info**.

## Verify connectivity to the internal network resources

 **Note:** You may not be able to connect to the internal file share, the internal Web site, ping lon-dc1 or run gpupdate since Direct Access is not fully functional in Windows Server 2016 TP5. This issue will be resolved in Windows Server 2016 RTM.

1. On the taskbar, click the **Internet Explorer** icon.
2. In Internet Explorer, in the Address bar, type **http://lon-svr1.adatum.com**, and then press Enter.
3. Verify that the default IIS 9.0 webpage for **LON-SVR1** appears.

4. Leave the **Internet Explorer** window open.
5. On the taskbar, click the **File Explorer** icon.
6. In **File Explorer**, in the address bar, type `\\LON-SVR1\CorpData`, and then press Enter.



**Note:** You are able to open `http://lon-svr1.adatum.com` and `\\lon-svr1\CorpData` because there is a record in NRPT that resolves any internal namespace from adatum.com by using the internal DNS server.

7. Switch to the **Command Prompt** window.
8. At the command prompt, type the following command, and then press Enter:

```
ping lon-dc1.adatum.com
```

9. Verify that you are receiving replies from **lon-dc1.adatum.com**.
10. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

11. Close all open windows.
12. Switch to **EU-RTR**.
13. On the taskbar, click the **Remote Access Management** icon.
14. In the **Remote Access Management Console** tree, click **Remote Client Status**.
15. Notice that **LON-CL2** is connected via IP-HTTPS.
16. In the **Connection Details** pane, in the bottom-right corner of the screen, note that **Machine Certificate & User Ntlm** are in use.
17. Close all open windows.

#### ► Task 2: Monitor client connectivity

1. On **EU-RTR**, open the **Remote Access Management Console**, and then in the left pane, click **Dashboard**.
2. Review the information in the central pane, under **DirectAccess** and **VPN Client Status**.
3. In the left pane, click **Remote Client Status**, and then in the central pane, review the information under the **Connected Clients** list.
4. In the left pane, click **Reporting**, and then in the central pane, click **Configure Accounting**.
5. In the **Configure Accounting** window, under **Select Accounting Method**, click **Use inbox accounting**, click **Apply**, and then click **Close**.
6. In the central pane, under **Remote Access Reporting**, review the options for monitoring historical data.

**Results:** After completing this exercise, you should have verified that a Windows 10 client can connect to the internal network by using DirectAccess.



► **Task 3: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for: **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-INET1**, **20741A-LON-CL1**, and **20741A-LON-CL2**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

## Module 8: Implementing VPNs

# Lab: Implementing VPN

### Exercise 1: Implementing VPN

#### ► Task 1: Verify certificate requirements for IKEv2 and SSTP

##### 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 a certificate for EU-RTR

1. On **EU-RTR**, click **Start**, and then type **Command Prompt**. In the results pane, click **Command Prompt**.
2. At the command prompt, 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 Certificate**, 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, 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 are prompted 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 Bindings** dialog box, under the **Type** select **https**, 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.

### ► Task 2: Review the default VPN configuration

1. On **EU-RTR**, in the **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 prompted, 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 prompted, 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 Secure Socket Tunneling Protocol (SSTP), Internet Key Exchange version 2 (IKEv2), Point to Point Tunneling Protocol (PPTP), and Layer Two Tunneling Protocol (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, 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 the 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 prompted, click **Yes**.

### ► Task 3: 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.

**Results:** After completing this exercise, you should have modified the Remote Access server configuration successfully to provide VPN connectivity.

## Exercise 2: Validating the VPN deployment

### ► Task 1: Remove the client computer from the domain

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **System**.
3. In the **System** window, click **Advanced system settings**, and then click the **Computer Name** tab.
4. On the **Computer name** tab, click **Change**.

5. In the **Computer Name/Domain Changes** dialog box, click **Workgroup**, in the **Workgroup** text box type **WORKGROUP**, and then click **OK**.
6. In the **Computer Name/Domain Changes** dialog box, click **OK**.
7. In the **Welcome to the WORKGROUP workgroup** dialog box, click **OK**.
8. To restart the computer, click **OK**.
9. To close **System Properties** dialog box, click **Close**.
10. Click **Restart Now**.

### ► Task 2: Move LON-CL1 to the Internet

1. When the **LON-CL1** computer has restarted, sign in with the user name **Admin** and the password **Pa\$\$w0rd**.
2. When prompted by the **Networks** dialog box, click **Yes**.
3. Right-click **Start**, and then click **Network Connections**.
4. In the **Network Connections** window, right-click **London\_Network**, and then click **Disable**.
5. Right-click **Internet**, and then click **Enable**.
6. Right-click **Internet**, and then click **Properties**.
7. In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, ensure that the following settings display, and then click **OK**:
  - IP address: **131.107.0.20**
  - Subnet mask: **255.255.255.0**
  - Preferred DNS server: **131.107.0.100**
9. In the **Internet Properties** dialog box, click **Cancel**.
10. Close all open windows.
11. On the **taskbar**, click the **File Explorer** icon.
12. In **File Explorer**, in the address bar, type **\\Lon-DC1\**, and then press Enter. Notice that a Network Error message displays.
13. Close all open windows.



**Note:** The client is unable to open the resources, because it is not on the internal network.

### ► Task 3: Configure a VPN connection and verify connectivity

#### Create a VPN profile

1. On **LON-CL1**, right-click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **Network and Internet**, and then click **Network and Sharing Center**.
3. In **Network and Sharing Center**, click **Set up a new connection or network**.
4. In the **Choose a connection option** window, click **Connect to a workplace**. Click **Next**.
5. On the **How do you want to connect?** page, click **Use my Internet connection (VPN)**.

6. On the **Do you want to set up an Internet connection before continuing?** page, click **I'll set up an Internet connection later**.
7. On the **Type the Internet address to connect to** page, configure the following settings, and then click **Create**:
  - o Internet address: **131.107.0.10**
  - o Destination name: **A. Datum VPN**
  - o Allow other people to use this connection: **selected**
8. In **Network and Sharing Center**, click **Change adapter settings**.
9. In the **Network Connections** window, right-click **A. Datum VPN**, and then select **Connect / Disconnect**.
10. On the **VPN** page, select **A. Datum VPN**, and then click **Connect**.
11. In the **Sign in** dialog box, in the **User name** text box, type **adatum\logan**, and in the **Password** text box, type **Pa\$\$w0rd**, and then click **OK**.
12. Switch to the **Network Connections** window.
13. In the **Network Connections** window, verify that **WAN Miniport (PPTP)** displays under **A. Datum VPN**.



**Note:** By default, the client will attempt to connect to the VPN server by using a secure connection, such as L2TP with IPsec, IKEv2, or SSTP. In this case, however, because the client does not have a computer certificate or a preshared key, the client could not establish an L2TP or IKEv2 connection. Additionally, the client could not establish an SSTP connection because this connection requires that the client trusts the certificate on the VPN server. Therefore, the only possible connection in this case is PPTP with the CHAP v2 authentication.

### Export a root CA certificate

1. Switch to **LON-DC1**.
2. Click **Start**, and then click the **Server Manager** tile.
3. In **Server Manager**, click **Tools**, and then click **Certification Authority**.
4. In the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.
5. In the **AdatumCA Properties** dialog box, on the **General** tab, click **View Certificate**.
6. In the **Certificate** window, click the **Details** tab, and then click **Copy to File**.
7. In the **Certificate Export Wizard**, click **Next**.
8. On the **Export file format** page, verify that **DER encoded binary x.509 (.CER)** is selected, and then click **Next**.
9. In the **File Name** text box, type **c:\AdatumRootCA.cer**, and then click **Next**. Click **Yes** at the prompt.
10. Click **Finish** to close the **Certificate Export Wizard**.
11. Click **OK** three times, and then close the **Certification Authority** console.

### Import a root CA certificate on a client

1. Switch to **LON-CL1**.
2. On the desktop, on the **taskbar**, click the **File Explorer** icon.
3. In the **This PC** window, in the address bar, type **\\172.16.0.10\C\$\** and then press Enter.
4. In the **Windows Security** dialog box, click **Use another account**.
5. When prompted for the username, type **Adatum\Administrator**, for the password, type **Pa\$\$w0rd**, and then press Enter.
6. In the **File Explorer** window, right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
7. In the **Open File – Security Warning** dialog box, click **Open**.
8. On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
9. In the **User Account Control** dialog box, click **Yes**.
10. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
11. On the **Certificate Store** page, click **Next**, and then click **Finish**.
12. In the **Certificate Import Wizard**, click **OK**.
13. Right-click **Start**, and click **Command Prompt**.
14. In the **Command Prompt** window, type **mmc**, and then press Enter.
15. In the **User Account Control** dialog box, click **Yes**.
16. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
17. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
18. In the **Certificates snap-in** dialog box, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
19. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
20. Verify that **AdatumCA** exists.



**Note:** You perform the above steps to import the **AdatumCA** certificate into the Trusted Root Certification Authorities store on **LON-CL1** and to verify that the **AdatumCA** certificate is imported into Trusted Root Certification Authorities of **LON-CL1**. This enables the clients to trust the certificate on the VPN server and to establish a VPN connection by using the SSTP protocol.

### Connect to VPN by using IKEv2 and SSTP

1. Switch to **Network Connections** and right-click **A. Datum VPN**, and then click **Properties**.
2. In the **A. Datum VPN Properties** dialog box, click the **Security** tab.
3. In the **Type of VPN** list, click **IKEv2**, and then click **Use Extensible Authentication Protocol (EAP)**.
4. Click **OK** twice.



5. In the **Network Connections** window, double-click the **A. Datum VPN** icon, and then click **Disconnect**.
6. In the **Network Connections** window, right click **A. Datum VPN**, and then click **Connect / Disconnect**.
7. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
8. If the **Network sign-in** dialog box appears, in the **User name** box, type **Adatum\logan**, in the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
9. Switch to the **Network Connections** window, and then verify that the connection is established by using the IKEv2 protocol.
10. In the **Network Connections** window, right-click **A. Datum VPN**, and then click **Properties**.
11. In the **Properties** dialog box, click the **Security** tab.
12. In the **Type of VPN** list, click **Secure Socket Tunneling Protocol (SSTP)**, and then click **Use Extensible Authentication Protocol (EAP)**.
13. Click **OK** twice.
14. In the **Network Connections** window, double-click the **A. Datum VPN** icon, and then click **Disconnect**.
15. In the **Network Connections** window, double-click the **A. Datum VPN** icon.
16. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
17. If the **Network sign-in** dialog box displays, in the **User name** box, type **Adatum\logan**, in the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
18. Switch to the **Network Connections** window, and then verify that the connection is established by using the **SSTP** protocol.



**Note:** Do not disconnect the A. Datum VPN connection.

#### ► Task 4: Sign in to the domain by using VPN

1. On **LON-CL1**, right-click **Start**, and then click **Command Prompt**.
2. In the **Command prompt** window, type **mmc**, and then press Enter. Click **Yes** at the User Account Control prompt.
3. In the **Console** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Group Policy Object Editor**, and then click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Finish**.
6. In **Add or Remove Snap-in** window, click **OK**.
7. In the **Console** window, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
8. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**.
9. In the **Interactive logon: Do not require CTRL+ALT+DEL Properties** window, select **Enabled**, and then click **OK**.
10. Close the **Console** window and do not save changes.

11. Right-click **Start**, and then click **System**.
12. In the **System** window, click **Advanced system settings**, and then click the **Computer Name** tab.
13. On the **Computer name** tab, click **Change**.
14. In the **Computer Name/Domain Changes** dialog box, click **domain**, in the **Domain** text box, type **adatum.com**, and then click **OK**.
15. In the **Windows Security** dialog box, type **adatum\administrator** in the **User name** text box and **Pa\$\$w0rd** in the **Password** text box, and then click **OK**.
16. In the **Welcome to the adatum.com domain** dialog box, click **OK**.
17. In the **Computer Name/Domain Changes** dialog box, click **OK**.
18. To close the **System Properties** dialog box, click **Close**.
19. Click **Restart Now**.

► **Task 5: Verify connectivity**

1. When **LON-CL1** has restarted, press Ctrl+Alt+End.
2. On the **sign-in** screen, click the **Network sign-in** icon.
3. On the **Network sign-in** screen, sign with the user name **Adatum\logan** and the password **Pa\$\$w0rd**.



**Note:** You now are signed in to the domain via the VPN connection.

4. Sign out of **LON-CL1**.

**Results:** After completing this exercise, you should have verified that the clients that cannot connect by using DirectAccess now can connect by using VPN, and that they can use Network Sign-in to sign in directly to the domain.

### Exercise 3: Troubleshoot VPN access

► **Task 1: Read the help-desk incident record for incident IN24578**

- Read the help-desk incident record IN24578 under the Exercise Scenario.

► **Task 2: Update the Plan of Action section of the incident record**

1. Read the **Additional Information** section of the incident record in the Student Handbook exercise scenario.
2. Update the **Plan of Action** section of the incident record with your recommendations:
  - Visit Logan's computer.
  - Try to connect to the VPN by using the A. Datum VPN profile.
  - Document the error message when connection.
  - Fix the connection issue and test the connection.

► **Task 3: Try to connect by using the A. Datum VPN connection on Logan's computer (LON-CL1)**

1. On **LON-CL1**, sign in with the user name **.\Admin** and the password **Pa\$\$w0rd**.
2. If prompted by the **Networks** dialog box, click **Yes**.
3. On **LON-CL1**, right-click **Start**, and then click **Command Prompt (Admin)**. When prompted by **User Account Control (UAC)**, click **Yes**.
4. At the command prompt, type the following command, and then press Enter:

```
cd C:\Labfiles\Mod08\
```

5. At the command prompt, type the following commands, and then press Enter after each one.

```
PowerShell
.\Mod8LabB.ps1
```

6. Wait for the script to complete.
7. At the command prompt type **.\Mod8LabB.ps1** to run the script a second time.
8. Wait for the script to complete.
9. Right-click **Start**, and then click **Network Connections**.
10. In the **Network Connections** window, double-click the **A. Datum VPN** icon.
11. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
12. If the **Network sign-in** dialog box displays, in the **User name** text box, type **Adatum\logan**, and in the **Password** text box, type **Pa\$\$w0rd**, and then click **OK**.
13. Wait for the connection to fail, and then write down the error message in the **Plan of Action** section of the incident record in the Student Handbook. (If the connection is successful, disconnect and then re-attempt the connection. It should fail.)

► **Task 4: Implement the fix, and test the solution**

1. On **LON-CL1**, click the **File Explorer** icon.
2. In the **This PC** window, in the address bar, type **\\172.16.0.10\C\$\**, and then press Enter.
3. In the **Windows Security** dialog box, click **Use another account**. When prompted, type **Adatum\Administrator** in the **User name** text box, type **Pa\$\$w0rd** in the **Password** text box, and then press Enter.
4. In the **File Explorer** window, right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
5. In the **Open File – Security Warning** dialog box, click **Open**.
6. On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
7. In the **User Account Control** dialog box, click **Yes**.
8. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
9. On the **Certificate Store** page, click **Next**, and then click **Finish**.
10. In the **Certificate Import Wizard**, click **OK**.
11. Right-click **Start**, and then click **Command Prompt**.

12. In the **Command Prompt** window, type **mmc**, and then press Enter.
13. In the **User Account Control** dialog box, click **Yes**.
14. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
15. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
16. In the **Certificates snap-in** dialog box, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
17. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
18. Verify that **AdatumCA** exists.
19. In the **Network Connections** window, double-click the **A. Datum VPN** icon.
20. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
21. In the **Network sign-in** dialog box, in the **User name** text box, type **Adatum\logan**, in the **Password** text box, type **Pa\$\$w0rd**, and then click **OK**.
22. Verify that you are now able to connect to the **A. Datum** VPN server.

**Results:** After completing this exercise, you should have resolved the VPN access issue successfully, and Logan should be able to connect to the A. Datum VPN.

#### ► Task 5: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-SVR1**, **20741A-EU-RTR**, **20741A-INET1**, and **20741A-LON-CL1**.

## Module 9: Implementing networking for branch offices

# Lab A: Implementing DFS for branch offices

### Exercise 1: Implementing DFS

#### ► Task 1: Install the DFS role on LON-SVR1 and TOR-SVR1

1. Switch to **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**, 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 on **TOR-SVR1**.

#### ► Task 2: Create the BranchDocs DFS Namespace

1. Switch to **LON-SVR1**.
2. In **Server Manager**, click **Tools**, and then click **DFS Management**.
3. In the **navigation** pane, 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, under **Name**, type **BranchDocs**, and then click **Next**.
7. On the **Namespace Type** page, ensure that **Domain-based namespace** is selected. Take note that the namespace will be accessed by **\\Adatum.com\BranchDocs**.
8. Ensure that the **Enable Windows Server 2008 mode** check box is selected, and then click **Next**.
9. On the **Review Settings and Create Namespace** page, click **Create**.
10. In the **New Namespace Wizard** window, click **Close**.

#### ► Task 3: Add the DataFiles folder to the BranchDocs namespace

1. On **LON-SVR1**, in **DFS Management**, right-click **Adatum.com\BranchDocs**, and then click **New Folder**.
2. In the **New Folder** dialog box, under **Name**, type **DataFiles**, and then click **Add**.
3. In the **Add Folder Target** dialog box, type **\\LON-SVR1\DataFiles**, and then click **OK**.
4. In the **Warning** dialog box, click **Yes**.

5. In the **Create Share** dialog box, in the **Local path of shared folder** box, type **C:\BranchDocs\DataFiles**.
6. Click **All users have read and write permissions**, and then click **OK**. The permissions will be configured later.
7. In the **Warning** dialog box, click **Yes**.
8. To close the **New Folder** dialog box, click **OK**.

► **Task 4: Create a folder target for DataFiles on TOR-SVR1**

1. On **LON-SVR1**, in **DFS Management**, expand **Namespaces**, **Adatum.com\BranchDocs**, and then click **DataFiles**.
2. In the **details** pane, notice that there is currently only one folder target.
3. Right-click **DataFiles**, and then click **Add Folder Target**.
4. In the **New Folder Target** dialog box, under **Path to folder target**, type **\\TOR-SVR1\DataFiles**, and then click **OK**.
5. To create the shared folder on **TOR-SVR1**, in the **Warning** dialog box, click **Yes**.
6. In the **Create Share** dialog box, under **Local path of shared folder**, type **C:\BranchDocs\DataFiles**.
7. In the **Create Share** dialog box, under **Shared folder permissions**, select **All users have read and write permissions**, and then click **OK**.
8. To create the folder on **TOR-SVR1**, in the **Warning** dialog box, click **Yes**.
9. In the **Replication** dialog box, click **Yes**. The **Replicate Folder Wizard** starts.

► **Task 5: Configure replication for the namespace**

1. In **DFS Management**, 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, click **Next**.
3. On the **Primary Member** page, select **LON-SVR1**, and then click **Next**.
4. On the **Topology Selection** page, select **No topology**, and then click **Next**.
5. In the **Warning** dialog box, click **OK**.
6. On the **Review Settings and Create Replication Group** page, click **Create**.
7. On the **Confirmation** page, click **Close**.
8. In the **Replication Delay** dialog box, click **OK**.
9. In the **DFS Management** console, expand **Replication**, and then click **Adatum.com\BranchDocs\DataFiles**.
10. In the **Action** pane, click **New Topology**.
11. In the **New Topology Wizard**, on the **Topology Selection** page, click **Full mesh**, and then click **Next**.
12. On the **Replication Group Schedule and Bandwidth** page, click **Next**.
13. On the **Review Settings and Create Topology** page, click **Create**.

14. On the **Confirmation** page, click **Close**, and in the **Replication Delay** dialog box, click **OK**.
15. In the **details** pane, on the **Memberships** tab, verify that the replicated folder displays on both **TOR-SVR1** and **LON-SVR1**.

**Results:** Upon completion of this exercise, you will have implemented DFS.

## Exercise 2: Validating the deployment

### ► Task 1: Verify DFSR functionality for TOR-SVR1

1. On **LON-SVR1**, on the taskbar, click the **File Explorer** icon.
2. In **File Explorer**, in the address bar, type **\\Adatum.com\BranchDocs\Datafiles**, and then press Enter.
3. In **File Explorer**, right-click in the empty space in the details pane, click **New**, and then click **Text Document**.
4. Type **Repltest**, and then press Enter.
5. In **File Explorer**, in the address bar, type **C:\BranchDocs\Datafiles**, and then press Enter. Confirm that the **Repltest.txt** file is located in the folder.
6. Switch to **TOR-SVR1**.
7. In **File Explorer**, in the address bar, type **C:\BranchDocs\Datafiles**, and then press Enter. Confirm that the **Repltest.txt** file is located in the folder.



**Note:** If **Repltest.txt** does not appear within 1 minute or even after refreshing the view, restart **TOR-SVR1**.

**Results:** Upon completion of this exercise, you will have validated the deployment of DFS in branch offices.

# Lab B: Implementing BranchCache

## Exercise 1: Implementing BranchCache

### ► Task 1: Configure SYD-SVR1 to use BranchCache

1. Switch to **SYD-SVR1**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, 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, ensure that **Select server from the server pool** is selected, and then click **Next**.
6. 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.
7. In the **Add Roles and Features** pop-up window, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. Click **Close**.
11. On the taskbar, click the **Search the web and Windows** icon, in the **Search** box, type **gpedit.msc**, and then press Enter.
12. In the **Local Group Policy Editor** console, in the **navigation** pane, under **Computer Configuration**, expand **Administrative Templates**, expand **Network**, and then click **Lanman Server**.
13. In the **Lanman Server result** pane, in the **Setting** list, right-click **Hash Publication for BranchCache**, and then click **Edit**.
14. In the **Hash Publication for BranchCache** dialog box, click **Enabled**. In the **Hash publication actions** list, select the **Allow hash publication only for shared folders on which BranchCache is enabled** check box, and then click **OK**.
15. Close the **Local Group Policy Editor**.

### ► Task 2: Prepare a file share for BranchCache

1. On **SYD-SVR1**, on the taskbar, click the **File Explorer** icon.
2. In the **File Explorer** window, navigate to **Local Disk (C:)**.
3. In the **Local Disk (C:)** window, on the menu, click the **Home** tab, and then click **New Folder**.
4. Type **Share**, and then press Enter.
5. Right-click **Share**, and then click **Properties**.
6. In the **Share Properties** dialog box, on the **Sharing** tab, click **Advanced Sharing**.
7. In the **Advanced Sharing** dialog box, select the **Share this folder** check box, and then click **Caching**.
8. In the **Offline Settings** dialog box, select the **Enable BranchCache** check box, and then click **OK**.
9. In the **Advanced Sharing** dialog box, click **OK**.
10. In the **Share Properties** dialog box, click **Close**.



11. On the taskbar, click **Search the web and Windows** icon, in the **Search** box type **cmd**, and then press Enter.
12. At the command prompt, type the following command, and then press Enter.

```
Copy C:\windows\system32\mspaint.exe c:\share
```

13. Close the command prompt.
14. Close **File Explorer**.

### ► Task 3: Configure client firewall rules for BranchCache

1. Switch to **LON-DC1**.
2. In **Server Manager**, on the menu bar, click **Tools**, and then in the **Tools** drop-down list, click **Group Policy Management**.
3. In **Group Policy Management**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
4. In the **Group Policy Management Editor**, in the **navigation** pane, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Windows Firewall with Advanced Security**.
5. In the **Windows Firewall with Advanced Security** window, in the **navigation** pane, expand **Windows Firewall with Advanced Security**, and then click **Inbound Rules**.
6. In the **Group Policy Management Editor**, on the **Action** menu, click **New Rule**.
7. In the **New Inbound Rule Wizard**, on the **Rule Type** page, click **Predefined**, click **BranchCache – Content Retrieval (Uses HTTP)**, and then click **Next**.
8. On the **Predefined Rules** page, click **Next**.
9. To create the firewall inbound rule, on the **Action** page, click **Finish**.
10. In the **Group Policy Management Editor**, in the navigation pane, click **Inbound Rules**, and then on the **Action** menu, click **New Rule**.
11. On the **Rule Type** page, click **Predefined**, click **BranchCache – Peer Discovery (Uses WSD)**, and then click **Next**.
12. On the **Predefined Rules** page, click **Next**.
13. On the **Action** page, click **Finish**.
14. Close the **Group Policy Management Editor** and **Group Policy Management** console.

### ► Task 4: Install the BranchCache feature on LON-SVR1

1. On **LON-SVR1**, 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**, and then select the **BranchCache for Network Files** check box.
6. On the **Select server roles** page, click **Next**.
7. On the **Select features** page, click **BranchCache**, and then click **Next**.

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

► **Task 5: Start the BranchCache host server on LON-SVR1**

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

```
Enable-BCHostedServer -RegisterSCP
```

3. In the **Windows PowerShell** window, type the following cmdlet, and then press Enter:

```
Get-BCStatus
```

4. Ensure that **BranchCache** is enabled and running.

► **Task 6: Configure client computers to use BranchCache in the hosted cache mode**

1. Switch to **LON-DC1**.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, double-click the **Computers** container.
4. Right-click **LON-CL1**, and then click **Move**.
5. In the **Move** window, click **IT**, and then click **OK**.
6. Right-click **LON-CL2**, and then click **Move**.
7. In the **Move** window, click **IT**, and then click **OK**.
8. Close **Active Directory Users and Computers**.
9. In **Server Manager**, on the menu bar, click **Tools**, and then in the **Tools** drop-down list, click **Group Policy Management**.
10. In the **Group Policy Management** console, in the **navigation** pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **IT**, and then click **Create a GPO in this domain and link it here**.
11. In the **New GPO** window, type **BCClient**, and then click **OK**.
12. In the **Group Policy Management** console, in the **navigation** pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, expand **IT**, right-click **BCClient**, and then click **Edit**.
13. In the **Group Policy Management Editor**, in the **navigation** pane, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Network**, and then click **BranchCache**.
14. In the **BranchCache results** pane, in the **Setting** list, right-click **Turn on BranchCache**, and then click **Edit**.
15. In the **Turn on BranchCache** dialog box, click **Enabled**, and then click **OK**.
16. In the **BranchCache results** pane, in the **Setting** list, right-click **Enable Automatic Hosted Cache Discovery by Service Connection Point**, and then click **Edit**.
17. In the **Enable Automatic Hosted Cache Discovery by Service Connection Point** dialog box, click **Enabled**, and then click **OK**.
18. In the **BranchCache results** pane, in the **Setting** list, right-click **Configure BranchCache for network files**, and then click **Edit**.

19. In the **Configure BranchCache for network files** dialog box, click **Enabled**; in the **Type the maximum round trip network latency (milliseconds) after which caching begins** box, type **0**, and then click **OK**.



**Note:** This setting is used to simulate access from a branch office and is not typically required.

20. Close the **Group Policy Management Editor**.
21. Close the **Group Policy Management Console**.
22. Start **20741A-LON-CL1**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
23. On the taskbar, click **Search the web and Windows** icon, in the **Search** box, type **cmd**, and then press Enter.
24. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
netsh branchcache show status all
```

26. Verify that BranchCache is **Enabled** with status **Running** and that the options from Group Policy are applied. If the status is **Stopped**, repeat steps 14 and 15.
27. Restart **20741A-LON-CL2**, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
28. Click **Start**, and then type **cmd.exe**. Press Enter.
29. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
netsh branchcache show status all
```

31. Verify that BranchCache is **Enabled** with status **Running** and that the options from Group Policy are applied. If the status is **Stopped**, repeat steps 14 and 15.

**Results:** Upon completion of this exercise, you will have implemented BranchCache.

## Exercise 2: Validating the deployment


### ► Task 1: Simulate slow link to the branch office

1. On **SYD-SVR1**, on the Start screen, type **gpedit.msc**, and then press Enter.
2. In the **navigation** pane of the **Local Group Policy Editor** console, under **Computer Configuration**, expand **Windows Settings**, right-click **Policy-based QoS**, and then click **Create new policy**.


3. On the **Create a QoS policy** page of the **Policy-based QoS Wizard**, in the **Policy name** box, type **Limit to 100 KBps**, click the **Specify Outbound Throttle Rate** check box, type **100**, and then click **Next**.
4. On the **This QoS policy applies to** page, click **Next**.
5. On the **Specify the source and destination IP addresses** page, click **Next**.
6. On the **Specify the protocol and port numbers** page, click **Finish**.
7. Close the **Local Group Policy Editor**.

► **Task 2: Verify BranchCache functionality for SYD-SVR1**

1. Switch to **LON-CL1**.
2. In the **Search the web and Internet box**, type **perfmon**, and then press Enter.
3. In the **navigation** pane of the **Performance Monitor** console, under **Monitoring Tools**, click **Performance Monitor**.
4. In the **Performance Monitor result** pane, click the **Delete (Delete Key)** icon.
5. In the **Performance Monitor result** pane, click the **Add (Ctrl+N)** icon.
6. In the **Add Counters** dialog box, under **Select counters from computer**, click **BranchCache**, click **Add**, and then click **OK**.
7. Click the arrow to the right of **Change graph type**, and then click **Report**. Notice that the value of all performance statistics is zero.
8. Repeat steps 1 through 7 for **LON-CL2** and **LON-SVR1**.
9. Switch to **LON-CL1**.
10. On the taskbar, click the **File Explorer** icon.
11. In **File Explorer**, in the address bar, type **\\SYD-SVR1\Share**, and then press Enter.
12. In **File Explorer**, right-click **mspaint.exe**, and then click **Copy**.
13. In **File Explorer**, right-click **Desktop**, and then click **Paste**.

 **Note:** This file copy will take some time because of the 100-Kbps bandwidth limit placed on **SYD-SVR1**.


14. In **Performance Monitor**, click any counter, and then press Ctrl+A.
15. Right-click any counter, and then click **Scale selected. counters**.

 **Note:** Note that several counters are no longer at zero, which indicates that BranchCache is active.


16. Switch to **LON-SVR1**.
17. On **LON-SVR1**, switch to **Performance Monitor**, and then note that counter statistics reflect BranchCache activity on **LON-SVR1**.
18. On **LON-SVR1**, click the **Windows PowerShell** icon on the taskbar.

19. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
Get-BCStatus
```

 **Note:** Note that under **DataCache**, the **CurrentActiveCacheSize** value is 6560896 bytes, which is the size of mspaint.exe.

20. Switch to **LON-CL2**.
21. On **LON-CL2**, on the taskbar, click the **File Explorer** icon.
22. In **File Explorer**, in the address bar, type `\\SYD-SVR1\Share`, and then press Enter.
23. In **File Explorer**, right-click **mspaint.exe**, and then click **Copy**.
24. In **File Explorer**, right-click **Desktop**, and then click **Paste**.

 **Note:** Note that the file copy time is much faster than to **LON-CL1**, because the file is cached on **LON-SVR1**.

**Results:** Upon completion of this exercise, you will have validated the deployment of network services in branch offices.

### ► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-DC1**, **20741A-LON-SVR1**, **20741A-TOR-SVR1**, **20741A-SYD-SVR1**, **20741A-EU-RTR**, **20741A-LON-CL1**, and **20741A-LON-CL2**.

**MCT USE ONLY. STUDENT USE PROHIBITED**

# Module 10: Configuring advanced networking features

## Lab: Configuring advanced Hyper-V networking features

### Exercise 1: Creating and using Hyper-V virtual switches

#### ► Task 1: Verify the current Hyper-V network configuration

1. On **LON-HOST1**, if necessary, on the task bar, click **Hyper-V Manager**.
2. In Hyper-V Manager, in the **Actions** pane, click **Virtual Switch Manager**.
3. In the **Virtual Switch Manager for LON-HOST1** window, note the virtual switch, **Private Network**, that has been created for **LON-HOST1**.

#### ► Task 2: Create virtual switches

1. On **LON-HOST1**, in the **Virtual Switch Manager for LON-HOST1** window, in the console tree, select the **New virtual network switch** item, and then in the **details** pane, in the **What type of virtual switch do you want to create?** area, ensure that **External** is selected, and then click **Create Virtual Switch**.
2. In the **Name** box, type **External Switch**, and then click **OK**.
3. In the **Apply Network Changes** dialog box, click **Yes**.
4. The **Virtual Switch Manager** window closes. Open it again, and then note the **External Switch** that you just created.
5. Repeat steps 1–4 to create an internal switch named **Internal Switch**.
6. Open the **Virtual Switch Manager** again, and then note the **Internal Switch** that you just created.

#### ► Task 3: Create virtual network adapters

1. On **LON-SVR1**, right-click **Start**, point to **Shut down or sign out**, and then click **Shut down**.
2. In the **Shutdown** dialog box, click **Continue**. Wait until the virtual machine is completely shut down before continuing to the next step.
3. On **LON-HOST1**, click **Start**, and then click **Windows PowerShell**.
4. At the **Windows PowerShell** command prompt, type the following commands, and then press Enter after each line:

```
Add-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -Name "New Network Adapter"  
  
Connect-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -Name "New Network Adapter" -  
SwitchName "External Switch"
```

#### ► Task 4: Use the Hyper-V virtual switches

1. In Hyper-V Manager, in the **Virtual Machines** pane, right-click **20741A-LON-SVR1-B**, and then click **Settings**.
2. In the **Settings for 20741A-LON-SVR1-B on LON-HOST1** window, in the console tree, select the **New Network Adapter**.
3. Note that the virtual switch assigned is **External Switch**.
4. In the **Settings** window, click **Cancel**.

5. In the **Hyper-V Manager** console, right-click **20741A-LON-SVR1-B**, and then click **Start**.
6. Right-click **20741A-LON-SVR1-B**, and then click **Connect**.
7. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
8. In the **Networks** dialog box, click **Yes**.
9. If **Server Manager** is not already open, click **Start**, and then click **Server Manager**.
10. In the **Server Manager** console tree, select the **Local Server** node.
11. Click the hyperlink entitled **IPv4 address assigned by DHCP, IPv6 enabled** on the **Ethernet 2** line.
12. In the **Network Connections** window, right-click **Ethernet 2**, and then click **Status**.
13. In the **Ethernet 2 Status** window, click **Details**.
14. Note the IP address and other settings assigned to the network adapter. They should be external to your virtual machine environment.
15. Close all open windows and leave the **Server Manager** open.

#### ► Task 5: Add NIC Teaming

1. On **LON-SVR1** in the **Server Manager** console tree, select the **Local Server** node.
2. In the **Properties details** pane, next to **NIC Teaming**, click the **Disabled** hyperlink.
3. In the **NIC Teaming** dialog box, in the **Adapters and Interfaces** pane, select **Ethernet 2**, click **Tasks** and then click **Add to New Team**.
4. In the **New team** dialog box, in the **Team name** box, type **LON-SVR1 NIC Team**, select **Ethernet 2**, and then click **OK**.
5. In the **NIC Teaming** dialog box, in the **Teams** pane, note the following:
  - Team: **LON-SVR1 NIC Team**
  - Status: **OK**
  - Teaming Mode: **Switch Independent**
  - Load Balancing: **Address Hash**
  - Adapters: **1**



**Note:** 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 virtual local area networks (VLANs).

**Results:** After completing this exercise, you should have successfully configured the Hyper-V virtual switch.



## Exercise 2: Configuring and using the advanced features of a virtual switch

### ► Task 1: Configure the network adapters to use DHCP guarding

1. On **LON-HOST1**, open **Hyper-V Manager**.
2. In Hyper-V Manager, in the **Virtual Machines** pane, select and right-click **20741A-LON-SVR1-B**, and then click **Settings**.
3. In the **Settings for 20741A-LON- SVR1-B on LON-HOST1** window, in the console tree, select and then expand **Network Adapter**.
4. Under **Network Adapter**, click **Advanced Features**.
5. In the **details** pane, in the **DHCP guard** area, click **Enable DHCP guard**, and then click **OK**.
6. Repeat steps 2–5 for **20741A-LON-CL1-B**.

### ► Task 2: Configure and use DHCP guard

1. On **LON-CL1**, in the notification area of the taskbar, right-click the **Network** icon, and then click **Open Network and Sharing Center**.
2. In the **Network and Sharing Center** window, click the **Ethernet** hyperlink.
3. In the **Ethernet Status** window, click **Properties**.
4. In the **Ethernet Properties** window, in the **This connection uses the following items** section, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. Note that **LON-CL1** is using the following TCP/IP settings:
  - IP Address: **172.16.0.50**
  - Subnet Mask: **255.255.255.0**
  - Default Gateway: **172.16.0.1**
  - Preferred DNS Server: **172.16.0.10**
6. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, click the **Obtain an IP address automatically** and **Obtain the DNS server address automatically** options, and then click **OK**.
7. In the **Ethernet Properties** window, click **Close**.
8. In the **Ethernet Status** window, click **Details**.
9. Note the IP address shown on the **IPv4 DHCP Server** line of the **Network Connections Details** window. It should be **172.16.0.10, LON-DC1**.
10. Click **Close** twice, and then close the **Network and Sharing Center**.
11. Switch to **LON-SVR1**, and if **Server Manager** is not already open, click **Start**, and then click **Server Manager**.
12. In **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
13. In the **Add Roles and Features Wizard**, click **Next** three times.
14. On the **Select Server Roles** page, click **DHCP Server**.
15. In the **Add Roles and Features that are required** dialog box that opens, click **Add Features**, and then click **Next**.
16. On the **Select Features** page, click **Next**.
17. On the **DHCP Server** page, click **Next**.

18. On the **Confirm installation selections** page, click **Install**.
  19. When the DHCP Server role installation successfully completes, click **Close**.
  20. In **Server Manager**, click **Tools**, and then click **DHCP**.
  21. In the console tree, expand **DHCP**, select and then right-click **lon-svr1.adatum.com**, and then click **Authorize**.
  22. In the console tree, select and then right-click **IPv4**, and then click **New Scope**.
  23. In the **New Scope Wizard**, on the **Welcome** page, click **Next**.
  24. On the **Scope Name** page, in the **Name** box, type **Lab 10 Scope**, and then click **Next**.
  25. On the **IP Address Range** page, in the **Start IP address** box, type **172.16.0.200**, in the **End IP address** box, type **172.16.0.210**, in the **Subnet Mask** box, type **255.255.0.0**, and then click **Next**.
  26. On the **Add Exclusion and Delay** page, click **Next**.
  27. On the **Lease Duration** page, click **Next**.
  28. On the **Configure DHCP Options** page, ensure that **Yes, I want to configure these options now** is selected, and then click **Next**.
  29. On the **Router (Default Gateway)** page, in the **IP Address** box, type **172.16.0.1**, click **Add**, and then click **Next**.
  30. On the **Domain Name and DNS Servers** page, accept the defaults, and then click **Next**.
  31. On the **WINS servers** page, click **Next**.
  32. On the **Activate Scope** page, ensure that **Yes, I want to activate this scope now** is selected, and then click **Next**.
  33. On the **Completing the New Scope Wizard** page, click **Finish**.
  34. On **LON-HOST1**, click **Start**, and then click **Windows PowerShell**.
  35. At the Windows PowerShell command prompt, type the following commands to prevent **LON-DC1** from issuing a DHCP lease, and then press Enter after each line:

```
Set-VMNetworkAdapter -VMName 20741A-LON-DC1-B -DhcpGuard On
Set-VMNetworkAdapter -VMName 20741A-LON-SVR1-B -DhcpGuard Off
```
  36. On **LON-CL1**, right-click **Start**, and then click **Command Prompt (Admin)**.
  37. In the **Command Prompt** window, type the following commands, and then press Enter after each line:

```
IPConfig /release
IPConfig/renew
```
  38. In the notification area of the taskbar, right-click the **Network** icon, and then click **Open Network and Sharing Center**.
  39. In the **Network and Sharing Center** window, click the **Ethernet** hyperlink.
  40. In the **Ethernet Status** window, click **Details**. Note that it now has an **DHCP Server IP Address** from **LON-SVR1**.
- **Task 3: Configure and use VLANs**
1. On **LON-SVR1**, in the **Server Manager** console tree, select the **Local Server** node.
  2. In the **Properties details** pane, next to the **NIC Teaming** item, click the **Enabled** hyperlink.

3. In the **NIC Teaming** dialog box, in the **Teams** pane, select **LON-SVR1 NIC Team**, and then on the **Tasks** menu, click **Delete team**.
4. In the **NIC Teaming** dialog box, click **Delete team**.
5. On **LON-HOST1**, open **Hyper-V Manager**.
6. In Hyper-V Manager, in the **Actions** pane, click **Virtual Switch Manager**.
7. In the **Virtual Switch Manager for LON-HOST1** window, select **External Switch**.
8. In the **details** pane for **External Switch**, in the **VLAN ID** area, select **Enable virtual LAN identification for management operating system**, and then click **OK**.
9. While still on **LON-HOST1**, in Hyper-V Manager, in the **Virtual Machines** pane, right-click **20741A-LON-SVR1-B**, and then click **Settings**.
10. In the **Settings for 20741A-LON-SVR1-B on LON-HOST1** window, in the console tree, select **New Network Adapter**.
11. In the **details** pane, in the **VLAN ID** section, select **Enable virtual LAN identification**, and then click **OK**.

► **Task 4: Configure and use bandwidth management**

1. While still on **LON-HOST1**, in Hyper-V Manager, in the **Virtual Machines** pane, right-click **20741A-LON-SVR1-B**, and then click **Settings**.
2. In the **Settings for 20741A-LON-SVR1 on LON-HOST1** window, in the console tree, select **New Network Adapter**.
3. In the **details** pane, in the **Bandwidth Management** area, select **Enable bandwidth management**.
4. In the **Maximum bandwidth** box, type **100**, and then click **OK**.
5. On the **LON-SVR1** virtual machine, right-click the taskbar, and then click **Task Manager**.
6. In the **Task Manager** window, click the **More details** arrow.
7. In Task Manager, click the **Performance** tab, and then select the second Ethernet item. The **Adapter name** should be **Ethernet 2**.
8. Right-click **Start**, click **Run**, type **iexplore.exe**, and then press Enter.
9. Internet Explorer opens. Move the **Internet Explorer** window to one side with the Task Manager on the other side, so that you can see both windows at same the time.
10. In the address bar of Internet Explorer, type **www.microsoft.com** and then press Enter.
11. While the data loads or attempts to load in the browser, observe the Task Manager **Ethernet** item. It should not exceed a bandwidth speed of 100 Mbps.
12. On **LON-HOST1**, in Hyper-V Manager, in the **Virtual Machines** pane, right-click **20741A-LON-SVR1-B**, and then click **Settings**.
13. In the **Settings for 20741A-LON-SVR1 on LON-HOST1** window, in the console tree, select **New Network Adapter**.
14. In the **details** pane, in the **Virtual Switch** list, select **Not Connected**, and then click **OK**.
15. In the **Actions** pane, open the **Virtual Switch Manager**.
16. Click **External Switch**, click **Remove** in the **details** pane, and then click **OK**.
17. In the **Apply Networking Changes** window, click **Yes**.

**Results:** After completing this exercise, you should have successfully configured the advanced features of the Hyper-V virtual switch.

► **Task 5: Prepare for the next module**

After you finish the lab, revert the virtual machines to their initial state, and return the physical computer to the default operating system.

1. On **LON-HOST1**, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741A-LON-DC1-B**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20741A-LON-SVR1-B** and **20741A-LON-CL1-B**.
5. Restart **LON-HOST1**, and in the boot menu, select the default trainer center computer.

# Module 11: Implementing Software Defined Networking

## Lab: Deploying Network Controller

### Exercise 1: Preparing to deploy Network Controller

#### ► Task 1: Create the required 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** box, type **Network Controller Admins**, and then click **OK**.
6. In the details pane, double-click **Network Controller Admins**, and 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)** 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** box, type **Network Controller Ops**, and then click **OK**.
10. In the details pane, double-click **Network Controller Ops**, and 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)** box, type **administrator; Beth**, and then click **OK** twice.
12. Close **Active Directory Users and Computers**.

#### ► Task 2: Request a certificate for authenticating Network Controller

1. Switch to **LON-SVR2**.
2. Right-click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **mmc.exe**, and then press Enter.
4. In the **Console1 – [Console Root]** window, click **File**, and then click **Add/Remove Snap-in**.
5. In the **Add or Remove Snap-ins** dialog box, in the **Snap-in** list, double-click **Certificates**.
6. Click the **Computer** account, click **Next**, and then click **Finish**.
7. Click **OK**.
8. In the navigation pane, expand **Certificates (Local Computer)**, and then click **Personal**.
9. Right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
10. In the **Certificate Enrollment** dialog box, on the **Before you Begin** page, click **Next**.
11. On the **Select Certificate Enrollment Policy** page, click **Next**.
12. Select the **Computer** check box, and then click **Enroll**.

13. Click **Finish**.
14. Close the management console and do not save changes.

**Results:** After completing this exercise, you should have successfully prepared your environment for Network Controller.

## Exercise 2: Deploying Network Controller

### ► Task 1: 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.
7. Click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Network Controller** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the role is installed, click **Close**.
12. Right-click **Start**, point to **Shut down or sign out**, and then click **Restart**.
13. In the **Choose a reason that best describes why you want to shut down this computer** dialog box, click **Continue**.
14. After **LON-SVR2** has restarted, sign in as **Adatum\administrator** with the password as **Pa\$\$w0rd**.

### ► Task 2: Configure the Network Controller cluster



**Note:** These steps are duplicated in the high level steps for this lab.

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 "Ethernet"
```

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" }
```

- 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
```

### ► Task 3: Configure the Network Controller application



**Note:** This step is duplicated in the high level steps for this lab.

- 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
```

### ► Task 4: Verify the deployment



**Note:** These steps are duplicated in the high level steps for this lab.

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

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

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

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

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

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

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

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

- 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
```

- Press **Y**, and then press Enter when prompted.

- 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
```

- You should receive output that looks similar to the output below:

```
Tags                :  
ResourceRef         : /credentials/cred1  
CreatedTime         : 1/1/0001 12:00:00 AM  
InstanceId           : e16ffe62-a701-4d31-915e-7234d4bc5a18  
Etag                 : W/"1ec59631-607f-4d3e-ac78-94b0822f3a9d"  
ResourceMetadata    :  
ResourceId           : cred1  
Properties           : Microsoft.Windows.NetworkController.CredentialProperties
```

**Results:** After completing this exercise, you should have successfully deployed Network Controller.

#### ► Task 5: Prepare for course completion

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

- On the host computer, start **Hyper-V Manager**.
- In the **Virtual Machines** list, right-click **20741A-LON-DC1**, and then click **Revert**.
- In the **Revert Virtual Machine** dialog box, click **Revert**.
- Repeat steps 2 and 3 for **20741A-LON-SVR2**.