

OFFICIAL MICROSOFT LEARNING PRODUCT

6420A

Fundamentals of a Windows Server® 2008 Network Infrastructure and Application Platform



Be sure to access the extended learning content on your Course Companion CD enclosed on the back cover of the book.

MCT USE ONLY. STUDENT USE PROHIBITED

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.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BitLocker, Excel, Internet Explorer, Outlook, PowerPoint, SharePoint, SQL Server, Visual Basic, Win32, Windows, Windows Media, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Technical Reviewer: Don Messier

Product Number: 6420A

Part Number :

Released: 11/2008

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS - TRAINER

EDITION – Pre-Release and Final Release Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the Licensed Content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this Licensed Content, unless other terms accompany those items. If so, those terms apply.

By using the Licensed Content, you accept these terms. If you do not accept them, do not use the Licensed Content.

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

1. DEFINITIONS.

- "Academic Materials"** means the printed or electronic documentation such as manuals, workbooks, white papers, press releases, datasheets, and FAQs which may be included in the Licensed Content.
- "Authorized Learning Center(s)"** means a Microsoft Certified Partner for Learning Solutions location, an IT Academy location, or such other entity as Microsoft may designate from time to time.
- "Authorized Training Session(s)"** means those training sessions authorized by Microsoft and conducted at or through Authorized Learning Centers by a Trainer providing training to Students solely on Official Microsoft Learning Products (formerly known as Microsoft Official Curriculum or "MOC") and Microsoft Dynamics Learning Products (formerly known as Microsoft Business Solutions Courseware). Each Authorized Training Session will provide training on the subject matter of one (1) Course.
- "Course"** means one of the courses using Licensed Content offered by an Authorized Learning Center during an Authorized Training Session, each of which provides training on a particular Microsoft technology subject matter.
- "Device(s)"** means a single computer, device, workstation, terminal, or other digital electronic or analog device.
- "Licensed Content"** means the materials accompanying these license terms. The Licensed Content may include, but is not limited to, the following elements: (i) Trainer Content, (ii) Student Content, (iii) classroom setup guide, and (iv) Software. There are different and separate components of the Licensed Content for each Course.
- "Software"** means the Virtual Machines and Virtual Hard Disks, or other software applications that may be included with the Licensed Content.
- "Student(s)"** means a student duly enrolled for an Authorized Training Session at your location.

BETA COURSEWARE. EXPIRES 5/16/2008

- i. **"Student Content"** means the learning materials accompanying these license terms that are for use by Students and Trainers during an Authorized Training Session. Student Content may include labs, simulations, and courseware files for a Course.
- j. **"Trainer(s)"** means a) a person who is duly certified by Microsoft as a Microsoft Certified Trainer and b) such other individual as authorized in writing by Microsoft and has been engaged by an Authorized Learning Center to teach or instruct an Authorized Training Session to Students on its behalf.
- k. **"Trainer Content"** means the materials accompanying these license terms that are for use by Trainers and Students, as applicable, solely during an Authorized Training Session. Trainer Content may include Virtual Machines, Virtual Hard Disks, Microsoft PowerPoint files, instructor notes, and demonstration guides and script files for a Course.
- l. **"Virtual Hard Disks"** means Microsoft Software that is comprised of virtualized hard disks (such as a base virtual hard disk or differencing disks) for a Virtual Machine that can be loaded onto a single computer or other device in order to allow end-users to run multiple operating systems concurrently. For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- m. **"Virtual Machine"** means a virtualized computing experience, created and accessed using Microsoft® Virtual PC or Microsoft® Virtual Server software that consists of a virtualized hardware environment, one or more Virtual Hard Disks, and a configuration file setting the parameters of the virtualized hardware environment (e.g., RAM). For the purposes of these license terms, Virtual Hard Disks will be considered "Trainer Content".
- n. **"you"** means the Authorized Learning Center or Trainer, as applicable, that has agreed to these license terms.

2. OVERVIEW.

Licensed Content. The Licensed Content includes Software, Academic Materials (online and electronic), Trainer Content, Student Content, classroom setup guide, and associated media.

License Model. The Licensed Content is licensed on a per copy per Authorized Learning Center location or per Trainer basis.

3. INSTALLATION AND USE RIGHTS.

- a. **Authorized Learning Centers and Trainers: For each Authorized Training Session, you may:**
 - i. either install individual copies of the relevant Licensed Content on classroom Devices only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of copies in use does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session, **OR**
 - ii. install one copy of the relevant Licensed Content on a network server only for access by classroom Devices and only for use by Students enrolled in and the Trainer delivering the Authorized Training Session, provided that the number of Devices accessing the Licensed Content on such server does not exceed the number of Students enrolled in and the Trainer delivering the Authorized Training Session.
 - iii. and allow the Students enrolled in and the Trainer delivering the Authorized Training Session to use the Licensed Content that you install in accordance with (i) or (ii) above during such Authorized Training Session in accordance with these license terms.

BETA COURSEWARE. EXPIRES 5/16/2008

protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
 - you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
 - you developed independently.
- d. **Term.** The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the Licensed Content, whichever is first ("beta term").
- e. **Use.** You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control and/or in the possession or under the control of any Trainers who have received copies of the pre-released version.
- f. **Copies.** Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

5. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Authorized Learning Centers and Trainers:

i. Software.

ii. **Virtual Hard Disks.** The Licensed Content may contain versions of Microsoft XP, Microsoft Windows Vista, Windows Server 2003, Windows Server 2008, and Windows 2000 Advanced Server and/or other Microsoft products which are provided in Virtual Hard Disks.

A. If the Virtual Hard Disks and the labs are launched through the Microsoft Learning Lab Launcher, then these terms apply:

Time-Sensitive Software. If the Software is not reset, it will stop running based upon the time indicated on the install of the Virtual Machines (between 30 and 500 days after you install it). You will not receive notice before it stops running. You may not be able to access data used or information saved with the Virtual Machines when it stops running and may be forced to reset these Virtual Machines to their original state. You must remove the Software from the Devices at the end of each Authorized Training Session and reinstall and launch it prior to the beginning of the next Authorized Training Session.

B. If the Virtual Hard Disks require a product key to launch, then these terms apply:

Microsoft will deactivate the operating system associated with each Virtual Hard Disk. Before installing any Virtual Hard Disks on classroom Devices for use during an Authorized Training Session, you will obtain from Microsoft a product key for the operating system software for the Virtual Hard Disks and will activate such Software with Microsoft using such product key.

C. These terms apply to all Virtual Machines and Virtual Hard Disks:

BETA COURSEWARE. EXPIRES 5/16/2008

You may only use the Virtual Machines and Virtual Hard Disks if you comply with the terms and conditions of this agreement and the following security requirements:

- You may not install Virtual Machines and Virtual Hard Disks on portable Devices or Devices that are accessible to other networks.
 - You must remove Virtual Machines and Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session, except those held at Microsoft Certified Partners for Learning Solutions locations.
 - You must remove the differencing drive portions of the Virtual Hard Disks from all classroom Devices at the end of each Authorized Training Session at Microsoft Certified Partners for Learning Solutions locations.
 - You will ensure that the Virtual Machines and Virtual Hard Disks are not copied or downloaded from Devices on which you installed them.
 - You will strictly comply with all Microsoft instructions relating to installation, use, activation and deactivation, and security of Virtual Machines and Virtual Hard Disks.
 - You may not modify the Virtual Machines and Virtual Hard Disks or any contents thereof.
 - You may not reproduce or redistribute the Virtual Machines or Virtual Hard Disks.
- ii. Classroom Setup Guide.** You will assure any Licensed Content installed for use during an Authorized Training Session will be done in accordance with the classroom set-up guide for the Course.
- iii. Media Elements and Templates.** You may allow Trainers and Students to use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the Licensed Content solely in an Authorized Training Session. If Trainers have their own copy of the Licensed Content, they may use Media Elements for their personal training use.
- iv. iv Evaluation Software.** Any Software that is included in the Student Content designated as "Evaluation Software" may be used by Students solely for their personal training outside of the Authorized Training Session.

b. Trainers Only:

- i. Use of PowerPoint Slide Deck Templates.** The Trainer Content may include Microsoft PowerPoint slide decks. Trainers may use, copy and modify the PowerPoint slide decks only for providing an Authorized Training Session. If you elect to exercise the foregoing, you will agree or ensure Trainer agrees: (a) that modification of the slide decks will not constitute creation of obscene or scandalous works, as defined by federal law at the time the work is created; and (b) to comply with all other terms and conditions of this agreement.
- ii. Use of Instructional Components in Trainer Content.** For each Authorized Training Session, Trainers may customize and reproduce, in accordance with the MCT Agreement, those portions of the Licensed Content that are logically associated with instruction of the Authorized Training Session. If you elect to exercise the foregoing rights, you agree or ensure the Trainer agrees: (a) that any of these customizations or reproductions will only be used for providing an Authorized Training Session and (b) to comply with all other terms and conditions of this agreement.

iii. Academic Materials. If the Licensed Content contains Academic Materials, you may copy and use the Academic Materials. You may not make any modifications to the Academic Materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any Academic Materials, you agree that:

- The use of the Academic Materials will be only for your personal reference or training use
- You will not republish or post the Academic Materials on any network computer or broadcast in any media;
- You will include the Academic Material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

Form of Notice:

© 2007 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the US and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

6. INTERNET-BASED SERVICES. Microsoft may provide Internet-based services with the Licensed Content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

7. 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 allow you to use it in certain ways. You may not

- install more copies of the Licensed Content on classroom Devices than the number of Students and the Trainer in the Authorized Training Session;
- allow more classroom Devices to access the server than the number of Students enrolled in and the Trainer delivering the Authorized Training Session if the Licensed Content is installed on a network server;
- copy or reproduce the Licensed Content to any server or location for further reproduction or distribution;
- disclose the results of any benchmark tests of the Licensed Content to any third party without Microsoft's prior written approval;
- work around any technical limitations in the Licensed Content;
- reverse engineer, decompile or disassemble the Licensed Content, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the Licensed Content than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the Licensed Content for others to copy;

BETA COURSEWARE. EXPIRES 5/16/2008

- transfer the Licensed Content, in whole or in part, to a third party;
 - access or use any Licensed Content for which you (i) are not providing a Course and/or (ii) have not been authorized by Microsoft to access and use;
 - rent, lease or lend the Licensed Content; or
 - use the Licensed Content for commercial hosting services or general business purposes.
 - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
8. **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.
9. **NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or Licensed Content marked as "NFR" or "Not for Resale."
10. **ACADEMIC EDITION.** You must be a "Qualified Educational User" to use Licensed Content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.
11. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of these license terms. In the event your status as an Authorized Learning Center or Trainer a) expires, b) is voluntarily terminated by you, and/or c) is terminated by Microsoft, this agreement shall automatically terminate. Upon any termination of this agreement, you must destroy all copies of the Licensed Content and all of its component parts.
12. **ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the Licensed Content and support services.**
13. **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.
14. **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.
15. **DISCLAIMER OF WARRANTY. The Licensed Content is licensed "as-is." You bear the risk of using it. Microsoft 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 excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.**

BETA COURSEWARE. EXPIRES 5/16/2008

16. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$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, software, 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.

Contents

About This Course

About This Course	i
Course Materials	iii
Virtual Machine Environment	iv

Module 1: Fundamentals of Network Infrastructure

Lesson 1: Network Communication Standards	1-3
Lesson 2: Physical Network Infrastructure	1-10
Lesson 3: Logical Network Organization	1-17
Lesson 4: Overview of Active Directory	1-24
Lab: Identifying Network Components	1-31

Module 2: IT Professionals in an Enterprise

Lesson 1: IT Professional Roles	2-3
Lesson 2: IT Management and Processes	2-8
Lesson 3: Professional Development for IT Professionals	2-15
Lab: Developing a Training Plan	2-23

Module 3: Configuring Basic TCP/IPv4 Settings

Lesson 1: Overview of the TCP/IP Protocol Suite	3-3
Lesson 2: Overview of TCP/IP Addressing	3-10
Lesson 3: Name Resolution	3-15
Lesson 4: Dynamic IP Addressing	3-24
Lesson 5: TCP/IPv4 Tools	3-31
Lab: Configuring Basic TCP/IPv4 Settings and Validating TCP/IPv4 Connectivity	3-37

Module 4: Fundamentals of Communication Technologies	
Lesson 1: Network Content Types	4-3
Lesson 2: Packet Delivery Method	4-8
Module 5: TCP/IPv4 Fundamentals	
Lesson 1: Overview of IPv4 Communication	5-3
Lesson 2: Subnetting Overview	5-9
Lesson 3: Subnetting for Complex Networks	5-14
Lab: Creating IPv4 Address Spaces	5-19
Module 6: IPv6 Fundamentals	
Lesson 1: Introduction to IPv6	6-3
Lesson 2: Unicast IPv6 Addresses	6-11
Lesson 3: Configuring IPv6	6-17
Lab: Configuring IPv6	6-23
Module 7: Fundamentals of Administering Windows Server 2008	
Lesson 1: Introduction to IPv6	7-3
Lesson 2: Unicast IPv6 Addresses	7-10
Lesson 3: Configuring IPv6	7-17
Lesson 4: Using Remote Desktop for Administration	7-24
Lesson 5: Configuring Security for Server Administration	7-30
Lab: Configuring IPv6	7-36
Module 8: Security Fundamentals	
Lesson 1: Defense-in-Depth	8-3
Lesson 2: Securing Access to Web Content	8-13
Lesson 3: Securing Access to Files	8-20
Lesson 4: Data Encryption	8-27
Lab: Configuring Data Security	8-33

Module 9: Fundamentals of Securing Network Communication	
Lesson 1: Public Key Infrastructure	9-3
Lesson 2: Using Certificates	9-10
Lab: Securing Web Communication	9-17
Module 10: Windows Firewall and Caching Fundamentals	
Lesson 1: Overview of Perimeter Security	10-2
Lesson 2: Windows Firewall Overview	10-8
Lesson 3: Creating Windows Firewall Rules	10-15
Lesson 4: Monitoring and Troubleshooting Windows Firewall	10-22
Lab: Using Windows Firewall	10-29
Module 11: Remote Access Fundamentals	
Lesson 1: Remote Access Overview	11-3
Lesson 2: RADIUS Overview	11-8
Lesson 3: Network Policy Server	11-14
Lesson 4: Troubleshooting Remote Access	11-20
Lab: Implementing Remote Access	11-24
Module 12: Routing Fundamentals	
Lesson 1: Routing Overview	12-3
Lesson 2: Configuring RRAS as a Router	12-8
Lesson 3: Quality of Service	12-14
Lab: Configuring Routing	12-20
Module 13: Network Load Balancing Fundamentals	
Lesson 1: Server Availability and Scalability Overview	13-3
Lesson 2: Windows Network Load Balancing	13-9
Lesson 3: Configuring Windows Network Load Balancing	13-14
Lab: Implementing Network Load Balancing	13-21

MCT USE ONLY. STUDENT USE PROHIBITED	Module 14: Configuring Print Resources and Printing Pools	
	Lesson 1: Printing Overview	14-3
	Lesson 2: Configuring Network Printers	14-11
	Lesson 3: Using Print Management	14-18
	Lesson 4: Managing Printers	14-25
	Lesson 5: Troubleshooting Network Printing	14-31
	Lab: Implementing Printing	14-34
	Module 15: Virtualization Overview	
	Lesson 1: Overview of Server Virtualization	15-3
	Lesson 2: Overview of Windows Server Virtualization	15-9
	Lesson 3: Creating a Virtual Environment	15-15

About This Course

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

Course Description

This five-day instructor-led course introduces students to network infrastructure and application platform concepts and configurations provided by Windows Server 2008. Students will be able to acquire a fundamental understanding in order to pursue advanced topics available for certification in the infrastructure or application platform services.

Audience

This course is intended for new IT employees or Desktop Support workers moving into server support. The information in this course allows them acquire a fundamental understanding of Windows networks to pursue advanced topics. This course is also useful for those migrating from competitive platforms to Windows Server 2008.

Student Prerequisites

This course requires that you meet the following prerequisites:

- A+, Server+, hardware portion of Net+, and familiarity with Windows (client side)
- Working knowledge of a Windows 2003 environment
- Working knowledge of networking technologies

Course Objectives

After completing this course, students will be able to:

- Describe the fundamentals of an enterprise networking environment.
- Describe the typical roles of IT Professionals in an enterprise environment.
- Describe TCP/IPv4 configurations, protocols, and tools.
- Describe the fundamentals of communication technologies.
- Create an IPv4 address range and subnet.
- Configure IPv6 addresses.
- Administer a Windows 2008 server.

- Describe basic security concepts for server roles.
- Describe how to secure network traffic by using certificates.
- Configure Windows Firewall.
- Configure and troubleshoot remote access.
- Describe routing concepts, protocols, and quality of service.
- Configure and test network load balancing.
- Configure network print resources and printing pools.
- Describe the functions included with Windows Server Virtualization (WSV).

Course Outline

This section provides an outline of the course:

Module 1: This module describes the fundamentals of an enterprise networking environment, which consists of Windows Infrastructure Services, Windows Application Platform Services, and Active Directory.

Module 2: This module describes the IT Professional roles (and their respective responsibilities) that may exist in a typical enterprise environment.

Module 3: This module describes the TCP/IPv4 configuration, protocols and the tools used to validate configurations.

Module 4: This module describes static and dynamic HTTP content, how to differentiate between the two, and the various mechanisms used by TCP/IPv4 to send and receive data traffic.

Module 5: This module explains how to define and create an IPv4 address range and subnetting for a network.

Module 6: This module introduces IPv6, describes the differences between IPv4 and IPv6, and explains how to configure IPv6 addresses.

Module 7: This module explains how to administer a Windows 2008 server.

Module 8: This module introduces basic industry standard security concepts for server roles.

Module 9: This module describes how to secure network traffic by using certificates.

Module 10: This module describes proxy and caching services; how to configure Windows Firewall by creating exceptions and modifying firewall rules; how to configure auditing and monitoring; and how to troubleshoot Windows Firewall.

Module 11: This module explains how to configure network policies, configure a radius proxy, and how to troubleshoot NPS as a radius proxy.

Module 12: This module describes routing concepts and protocols, and explains how quality of service can be used within a network environment.

Module 13: This module explains how to configure and test network load balancing.

Module 14: This module explains how to configure network print resources and printing pools.

Module 15: This module describes the fundamental functions included with Windows Server Virtualization (WSV).

Course Materials

The following materials are included with your kit:

- *Course handbook.* The Course handbook contains the material covered in class. It is meant to be used in conjunction with the Course Companion CD.
- *Course Companion CD.* The Course Companion CD contains the full course content, including expanded content for each topic pages, full lab exercises and answer keys, topical and categorized resources and Web links. It is meant to be used both inside and outside the class.

Note To access the full course content, insert the Course Companion CD into the CD-ROM drive, and then in the root directory of the CD, double-click StartCD.exe.

- *Course evaluation.* At the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.

To provide additional comments or feedback on the course, send e-mail to support@microsoft.com. To inquire about the Microsoft Certification Program, send e-mail to mcphelp@microsoft.com.

Virtual Machine Environment

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

Virtual Machine Configuration

In this course, you will use Microsoft Virtual Server 2005 to perform the labs.

Important: At the end of each lab, you must close the virtual machine and must not save any changes. To close a virtual machine without saving the changes, perform the following steps: 1. On the host computer, click **Start**, point to **All Programs**, point to **Microsoft Virtual Server**, and then click **Virtual Server Administration Website**. 2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, point to the virtual machine name, and, in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.

The following table shows the role of each virtual machine that this course uses:

Virtual machine	Role
6420A-NYC-DC1	Domain controller in the WoodgroveBank.com domain
6420A-NYC-WEB	Web server in the WoodgroveBank.com domain
6420A-NYC-RAS	Routing and Remote Access server in the WoodgroveBank.com domain
6420A-NYC-SVR1	Standalone server
6420A-NYC-CL1	Windows Vista computer in the WoodgroveBank.com domain

Software Configuration

The following software is installed on each virtual machine:

- Windows Server 2008 Enterprise; Windows Vista

Classroom Setup

Each classroom computer will have the same virtual machine configured in the same way.

Course Hardware Level

To ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft Learning Product courseware are taught. This course requires a computer that meets or exceeds hardware level 5, which specifies a 2.4-gigahertz (minimum) Pentium 4 or equivalent CPU, at least 2 gigabytes (GB) of RAM, 16 megabytes (MB) of video RAM, and a 7200 RPM 40-GB hard disk.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 1

Fundamentals of Network Infrastructure

Contents:

Lesson 1: Network Communication Standards	1-3
Lesson 2: Physical Network Infrastructure	1-10
Lesson 3: Logical Network Organization	1-17
Lesson 4: Overview of Active Directory	1-24
Lab: Identifying Network Components	1-31

MCT USE ONLY. STUDENT USE PROHIBITED

Module Overview

- Network Communication Standards
- Physical Network Infrastructure
- Logical Network Organization
- Overview of Active Directory
- Server Roles

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 1

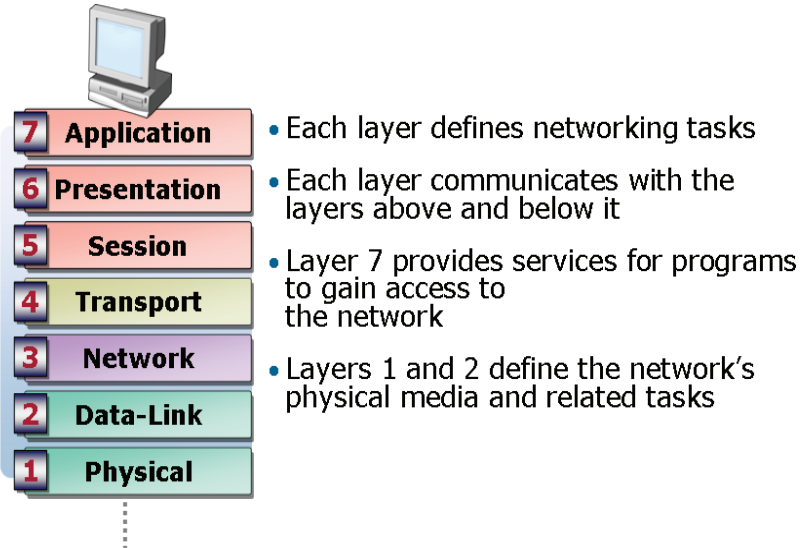
Network Communication Standard

- What Is the OSI Model?
- Why Use the OSI Model?
- Discussion: Common Network Standards
- Benefits of Network Standards
- Standards Defining Bodies

Understanding network communication standards is an integral part of managing a Windows Server 2008 network. Various network communication standards are used to provide connectivity between servers, clients, and network devices. Being aware of network communication standards allows you to ensure that all devices on your network can communicate.

What Is the OSI Model?

The Open System Interconnection (OSI) model defines the generic tasks that are performed for network communication



Key Points

The Open System Interconnection (OSI) model defines the generic tasks that are performed for network communication. You can think of each layer of the OSI model as a piece of software that performs specific tasks for that layer. Each layer communicates with the layer below and the layer above. Data that is transmitted over the network must pass through all seven layers.

Question: How is the application layer of the OSI model different from an application such as Microsoft Word?

Why Use the OSI Model?

The OSI model is a common reference point for discussing network communication that is used to describe device and protocol functionality

Examples:

- Router is a layer 3 device
- HTTP is a layer 5-7 protocol
- Ethernet is a standard for layers 1-2

Key Points

The OSI model is used as a common reference point when comparing the function of different protocols and types of network hardware. Understanding the OSI model is important for comparing different products. Also, understanding the layers of the OSI model allows you to understand the functions that a device is performing.

Question: How will you use the OSI model?

Discussion: Common Network Standards

What are some common network standards?

Key Points

Answer the questions in a classroom discussion.

Benefits of Network Standards

Network standards:

- **Enable vendor interoperability**
- **Reduce costs**

Key Points

Network standards enhance the interoperability of vendor products. If each vendor has a proprietary method for network communication, their products will not be able to communicate without the addition of additional software or hardware to translate between them.

Question: Why is vendor interoperability important?

Standards Defining Bodies

Standards defining bodies include:

- **Internet Engineering Task Force (IETF)**
- **World Wide Web Consortium (W3C)**
- **Institute of Electrical and Electronics Engineers (IEEE)**
- **International Telecommunication Union (ITU)**

Key Points

Standards defining bodies provide a forum for the development of network standards. Each organization is responsible for a specific area. Vendors such as Microsoft participate on committees that negotiate the standards.

Question: Why would you want to know which organization is responsible for defining a particular network standard?

Additional Resources:

IETF Web site: <http://www.ietf.org>

W3C Web site: <http://www.w3.org>

IEEE Web site: <http://www.ieee.org>

ITU Web site: <http://www.itu.int>

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 2

Physical Network Infrastructure

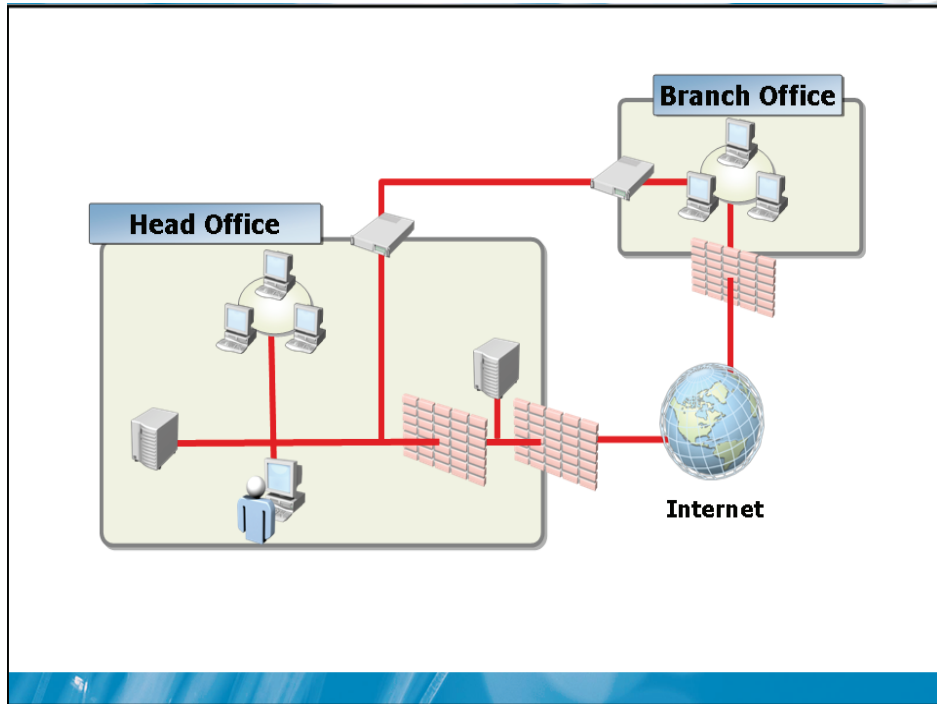
MCT USE ONLY. STUDENT USE PROHIBITED

- Discussion: Network Components
- Common Types of Media
- What is a Switch?
- What Is a Router?
- What is a Firewall?

Key Points

Computers require a physical network infrastructure to communicate over. This infrastructure allows and controls communication between computers. Understanding these components and how they work is essential to understanding how data moves through a computer network and to troubleshooting network communication.

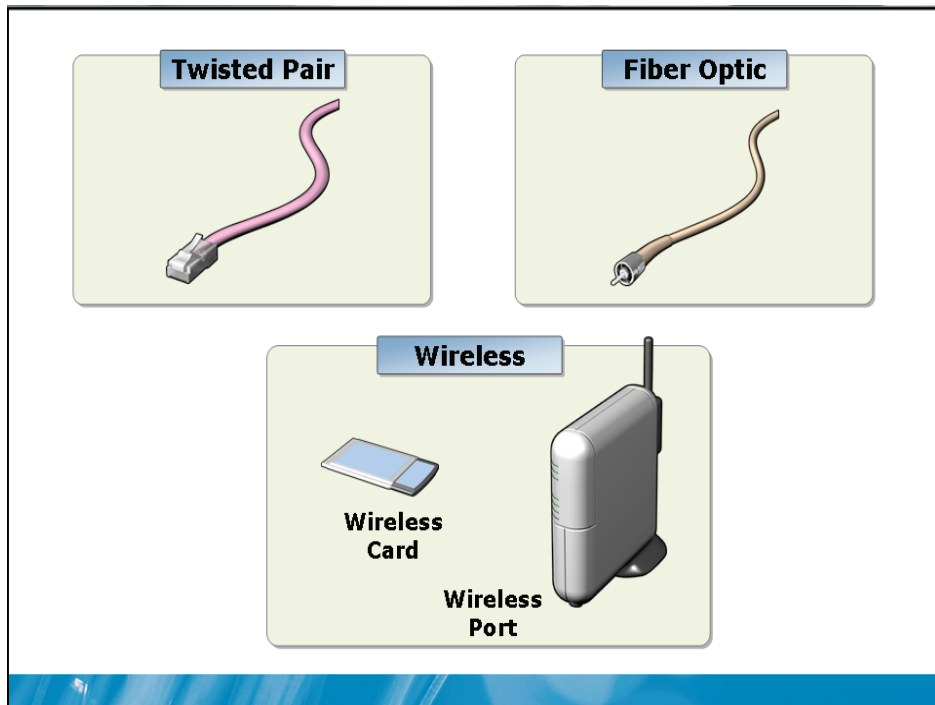
Discussion: Network Components



Question: Which of these devices is present in your network?

USE PROHIBITED

Common Types of Media



Key Points

Twisted-pair cabling is the most common type of cabling used on internal corporate networks. A single cable consists of four pairs of wire that are twisted around each other. Maximum length when used for Ethernet is 100m.

Fiber optic cabling carries light pulses rather than electrical signals. This type of cabling is less susceptible to signal deterioration and can be used for longer distances. Multimode fiber uses a plastic core to carry the light pulses, while single-mode fiber uses a glass core. Multimode fiber supports distances up to 2 km for 100 Mbps Ethernet while single-mode fiber supports distances up to 40 km for 10 Gbps Ethernet.

Wireless networking is used in corporate networks to support users that roam within a building or within a campus. The primary advantage of wireless networking is lack of cabling requirements. However, wireless access points must be placed carefully to ensure that signal strength is strong enough in all areas.

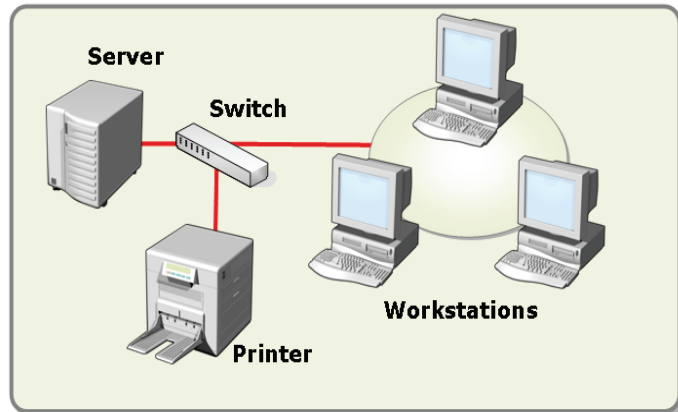
Question: What type of media would you implement between two buildings 1 km apart?

MCT USE ONLY. STUDENT USE PROHIBITED

What Is a Switch?

A switch:

- Is a LAN communication device
- Tracks the location of computers



Key Points

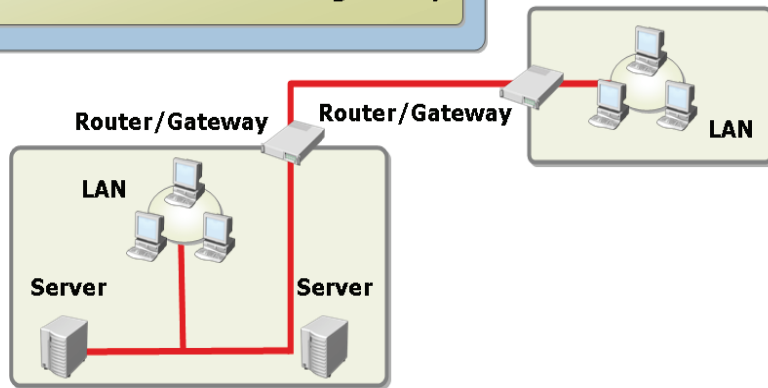
Computers on an internal network are connected to a switch that controls network communication. A switch is a layer 2 device that has multiple ports and a computer or another network device can be connected to each port. The switch tracks the location of each computer or network device and delivers packets only to the appropriate network port.

Question: If a single port in a switch fails, how will network communication be affected?

What Is a Router?

A router:

- Moves packets between networks
- Tracks networks not computers
- Is required between physical locations
- Is sometimes referred to as a gateway



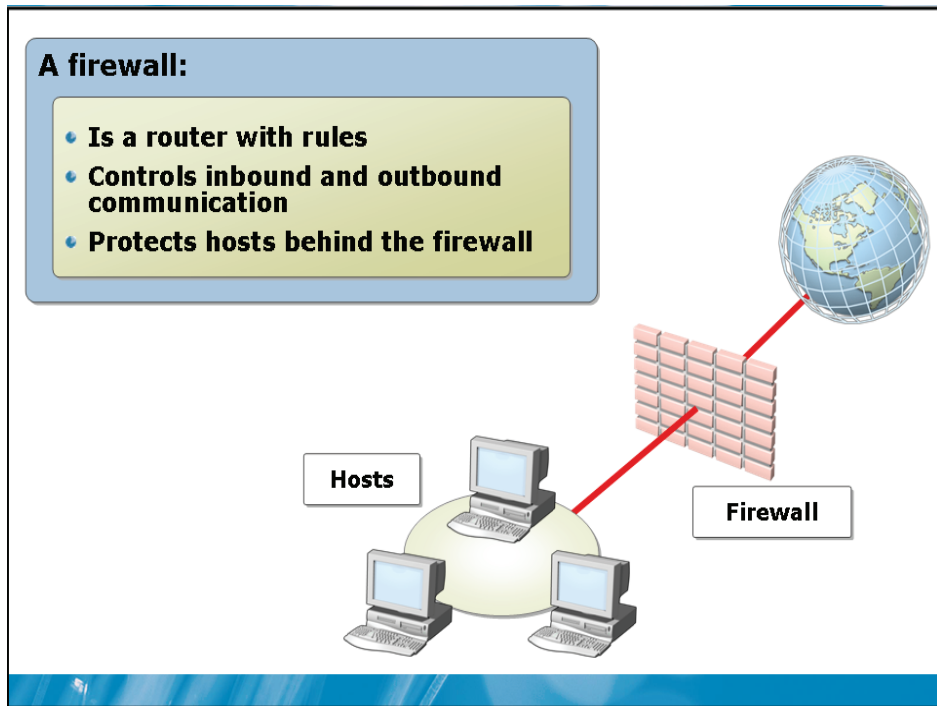
Key Points

A router is a layer 3 device that is used to move packets between networks. A router uses a routing table to keep a list of available networks. A router does not track the location of individual computers. This makes a router more scalable and suitable for tasks such as moving packet on the Internet.

Question: If a port on a router fails, how will network communication be affected?

USE PROHIBITED

What Is a Firewall?



Key Points

A firewall is a layer 4 device that is used to protect corporate networks. A typical firewall acts as a router between two networks and filters out packets that do not meet the specified criteria. Packets may be filtered based on the source and destination addresses or the application generating the packets.

Question: Why is it important to have a firewall between corporate networks and the Internet?

Lesson 3

Logical Network Organization

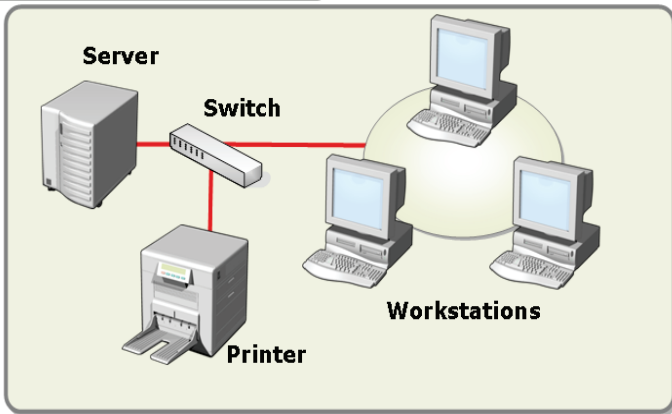
- What Is a LAN?
- What Is a WAN?
- What Is a Branch Office?
- Discussion: Branch Office Challenges
- What Is a Perimeter Network?
- What Is Remote Access?

The physical network infrastructure is used to organize computer networks into a logical network organization. The logical organization of computers and network devices makes it easier to understand how the physical network infrastructure is used.

What Is a LAN?

A LAN:

- Is a single physical location
- Has fast network connectivity
- Has typically minimal control



Key Points

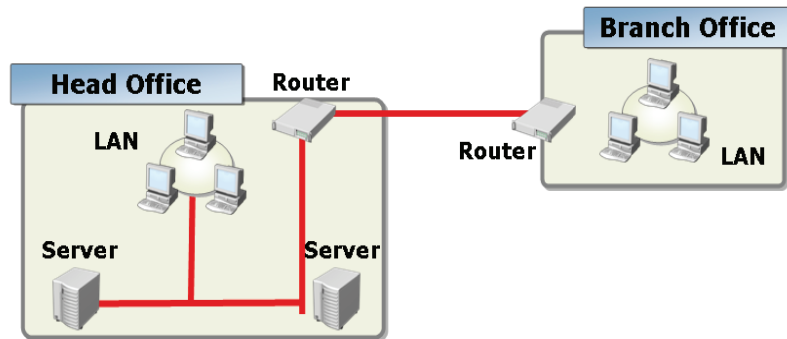
A local area network (LAN) is a network with a single physical location. This location could be a single building or a campus with multiple buildings in close proximity.

Question: What controls do you think should be in place to control LAN traffic?

What is a WAN?

A WAN:

- Is used between physical locations
- Has slower connection speed than a LAN
- Is more expensive than LAN connectivity
- Uses connectivity typically provided by another company



Key Points

A wide area network (WAN) is used between physical locations, such as a head office and branch office. In general, a WAN has much slower connectivity than within a LAN. For example, a T1 connection between WAN locations operates at 1.5 Mbps versus LAN speeds of 100 Mbps and up.

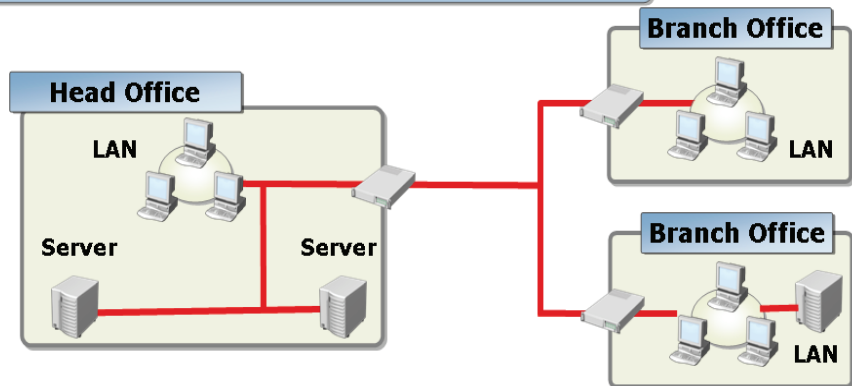
Question: What are some examples of WAN connectivity?

USE PROHIBITED

What Is a Branch Office?

A branch office is remote location that is connected by WAN links to the head office with:

- A generally small number of users
- Limited local support resources
- Limited local computing resources



Key Points

A branch office is a remote location that is connected by WAN links to the head office.

Question: What are some examples of branch offices?

Discussion: Branch Office Challenges

What are the challenges of branch office communication?

Key Points

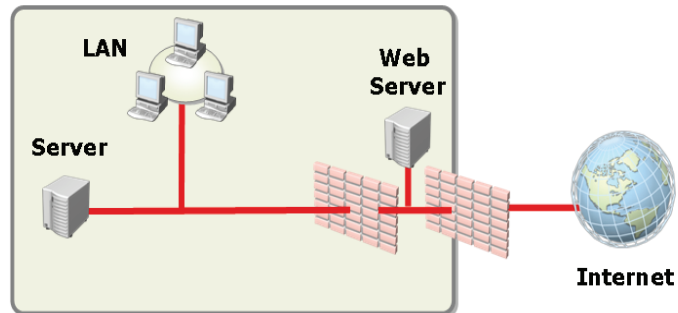
Answer the questions in a classroom discussion.

USE PROHIBITED

What Is a Perimeter Network?

A perimeter network:

- Isolates LAN resources
- Increases security



Key Points

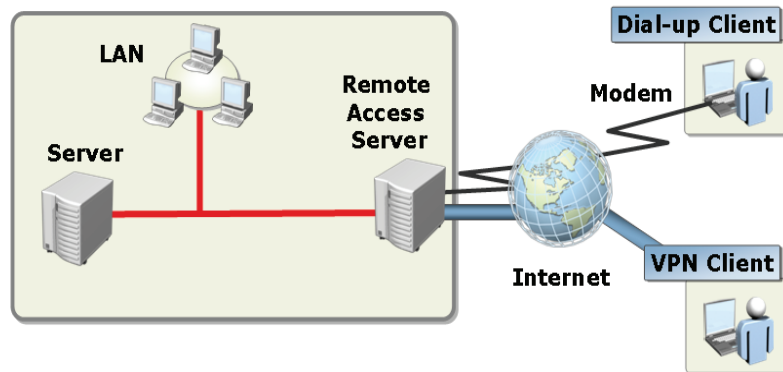
A perimeter network is used to isolate externally accessible resources from the LAN and from the Internet. A perimeter network is formed by using two firewalls. One firewall is located between the Internet and the perimeter network. The second firewall is located between the perimeter network and the LAN.

Question: Why would using a single firewall to create a perimeter network be considered less secure than using two firewalls?

What Is Remote Access?

Remote access:

- Provides access to LAN resources from outside the office
- Can be VPN or dial-up



Key Points

Remote access is the process used to give users access to LAN resources from outside the office. This type of connectivity is increasingly important as more users become mobile and work from home and other locations outside the office

Question: Why do users need access to data and applications remotely?

Lesson 4

Overview of Active Directory Topic

- What Is Active Directory?
- Benefits of Active Directory
- What Is a Domain?
- What Is a Forest?
- What Is a Domain Controller?
- Demonstration: Joining a Domain

Key Points

Active Directory is a central repository of network information. Understanding how Active Directory is organized is essential to understanding network security and management. In this lesson, you will learn about Active directory domains, forests, and domain controllers.

What Is Active Directory?

Active Directory:

- Is a central repository of network information
- Is organized into domains, trees, and forests
- Has multiple partitions:
 - Domain
 - Configuration
 - Schema

Key Points

Active Directory is a central repository of network information that is used for logon security and application configuration. The information stored in Active Directory includes:

- User accounts
- Computer accounts
- Application configuration information
- Subnet addresses

Benefits of Active Directory

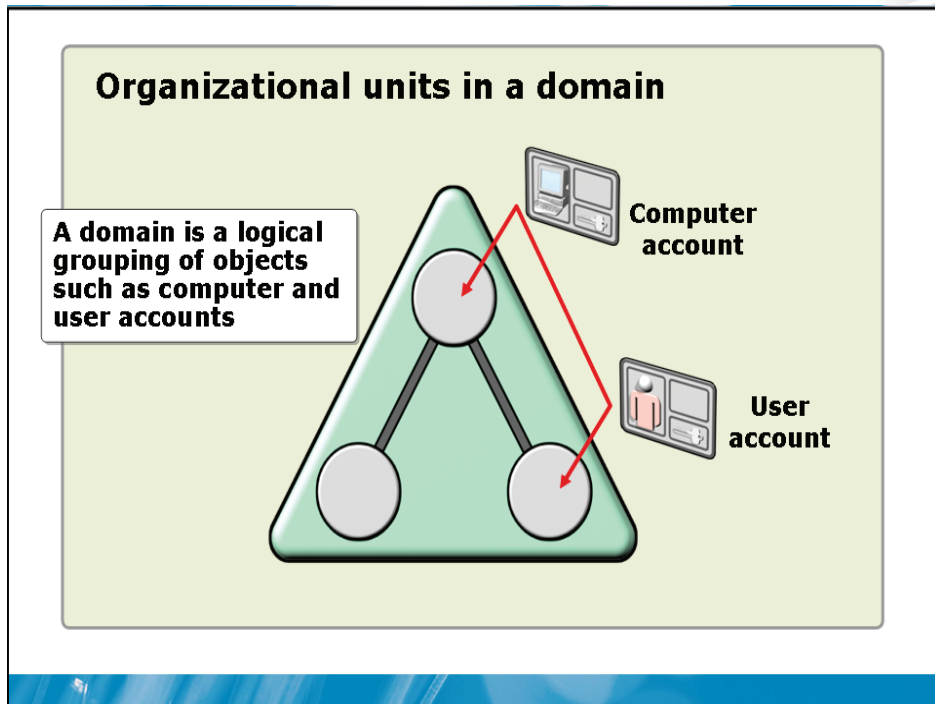
Compared to a workgroup, the benefits of Active Directory include:

- Simplified security management
- Redundant storage of security information
- Group Policy
- Extensibility

Key Points

Active Directory provides a single repository of information that is used for network management. A workgroup is a peer-to-peer network without a centralized security database.

What Is a Domain?

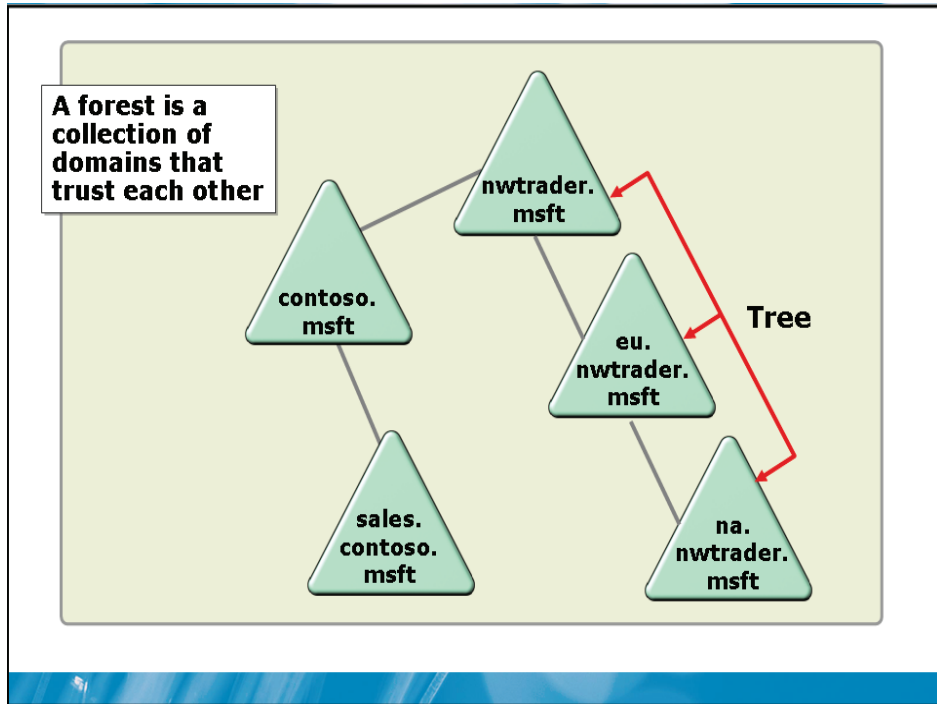


Key Points

A domain is a logical grouping of objects such as:

- **User accounts.** These are required for users to log on and access network resources. Information such as e-mail addresses and mailing addresses can be stored as part of a user account.
- **Computer accounts.** These are required for a computer to participate in the domain and become part of the security infrastructure. To log on with a domain user account, you must use a computer that has a computer account in the domain.
- **Groups.** These are used to organize users and computers into sets for assigning permissions to resources. Using groups make is easier to manage access to resources such as files.

What Is a Forest?



Key Points

A forest is collection of domains that automatically have a trust relationship. When domains have a trust relationship, accounts in the trusted domain can be granted access to resources in the trusting domain.

What Is a Domain Controller?

A Domain Controller:

- Holds a copy of Active Directory
- Responds to requests for Active Directory information
- Authenticates users to the network
- Is located by querying DNS

Key Points

A domain controller is a computer that holds a copy of Active Directory information. At minimum, a domain controller holds a copy of the local domain partition, the configuration partition, and the schema partition.

Demonstration: Joining a Domain

In this demonstration, you see how to join a computer to a domain

Lesson 5

Server Roles

- Windows Server 2008 Editions
- What Are Server Roles?
- What Are the Windows Infrastructure Services Roles?
- What Are the Windows Application Platform Services Roles?
- What Are the Active Directory Roles?
- What Are Server Features?
- What Is Server Core?

Windows Server 2008 is configured by adding and removing server roles and features. This is a new method of organizing the addition and removal of services. Understanding server roles and features allows you to install and support only the Windows Server 2008 components you need in your environment.

Windows Server 2008 Editions

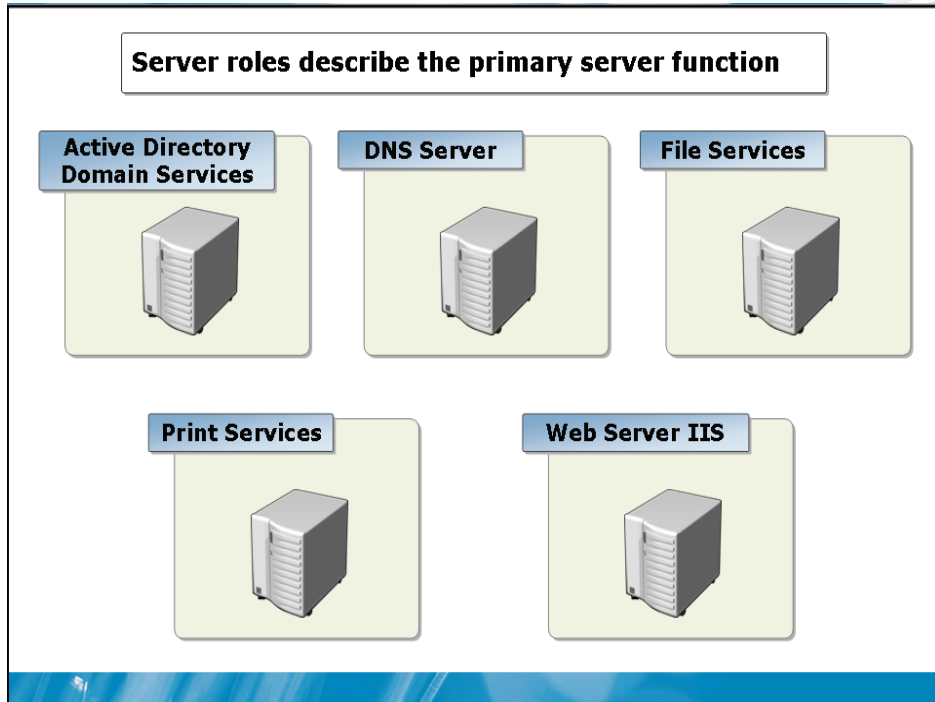
The Windows Server 2008 editions are:

- Windows Server 2008 Web Edition
- Windows Server 2008 Standard Edition
- Windows Server 2008 Enterprise Edition
- Windows Server 2008 Datacenter Edition

Key Points

Windows Server 2008 is available in several editions to meet the needs of various organizations. The editions are available for x86, x64, and Itanium processors.

What Are Server Roles?



Key Points

Server roles are a way to configure a computer running Windows Server 2008 to perform a specific function. In a large enterprise, computers can be configured to perform a single role to ensure sufficient scalability. In a small organization, many roles can be combined on a single computer.

USE PROHIBITED

What Are the Windows Infrastructure Services Roles?

Windows Infrastructures Services roles include:

- Active Directory Certificate Services
- Active Directory Rights Management Services
- DHCP Server
- DNS Server
- Fax Server
- File Services
- Network Policy and Access Services
- Print Services
- Terminal Services
- Windows Deployment Services

Key Points

Windows infrastructure services roles are used to form the underlying framework of software and services that are used by other applications within the organization.

What Are the Windows Application Platform Services Roles?

Windows Application Platform Services roles include:

- Application Server
- UDDI Services
- Web Server (IIS)
- Windows SharePoint Services

Key Points

Windows application platform services roles are used as a platform for the development of applications.

USE PROHIBITED

What Are the Active Directory Roles?

Active Directory roles include:

- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services

Key Points

The Active Directory roles allow you to implement and control Active Directory for your organization.

What Are Server Features?

Server features are supporting services that can be installed

Examples of server features:

- **.NET Framework 3.0**
- **BitLocker**
- **Network Load Balancing**
- **Failover Clustering**
- **Desktop Experience**
- **Windows PowerShell**

Key Points

Server features support server roles or enhance the functionality of a server.

USE PROHIBITED

What Is Server Core?

A server core is an installation of Windows Server 2008 that:

- Has minimal services
- Has no graphical interface
- Increases security
- Can be configured in a limited number of roles

Key Points

Server Core is a new installation option for Windows Server 2008. It provides a minimal environment for running specific server roles. A graphical interface is not included as part of the Server core installation.

Lab: Identifying Network Components

- Exercise 1: Create a Network Diagram
- Exercise 2: Expand the Network Diagram

Estimated time: 30 minutes

Scenario

Margie's Travel is a company that performs travel bookings for clients. There is a single physical location with 20 staff with the following characteristics:

- Staff need to use Microsoft Office applications to create correspondence and perform financial analysis
- Staff require an e-mail and calendaring solution
- Files are shared between staff
- A Web site is used by clients to download travel information
- Some staff require remote access to company data from home
- Wireless access to support network access in the conference room

- ▶ Task 1: Draw a diagram that includes the necessary network components for Margie's Travel.

The network diagram should include:

- A server for sharing files
 - Workstations for users to logon
 - A switch to connect the workstations and server
 - Media connecting the workstations and server to the switch
 - A wireless access point for the boardroom
 - A perimeter network for hosting the Web server used by clients
 - Firewalls to create the perimeter network
 - A remote access server in the perimeter network for VPN connectivity
 - An e-mail server
- ▶ Task 2: Expand the network diagram to include two new branch offices that have been opened in shopping malls.
 - The expanded network diagram should include:
 - Two additional physical locations
 - Routers connecting to the physical locations
 - WAN links between the physical locations

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools

Review Questions

1. Which server role must be installed to configure Windows Server 2008 as a domain controller?
2. How are a switch and a router different?
3. How are large networks with WAN links different from small networks with a single location?
4. What is the relationship between Active Directory domains and Active Directory forests?
5. What is the benefit of the OSI model?

Real-world Issues and Scenarios

1. A single user has called the help desk at 10am. This user is unable to log on to the network. The user has made several attempts between 9am and 10am. Which network components could be the source of the problem?
2. The School of Fine Arts has a film program where students develop their own films. The school would like to use the student films as a promotional method to obtain more students. Potential students will access the content from a Web site. How will you design the network to accommodate the Web server?

Tools

Tool	Use for	Where to find it
Active Directory Users and Computers	Create user accounts	Administrative Tools
Active Directory Domains and Trusts	View and manage trusts	Administrative Tools
Active Directory Sites and Services	View and manage Active Directory sites	Administrative Tools
ADSI Edit	Perform manual edits of Active Directory objects	Administrative Tools
Server Manager	Add server roles and features	Administrative Tools

Module 2

IT Professionals in an Enterprise

Contents:

Lesson 1: IT Professional Roles	2-3
Lesson 2: IT Management and Processes	2-8
Lesson 3: Professional Development for IT Professionals	2-15
Lab: Developing a Training Plan	2-23

MCT USE ONLY
STUDENT USE PROHIBITED

Module Overview

- IT Professional Roles
- IT Management and Processes
- Professional Development for IT Professionals

To be an effective part of an IT support team, you must understand how your job relates to the rest of the IT support organization. This module provides an overview of the roles that are performed by IT professionals in an enterprise. Also, some of the IT management processes and professional development are discussed.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 1

IT Professional Roles

- Discussion: IT Professional Roles
- Job Responsibilities of an Enterprise Administrator
- Job Responsibilities of a Server Administrator
- Job Responsibilities of a Desktop Support Technician

As an IT professional you need to understand the job roles of everyone on your team to ensure that you understand which team member performs which tasks. Some of most common job roles present in an enterprise are: Enterprise Administrator, Server Administrator, and Desktop Support Technician.

MOORE
COURSEWARE
PROHIBITED

Discussion: IT Professional Roles

What are some of the IT professional roles in an enterprise?

Key Points

There is a wide variety of IT professional roles that can be present in an enterprise. Each organization is structured in a slightly different way. Understanding how your organization structures job roles is essential to understanding your own job roles and responsibilities.

Question: What are some of the IT professional roles in an enterprise?

Job Responsibilities of an Enterprise Administrator

An enterprise administrator is typically responsible for:

- ✓ High level tasks
- ✓ Planning
- ✓ Troubleshooting difficult problems
- ✓ Team management

Key Points

Enterprise administrators are technical experts in their organizations that understand a wide range of technologies. However, they do not perform daily maintenance tasks on IT systems. Their time is very valuable and their benefit is maximized by performing high level tasks related to supporting and implementing IT systems.

Question: Why is the role of an enterprise administrator important?

USE PROHIBITED

Job Responsibilities of a Server Administrator

A server administrator is typically responsible for:

- ✓ Daily management of servers
- ✓ Monitoring server performance
- ✓ Resolving server level problems

Key Points

Server administrators are technical experts in supporting servers. They may also be experts in supporting a particular application that runs on their servers.

Question: How is the role of a server administrator different from that of an enterprise administrator?

Job Responsibilities of a Desktop Support Technician

A desktop support technician is typically responsible for:

- Deploying desktop computers**
- Maintaining desktop computers**

A desktop support technician has more user interaction than some job roles

Key Points

A desktop support technician is an expert in supporting the desktop computers used by organizational staff each day. This includes supporting both the operating system and productivity applications such as Microsoft Office.

Question: Describe some of the daily tasks of a desktop support technician.

Lesson 2

IT Management and Processes

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is ITIL?
- What Is MOF?
- What Is an SLA?
- What Is Change Management?
- Incident Management
- Incident and System Documentation

As an IT professional, you need to understand how IT is managed in your organization. When you understand the overall processes used to manage IT in your organization, you can better understand your own role and perform your job more effectively. All IT professionals should understand the processes that are in place to build an effective IT support structure. This module covers some of the more commonly used IT management and processes.

What Is ITIL?

The IT Infrastructure Library (ITIL) is a set of books with best practices for IT service management

Following best practices can:

- Reduce costs
- Improve customer satisfaction
- Improve productivity

Understanding ITIL allows all IT professional roles to increase their performance

Key Points

The IT Infrastructure Library (ITIL) is a set of books with best practices for IT service management. These books are developed and maintained by the United Kingdom's Office of Government Commerce (OGC). There is a large certification and training industry built around ITIL.

Question: How do best practices help professionals in each IT job role perform better?

Additional Resources

- ITIL home page, www.itil.co.uk
- Wikipedia ITIL page, <http://en.wikipedia.org/wiki/ITIL>

USE PROHIBITED

What Is MOF?

Microsoft Operations Framework (MOF):

- Describes proven team structures and operational processes
- Applies best IT practices
- Improves the efficiency and quality of IT operations
- Is based on ITIL

MOF Components:

- Team model
- Process model
- Risk management model

Key Points

The Microsoft Operations Framework (MOF) is a collection of proven team structures and operations processes that apply best practices derived from the experience of Microsoft operations groups, partners, and customers. MOF builds on and extends ITIL.

Question: How does MOF differ from ITIL?

Additional Resources

- Microsoft Operations Framework (MOF) page on the Microsoft Web site, <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/default.mspx>

What Is an SLA?

A service level agreement (SLA) is an agreement between an IT group and an organization that defines expectations for IT system performance

SLA type	Description
Internal	An agreement between two departments within the same organization
External	A formal, legally binding contract
Informal	A verbal agreement between the IT service provider and the organization
Formal	A written, usually signed, agreement

Key Points

A service level agreement (SLA) is an agreement between an IT group and an organization that defines expectations for system performance. When the expectations for performance are not met, the SLA defines the method used for problem resolution.

Question: Why should IT professionals be aware of the SLAs in their organization?

USE PROHIBITED

What Is Change Management?

Change management is the process by which changes are approved, implemented, and monitored

Change management may include:

- A formal process
- A change management board

Change management benefits:

- Better coordination of changes
- Reduced incidents of changes causing unintended results

Key Points

Change management is the process by which changes to IT systems are approved, implemented, and monitored. When a change management process is in place, all system changes must be approved before they are implemented. In smaller organizations, change approvals may be done by a supervisor or an IT manager. In larger organizations, a change management board composed of IT and business representatives may be required to approve the changes.

Question: Why should all IT professionals be aware of the change management process?

Incident Management

The process for managing an incident is defined in an SLA

For example:

- 1** A user calls the help desk
- 2** The Help desk attempts to resolve the problem
- 3** If unresolved after 30 minutes, the problem is escalated to the responsible server administrator
- 4** The server administrator attempts to resolve the problem
- 5** If unresolved after 1 day, the problem is escalated to the enterprise administrator

Key Points

When a system problem occurs there should be a formal process in place for troubleshooting and resolving the problem. The resolution process should include timelines for how long any level of support technician will attempt to work on the problem before passing it along to another person with more expertise. When a formal SLA is in place, the process for managing an incident is defined in an SLA.

Question: Why is it important to have a formal process in place for incident management?

USE PROHIBITED

Incident and System Documentation

Documentation is an essential part of system maintenance

Properly updated documentation simplifies:

- Change management
- Troubleshooting
- Disaster recovery

Key Points

Proper documentation is indispensable for troubleshooting, disaster recovery, and change management. This documentation should be updated during the change management process and can be used when planning changes. Thorough documentation also ensures that a rollback procedure can be attempted if a problem results from a change.

Question: How does documentation help each of the IT professional roles?

Lesson 3

Professional Development for IT Professionals

- Certifications
- Windows Server 2008 Certifications
- Options for Formal Training
- Other Learning Resources
- Microsoft Technical and Support Resources
- Soft Skills for Successful IT Professionals

All professionals have a need for ongoing development of their skills to stay current within their industry. However, the IT industry changes faster than most industries and requires IT professionals to be very active in professional development. IT professionals that do not actively pursue new skills can find themselves with outdated skills and careers that progress slowly.

Certifications

Certifications:

- Show a defined level of expertise with products and technologies
- Offered by many vendors

Microsoft certifications:



Architect Series: The Microsoft Certified Architect program allows companies to easily identify experienced, trusted, IT architects that have completed a rigorous industry-drive peer validation process.



Professional Series: Professional credential validate a comprehensive and current set of skills required to be successful in the job, providing a reliable indicator of performance.

Technology Series: Technology Specialist certifications let you target specific Microsoft technologies and gain in-depth skills for working those technologies.

Key Points

Certifications are a useful tool for IT professionals and their employers. There are certifications available for a wide variety of technologies and offered by many vendors. IT professionals can use certifications as a way to demonstrate expertise with a particular product or technology. Employers can use certifications as a benchmark of technical knowledge that is required for hiring.

Question: Which of these certification types is most relevant to you?

Windows Server 2008 Certifications

MCTS certifications:

- Windows Server 2008 Active Directory Configuration
- Windows Server 2008 Networking Infrastructure Configuration
- Windows Server 2008 Applications Platform Configuration

MCITP

- Server Administrator
- Enterprise Administrator

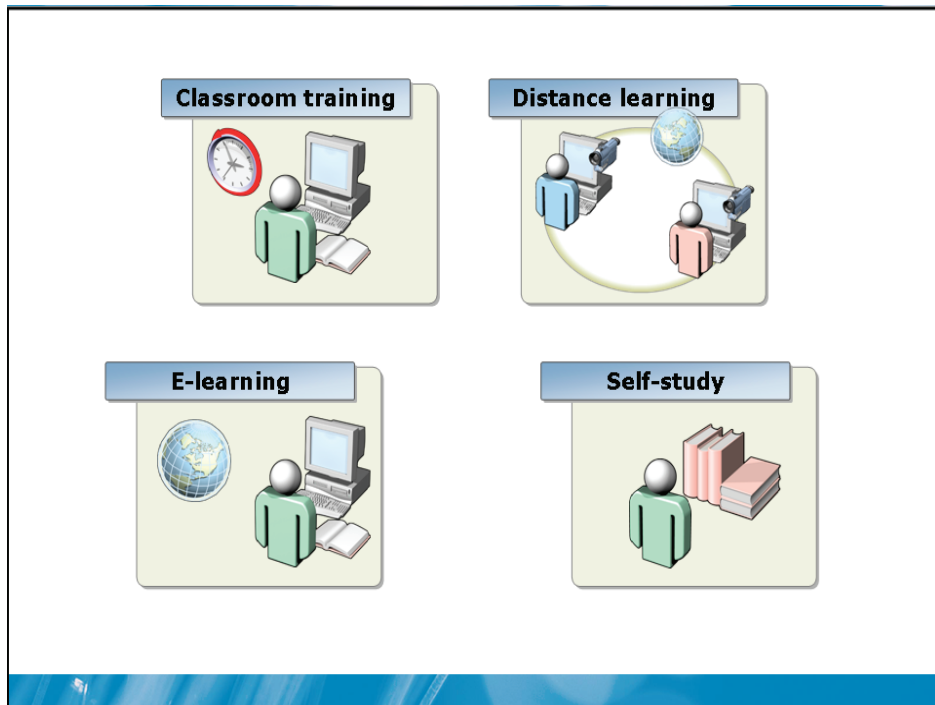
Key Points

There are several Microsoft Certified Technical Specialist (MCTS) and Microsoft Certificate IT Professional (MCTIP) certifications that are relevant to Windows Server 2008. The MCTS certifications require only a single exam. The MCTIP certifications require multiple exams.

Question: Which of these certifications are most relevant to you?

USE PROHIBITED

Options for Formal Training



Key Points

Formal training is training that has been designed to achieve a specific goal. This type of training provides structure for the learning process and is preferred by many students. A variety of formal training methods are available to obtain the knowledge necessary to pass certification exams.

Windows Server 2008 Classroom Courses

The Windows Server 2008 Classroom courses are:

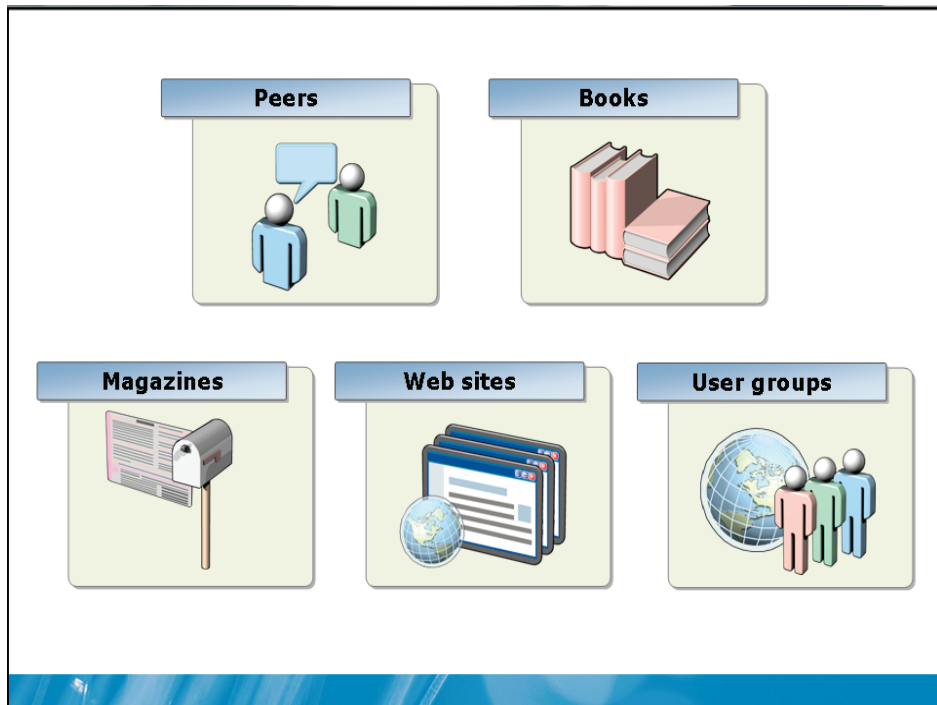
- 6420 Fundamentals of Windows Server 2008 Network Infrastructure and Application Platform
- 6421 Configuring and Troubleshooting a Windows Server 2008 Network Infrastructure
- 6424 Fundamentals of Windows Server 2008 Active Directory
- 6425 Configuring Windows Server 2008 Active Directory Domain Services
- List to be completed

Key Points

Microsoft Learning has created classroom courses to help you get certified and learn the skills you need for your job.

Question: Are there additional Windows Server 2008 classroom courses that you will be taking to meet your career goals?

Other Learning Resources



Key Points

Formal training is a popular option for obtaining new skills and technical knowledge, but there are many other options.

Question: Will you use any of these learning resources to learn about Windows Server 2008?

Microsoft Technical and Support Resources

Microsoft technical and support resources include:

- TechNet
- Microsoft Web site
- Microsoft blogs
- Phone support
- Microsoft consulting

Question: Have you used any of these support resources?

USE PROHIBITED

Soft Skills for Successful IT Professionals

Successful IT professionals have the following non-technical skills:

- Project management
- Organization and prioritization skills
- Teamwork and collaboration
- Verbal communication skills
- Business writing

Key Points

A successful IT profession requires technical skills, but these alone are not enough. There are a number of soft skills that are also important for IT professionals.

Question: Have you used any of these support resources?

Lab: Developing a Training Plan

- Exercise 1: Review Information about Microsoft Learning Resources
- Exercise 2: Create a Training Plan

Estimated time: 30 minutes

Scenario

You are an IT professional with an organization that is planning to implement Windows Server 2008. Based on your personal experience you need to determine the training you require to be successful as an IT professional.

USE PROHIBITED

Exercise 1: Review Information about Microsoft Learning

1. On the host operating system, open Internet Explorer.
2. Visit the Windows Server 2008 – Learning Portal:
<http://www.microsoft.com/learning/windowsserver2008>
3. Visit the New Generations of Microsoft Certifications Web page:
<http://www.microsoft.com/learning/mcp/newgen>
4. Visit the Microsoft Certified Technology Specialist (MCTS) Web page:
<http://www.microsoft.com/learning/mcp/mcts>
5. Visit the Microsoft Certifications for IT Professionals Web page:
<http://www.microsoft.com/learning/mcp/mcitrp>
6. Visit the Web site of your training provider:
Obtain this from your instructor.

Exercise 2: Create a Training Plan

1. Use the training plan document on your student CD as a template.
2. Create a list of the certification you want to obtain.
3. Create a list of additional skills you want to acquire.
4. Create a plan for how to obtain the desired certifications and skills:
 - Include specific learning resources you will use
 - Determine costs for those resources so you can budget appropriately
 - Include a timeline for writing exams and obtaining learning resources

Training Plan—Sample**Desired knowledge:**

Certifications	MCIPT: Server Administrator
Other skills	MOF

Certification plan:

Certification	Exams	Exam Dates
MCTIP: Server Administrator	70-640: TS: Windows Server 2008 Active Directory, Configuring	July 1
	70-642: TS: Windows Server 2008 Network Infrastructure, Configuring	September 1
	70-646: Pro: Windows Server 2008 Administrator	November 1

Training budget:

Exam/Skill	Resource	Cost	Time
70-642	Microsoft course 6420	\$2000	5 days
	Microsoft course 6421	\$2000	5 days
	Review Windows Server 2008 help files	\$0	1 day
	General studying	\$0	5 days
70-640	Microsoft course 6416	\$2000	5 days
	Talk to Greg the AD guy at work	\$0	½ day
	General studying	\$0	5 days
70-646	Review Microsoft best practices from Web site	\$0	5 days
MOF	Review MOF documentation on Microsoft Web site	\$0	3 days

Training Plan—Blank**Desired knowledge:**

Certifications	
Other skills	

Certification plan:

Certification	Exams	Exam Dates

Training budget:

Exam/Skill	Resource	Cost	Time

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Best Practices

Review Questions

1. Which job role is an entry level position most likely to be?
2. Why is having an SLA in place beneficial to IT professionals?
3. Which type of training is the most effective?

Module 3

Configuring Basic TCP/IPv4 Settings

Contents:

Lesson 1: Overview of the TCP/IP Protocol Suite	3-3
Lesson 2: Overview of TCP/IP Addressing	3-10
Lesson 3: Name Resolution	3-15
Lesson 4: Dynamic IP Addressing	3-24
Lesson 5: TCP/IPv4 Tools	3-31
Lab: Configuring Basic TCP/IPv4 Settings and Validating TCP/IPv4 Connectivity	3-37

Module Overview

- Overview of the TCP/IP Protocol Suite
- Overview of TCP/IP Addressing
- Name Resolution
- Dynamic IP Addressing
- TCP/IPv4 Tools

TCP/IPv4 is the most commonly used networking protocol. To effectively support a Windows-based network, you must understand how TCP/IPv4 works from both a conceptual and practical level.

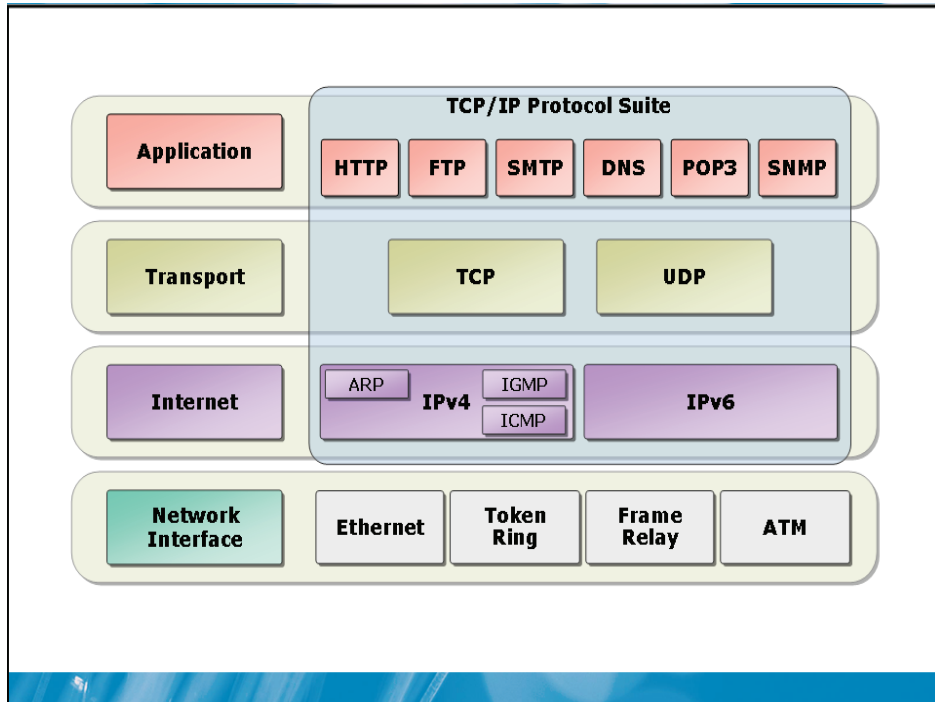
Lesson 1

Overview of the TCP/IP Protocol Suite

- TCP/IP Architecture
- How the TCP/IP Model Relates to the OSI Model
- Transport Layer Protocols
- Common Application Layer Protocols
- What Is an RFC?

Understanding the protocols that are part of the TCP/IP protocol suite is an essential skill to have when reviewing documentation or performing troubleshooting. It is also beneficial to understand the process used to define the protocols so you understand whether protocols are mature enough to be implemented.

TCP/IP Architecture



Key Points

TCP/IP is an industry-standard suite of protocols that provides communication in a heterogeneous network. The tasks performed by TCP/IP in the communication process are distributed between protocols that are organized into four distinct layers of the TCP/IP stack. The four layers of the TCP/IP protocol stack are:

- **Application layer.** Protocols used by applications to access network resources.
- **Transport layer.** Protocols used to control data transfer reliability on the network.
- **Internet layer.** Protocols used to control packet movement between networks.
- **Network interface layer.** Protocols that define how datagrams from the Internet layer are transmitted on the media.

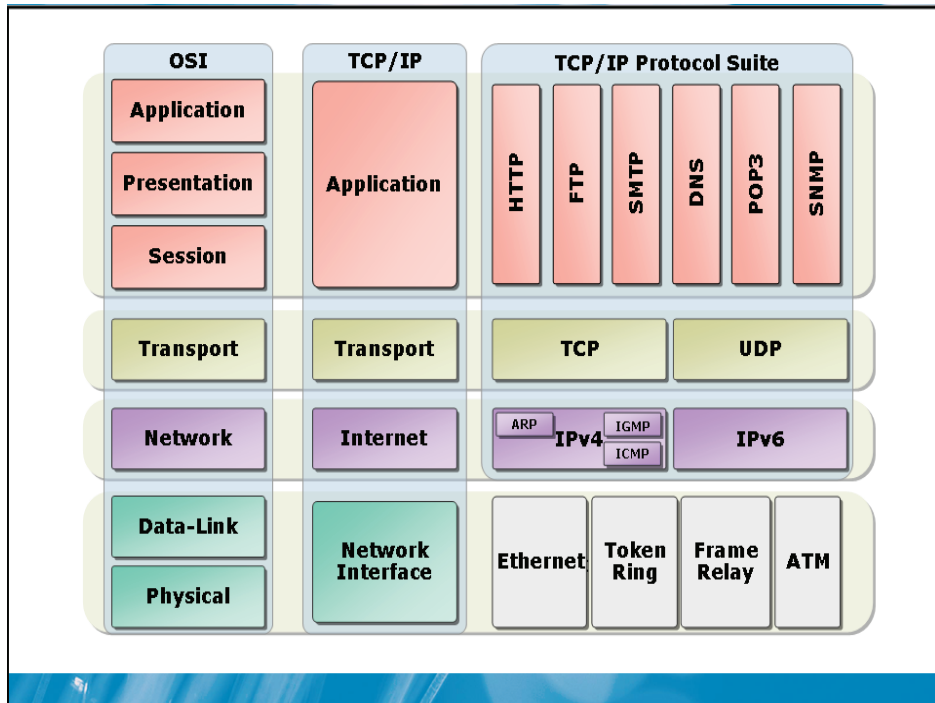
Question: Why is understanding the TCP/IP architecture beneficial to you?

Additional reading

- TCP/IP Fundamentals for Microsoft Windows

MCT USE ONLY. STUDENT USE PROHIBITED

How the TCP/IP Model Relates to the OSI Model



Key Points

The Open System Interconnection (OSI) model defines distinct layers related to packaging, sending, and receiving data transmissions over a network. The layered suite of protocols that form the TCP/IP stack carry out these functions.

Question: Why is it useful to know how the TCP/IP model relates to the OSI model?

Transport Layer Protocols

TCP:

- Connection oriented
- Reliable

UDP:

- Connectionless
- Unreliable

Key Points

The TCP/IP protocol suite offers application programmers the choice of TCP or UDP as a transport layer protocol.

Question: Why is it useful to understand the difference between TCP and UDP?

Common Application Layer Protocols

Some common application layer protocols are:

- HTTP/HTTPS
- RPC over HTTP
- FTP
- RDP
- SMB
- SMTP
- POP3

Key Points

Application layer protocols are used by applications to communicate over the network.

Question: Why is it useful to understand the difference between TCP and UDP?

What Is An RFC?

A Request for Comments (RFC) is description of network functionality

Status levels:

- Required
- Recommended
- Elective
- Limited use
- Not recommended

Maturity levels:

- Proposed standard
- Draft standard
- Internet standard

Key Points

The standards for TCP/IP are developed in a series of documents called requests for comments (RFCs).

Question: Why is it important to understand RFCs?

Additional Reading

A complete list of RFCs is available from the IETF web site

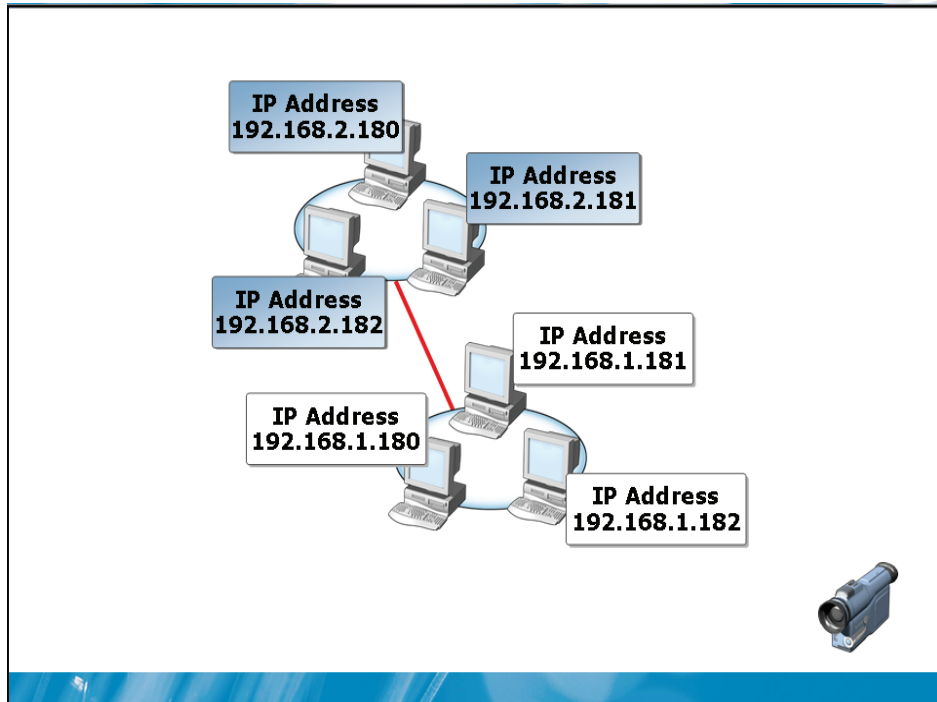
Lesson 2

Overview of TCP/IP Addressing

- The Components of an IP Address
- What Is a Subnet Mask?
- What Is a Default Gateway?
- What Is DNS?
- Demonstration: Configuring a Static IP Address

IP addressing is an essential skill for network administrators. Understanding IP addressing is required to troubleshoot network communication between clients and servers or connectivity to the Internet.

Multimedia: The Components of an IP Address



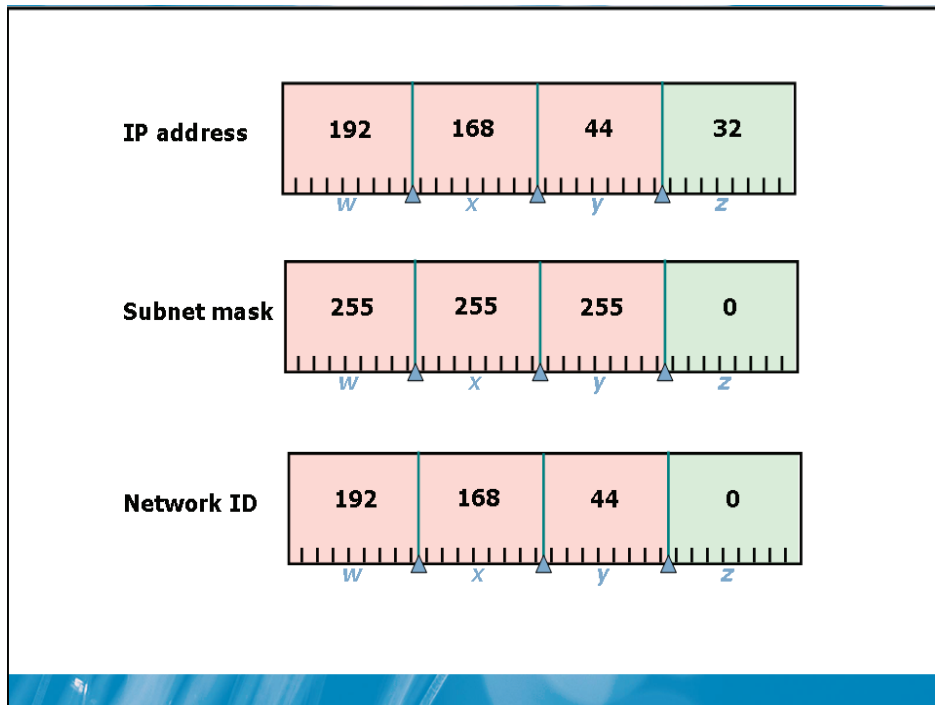
This multimedia describes:

- What a media access control (MAC) address is
- Why IPv4 addresses are required
- The structure of IPv4 addresses

Question: What are the two components of an IP address?

USE PROHIBITED

What Is a Subnet Mask?



Key Points

A subnet mask defines the part of an IP address that is the network ID and the part of an IP address that is the host ID. A subnet mask is composed of four octets, similar to an IP address.

Question: If a computer has an IP address of 172.31.99.220 and a subnet mask of 255.255.0.0, what is the network ID and host ID?

What Is a Default Gateway?

The default gateway:

- Is used to route packets to other networks
- Is used when the internal routing table on the host has no information about the destination subnet

Use DHCP to automatically deliver the IP address for the default gateway to the client

Key Points

A default gateway is a device, usually a router, on a TCP/IP internetwork that can forward IP packets to other networks. An internetwork is a group of networks that are connected by routers.

Question: What symptom will occur if computers are not configured correctly with a default gateway?

USE PROHIBITED

What Is DNS?

DNS is used to:

- Resolve host names to IP addresses
- Locate domain controllers and global catalog servers
- Used to resolve IP addresses to host names
- Used to locate mail servers during e-mail delivery

Key Points

Domain Name System (DNS) is a service that manages the resolution of host names to IP addresses.

Demonstration: Configuring a Static IP Address

In this demonstration, you will see how to configure a static IPv4 address

Question: In the properties of which component do you configure a static IP address?

MOCK COURSEWARE USE PROHIBITED


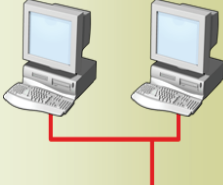
Lesson 3

Name Resolution

- Types of Names that Computers Use
- What Are DNS Zones and Records?
- How Internet DNS Names are Resolved
- Host Name Resolution Process
- Demonstration: Configuring Host Name Resolution
- What Is WINS?
- NetBIOS Name Resolution Process

Name resolution is an essential part of computer networking because people are much better at remembering names than abstract numbers like an IP address. Name resolution is responsible for converting computer names to IP addresses so that users do not need to remember computer addresses.

Types of Names That Computers Use

Name	Description
 <p>Host names</p>	<ul style="list-style-type: none"> • Up to 255 characters in length • Can contain alphabetic and numeric characters, periods, and hyphens • Part of FQDN
 <p>NetBIOS names</p>	<ul style="list-style-type: none"> • Represent a single computer or group of computers • 15 characters used for the name • 16th character identifies service • Flat namespace

Key Points

The name type used by an application is determined by the application developer. Windows operating systems allow applications to request network services through Windows Sockets, Winsock Kernel, or NetBIOS.

Question: When would you be required to support NetBIOS names on your network?

What Are DNS Zones and Records?

A DNS zone is a specific portion of DNS namespace that can contain DNS records

Records in forward lookup zones include:

- A
- SRV
- MX
- CNAME

Records in reverse lookup zones include:

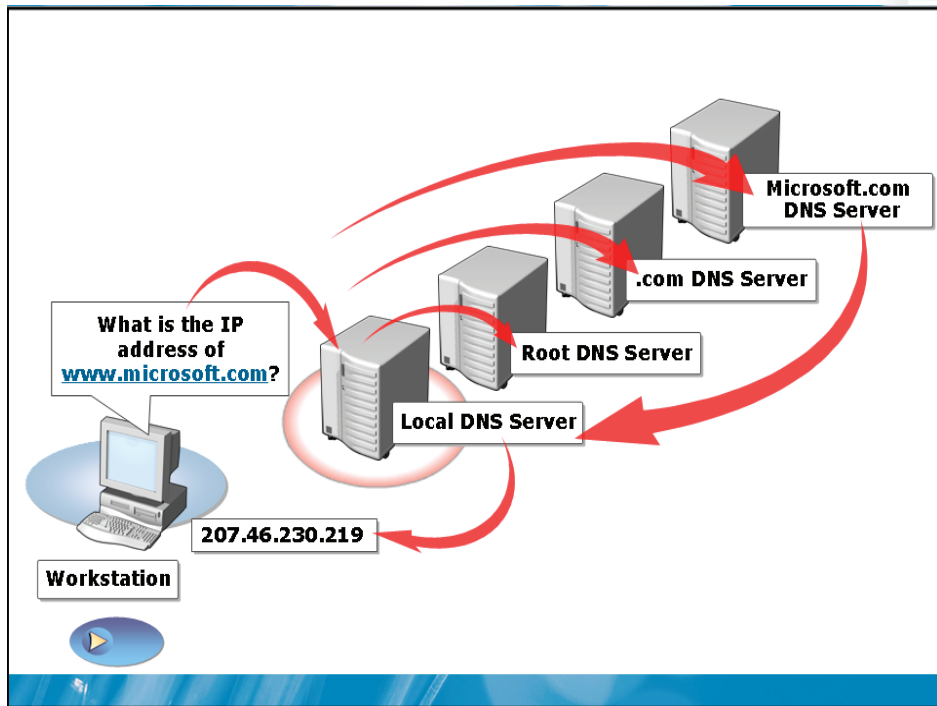
- PTR

Key Points

A DNS zone is a specific portion of DNS namespace that can contain DNS records.

Question: Which computers in your organization should have an A record configured?

How Internet DNS Names are Resolved



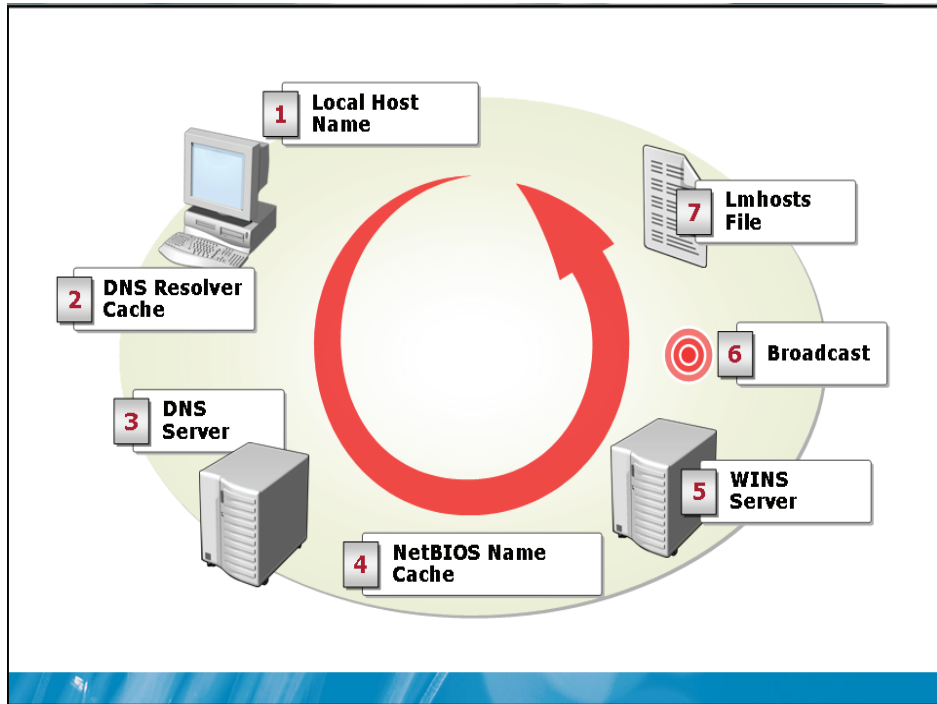
Key Points

When DNS names are resolved on the Internet, an entire system of computers is used rather than just a single server.

Question: Why is understanding the DNS name resolution process important?

USE PROHIBITED

The Host Name Resolution Process



Key Points

When an application uses Windows Sockets and a host name is specified, TCP/IP will use the DNS resolver cache and DNS when attempting to resolve the host name.

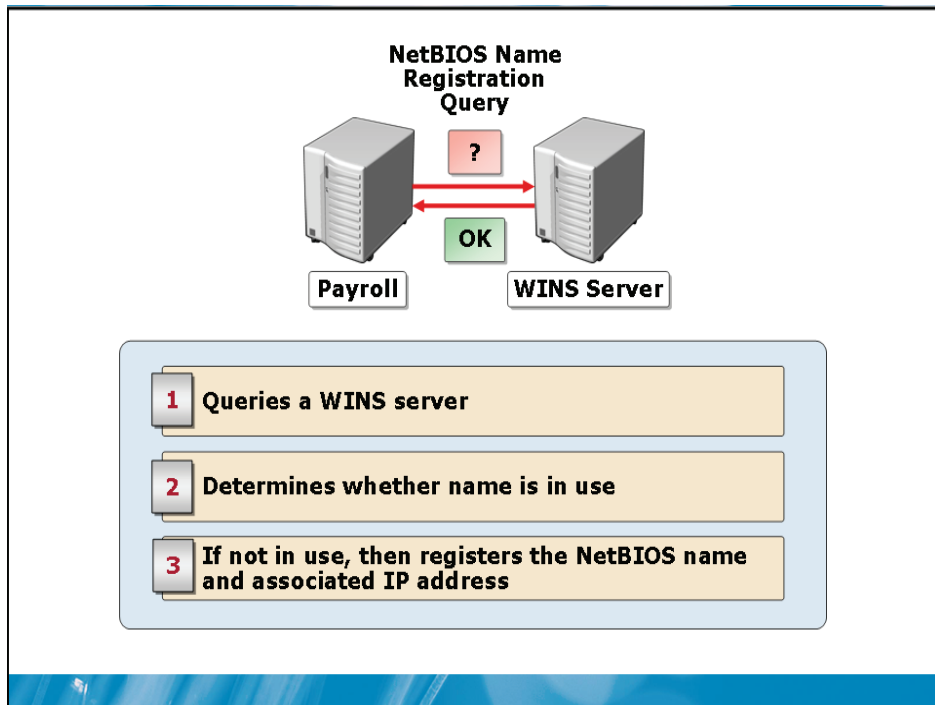
Demonstration: Configuring Host Name Resolution

In this demonstration, you will see how to configure host name resolution

Question: Under what circumstances will a resolved host name be added to the DNS resolver cache?

USE PROHIBITED

What Is WINS?

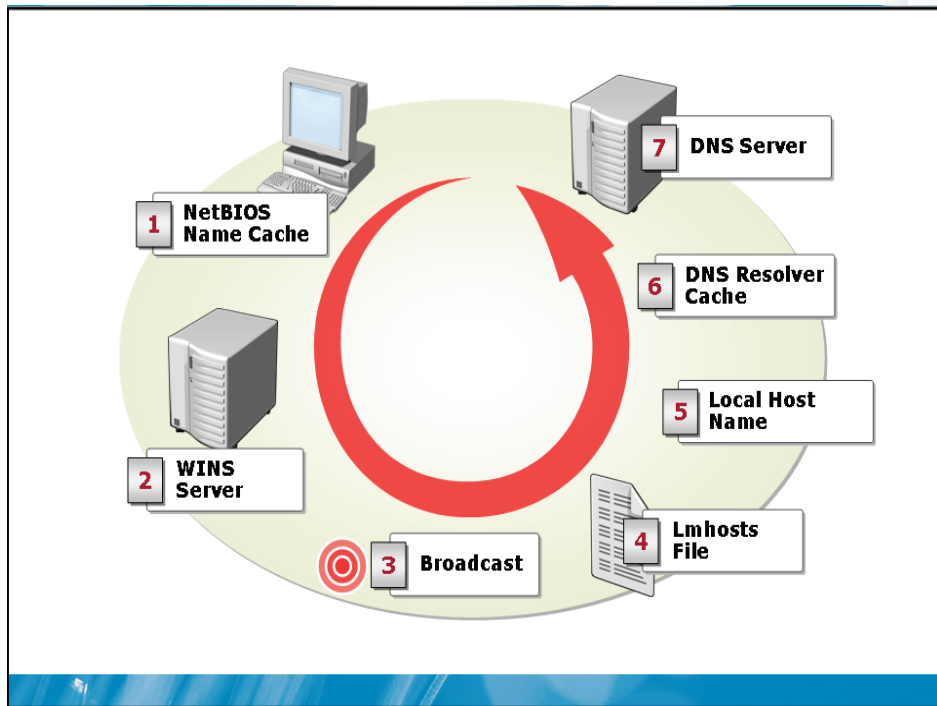


Key Points

Windows Internet Naming Service (WINS) is a NetBIOS name server that you can use to resolve NetBIOS names to IP addresses.

Question: When should WINS be used on a network?

The NetBIOS Name Resolution Process



Key Points

The NetBIOS name resolution process varies, depending on the NetBT node type that is specified on the computer.

USE PROHIBITED

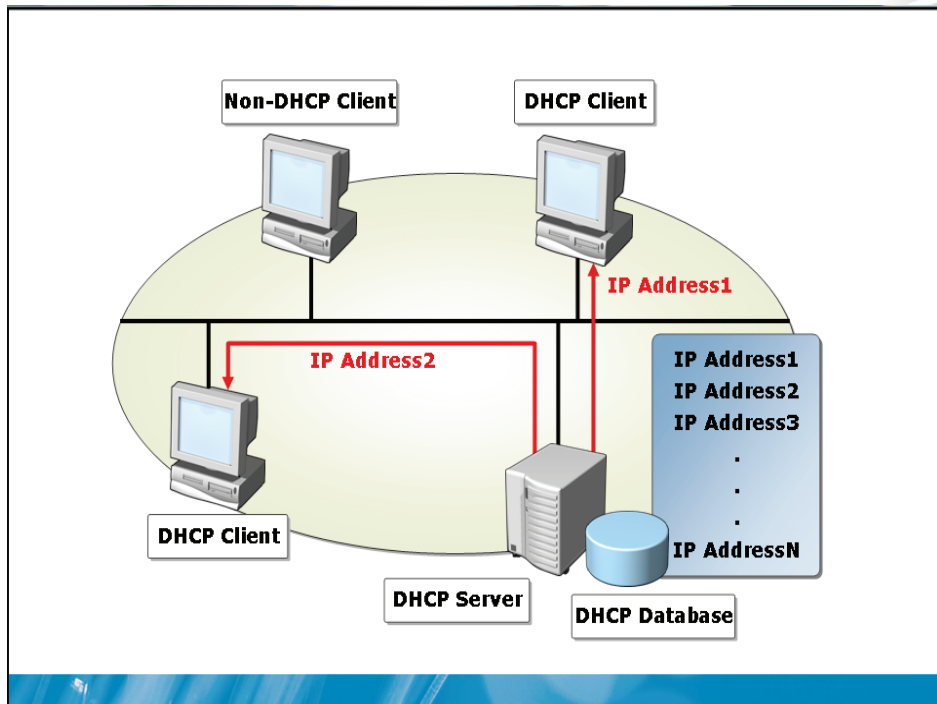
Lesson 4

Dynamic IP Addressing

- What Is DHCP?
- DHCP Address Renewal
- DHCP Configuration Options
- What Is Alternate Configuration?
- What s Automatic Private IP Addressing?
- Demonstration: Configuring Dynamic IP Addressing

Most servers and other devices on a network, such as printers, are configured with static IP addresses. This ensures that clients are able to locate them. Client computers typically use dynamic IP addressing. The makes it easier to add and remove clients from the network.

What Is DHCP?



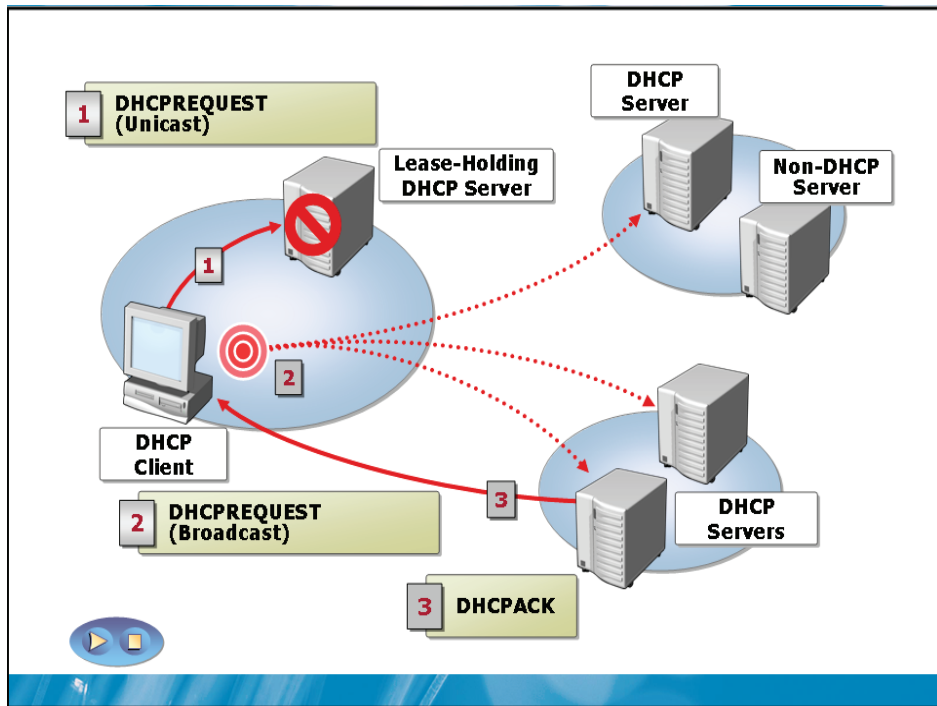
Key Points

DHCP is a service and a protocol that work together to automatically assign IP addresses and other configuration settings to the computers on a network. DHCP dynamically assigns IP addresses to clients from a pool of addresses.

Question: Which computers and devices will not have an address assigned by DHCP?

USE PROHIBITED

DHCP Address Renewal



Key Points

The length of an IP address lease is typically measured in days and is generally based on whether computers are frequently moved around the network or whether IP addresses are in short supply.

Question: If you are planning changes to the IP structure of your network, will you make the lease time longer or shorter?

DHCP Configuration Options

DHCP configuration options include:

- Creating scopes
- Start and end IP addresses
- Subnet mask
- Lease duration
- Router
- DNS server
- Exclusions
- Reservations

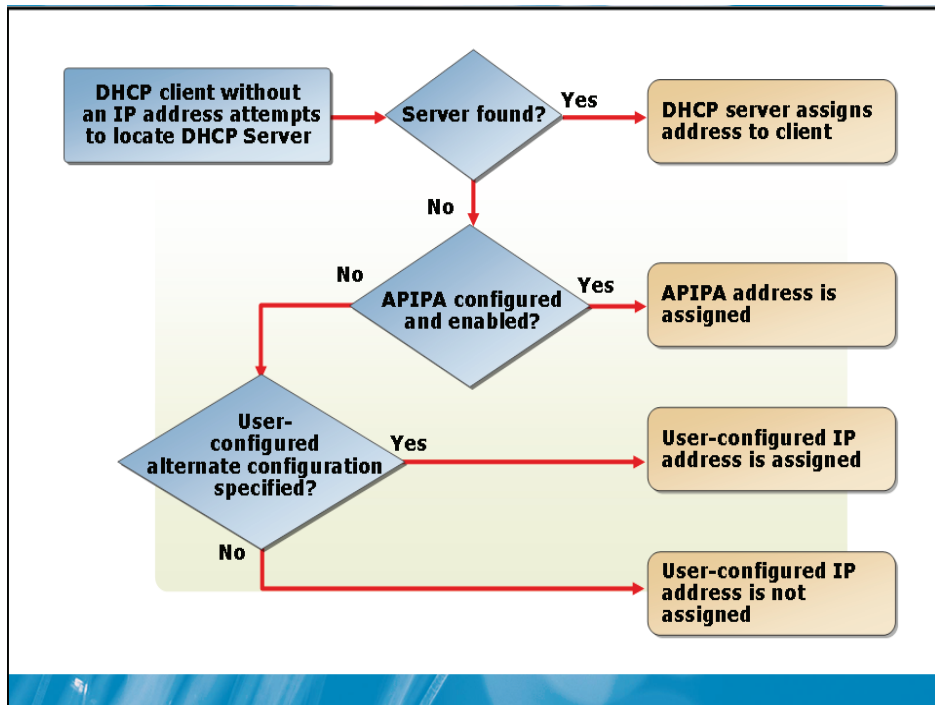
Key Points

When Windows Server 2008 is configured as a DHCP server, the IP addresses are organized into scopes.

Question: Why is it important to configure DHCP options such as router and DNS server?

USE PROHIBITED

What Is Alternate Configuration?



Key Points

Alternate configuration is a system used to assign IPv4 addresses to clients when a DHCP server is unavailable.

Question: When is User-Configured Alternate Configuration useful?

What Is Automatic Private IP Addressing?

Automatic private IP addressing (APIPA):

- Is used if a DHCP server cannot be contacted
- Assigns IP addresses on the 169.254.0.0/16 network
- Cannot be used with:
 - Active Directory
 - Internet connectivity
 - Multiple subnets
 - DNS or WINS servers

Key Points

APIPA assigns an IPv4 address on the 169.254.0.0 network when a computer configured to obtain a DHCP lease cannot communicate with a DHCP server.

Question: Why is APIPA not suitable for use with Active Directory?

USE PROHIBITED

Demonstration: Configuring Dynamic IP Addressing

In this demonstration, you will see how to configure dynamic IP addressing

Question: What is the relationship between APIPA and User-Configured Alternate Configuration?

Lesson 5

TCP/IPv4 Tool

- What Is IPConfig?
- What Is NETStat?
- What Is NBTStat?
- What Is Netsh?
- Demonstration: Using TCP/IPv4 Tools

Windows Server 2008 includes a number of tools to help troubleshoot and configure an IPv4 network. These tools include: IPConfig, NETStat, NBTStat, and Netsh. Understanding how these tools work will improve your skills in troubleshooting Windows Server 2008 and IPv4.

What Is IPConfig?

IPConfig is used to display IP configuration information and control the DNS resolver cache

Option	Description
/all	Displays all IP address configuration information
/release	Releases a dynamic IPv4 address lease
/renew	Renews a dynamic IPv4 address lease
/flushdns	Purges the DNS resolver cache
/registerdns	Refreshes DHCP leases and re-registers DNS names
/displaydns	Displays the contents of the DNS resolver cache

Key Points

IPConfig is used to display IPv4 and IPv6 configuration information and control the DNS resolver cache.

Question: What is the most common task that IPConfig is used for?

What Is NETStat?

NETStat is used to display protocol statistics and current TCP/IP network connections

Option	Description
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection and listening port
-e	Displays Ethernet statistics
-r	Displays the routing table
-s	Displays per protocol statistics

Key Points

NETStat is a utility that is used to display protocol statistics and current TCP/IP network connections.

Question: When would you use NETStat?

USE PROHIBITED

What Is NBTStat?

NBTStat is used to display NetBIOS information on the local computer

Option	Description
-a	View NetBIOS information for a specific NetBIOS name
-c	View the local cache of machine names and their IP addresses
-n	View local NetBIOS names
-R	Purges and reloads the remote cache name table
-s	Lists sessions table by using IPv4 addresses

Key Points

NBTStat is a utility that is used to display NetBIOS information on the local computer. You can view and manipulate the NetBIOS name cache and view connections.

Question: When would you purge and reload the remote name cache table?

What Is Netsh?

Netsh is a command-line utility that is used to configure and monitor network settings

You can configure and monitor:

- Windows Firewall
- IP settings
- Interface settings
- IPsec

Key Points

Netsh is a command-line and scripting utility for networking components for local or remote computers.

Question: How can Netsh be useful for managing Server Core installations of Windows Server 2008?

USE PROHIBITED

Demonstration: Using TCP/IPv4 Tools

In this demonstration, you will see how to use:

- IPConfig
- NETStat
- Netsh

Question: How will you use each of the TCP/IPv4 tools?

Lab: Configuring Basic TCP/IPv4 Settings and Validating TCP/IPv4 Connectivity

- Exercise 1: Configuring a Dynamic IP Address
- Exercise 2: Configuring a Static IP Address
- Exercise 3: Testing DNS Configuration
- Exercise 4: Connecting to a Web Application

Virtual machine	NYC-DC1, NYC-CL1, NYC-WEB
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario:

You are a desktop support technician for Woodgrove Bank. You are responsible for configuring desktop computers before they are delivered to clients. In addition, you are also involved in the testing of new applications before they are rolled out to clients.

Exercise 1: Configuring a Dynamic IP Address

Scenario:

In the financial analysis department, all desktop computers are configured with a dynamic IP address. A new computer has been prepared for a client a now needs to be configured to use a dynamic IP address.

- ▶ Task 1: Verify DHCP configuration
 1. On NYC-DC1, log on as Administrator with a password of Pa\$\$w0rd.
 2. Open the DHCP administrative tool.
 3. View the properties of the HeadOffice scope.
 4. Review the following settings:
 - Address Pool
 - Scope Options
- ▶ Task 2: Configure a dynamic IP address
 1. On NYC-CL1, log on as Administrator with a password of Pa\$\$w0rd.
 2. Open the properties of Local Area Connection in Network and Sharing Center.
 3. Open the properties of Internet Protocol Version 4 (TCP/IPv4).
 4. Select the options to:
 - Obtain an IP address automatically
 - Obtain DNS server address automatically
- ▶ Task 3: Verify Connectivity
 1. On NYC-CL1, open a command prompt.
 2. Use IPConfig /all to verify the static IP address.
 3. Use the ping command to test connectivity to the server:
 - Server IP address: 10.10.0.10
 4. Browse to the server NYC-DC1 over the network to verify connectivity.

Exercise 2: Configuring a Static IP Address

Scenario:

To increase security in the financial analysis department, all desktop computers are being configured with static IP addresses. This will allow firewalls to control access to some resources. You must configure a desktop computer with a static IP address and verify its functionality afterwards.

- ▶ Task 1: Configure a static IP address
 1. On NYC-CL1, open the properties of Local Area Connection in Network and Sharing Center.
 2. Open the properties of Internet Protocol Version 4 (TCP/IPv4).
 2. Configure a static IP address by using the following settings:
 - IP address: **10.10.0.50**
 - Subnet mask: **255.255.255.0**
 - Default gateway **10.10.0.1**
 - Preferred DNS server: **10.10.0.10**
- ▶ Task 2: Verify Connectivity
 1. On NYC-CL1, open a command prompt.
 2. Use IPConfig /all to verify the static IP address.
 3. Use the ping command to test connectivity to the server.
 - Server IP address: **10.10.0.10**
 4. Browse to the server NYC-DC1 over the network to verify connectivity.

Exercise 3: Testing DNS Configuration

Scenario:

A new Web-based application is being implemented for the financial analysis department of Woodgrove bank. Users accessing this application will be using the FQDN finance.woodgrovebank.com. You must verify that this DNS name resolves to the IP address 10.10.0.21.

► Task 1: Test DNS resolution

1. On NYC-CL1, open a command prompt.
2. Use the ping command to test connectivity to the server:
 - Server name: **finance.woodgrovebank.com**

This is unsuccessful.

3. Use the ping command to test connectivity to the server:
 - Server IP address: **10.10.0.21**

This is successful.

► Task 2: View and configure DNS records

1. On NYC-DC1, open the DNS administrative tool.
2. View the WoodgroveBank.com forward lookup zone.
The *finance.WoodgroveBank.com* host record does not exist.
3. Create the *finance.WoodgroveBank.com* host record:
 - Name: **finance**
 - IP address: **10.10.0.10**

► Task 3: Verify DNS resolution

1. On NYC-CL1, open a command prompt.
2. Use the ping command to test connectivity to the server.
 - Server name: **finance.woodgrovebank.com**

This is unsuccessful.

3. Open a command prompt with administrative privileges.

4. Use IPConfig to clear the DNS resolver cache:
 - **Ipconfig /flushdns**
5. Use the ping command to test connectivity to the server:
 - Server name: **finance.woodgrovebank.com**

This is successful.

6. Use the nslookup command to verify the host record:
 - **Nslookup finance.woodgrovebank.com**

This command responds with the IP address 10.10.0.10

Exercise 4: Connecting to a Web Application

Scenario:

A new Web-based application has been installed for the financial analysis department. However, when users attempt to access the application they are receiving an error. The application uses port 8080. You must verify that the Web server is configured correctly.

- ▶ **Task 1: Verify the Web site configuration**
 1. On NYC-WEB, open the Internet Information Services (IIS) Manager administrative tool.
 2. View the port number being used by the Default Web site.
 - Edit the bindings
 - Port 8080 is used by the Default Web site
 3. Open a command prompt.
 4. Use NETStat to view whether port 8080 is in use.
 - **-a** to view all listening ports

► Task 2: Test the Web-based application

1. On NYC-CL1, open Internet Explorer.
2. Access the URL for the web-based application:
 - **<http://finance.woodgrovebank.com>**

Attempting to access this web page returns an error.

3. Access the URL for the web-based application:
 - **<http://finance.woodgrovebank.com:8080>**

Attempting to access this web page is successful.

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Best Practices
- Tools

Review Questions

1. Can one application use TCP port 80 while another uses UDP port 80?
2. What TCP/IP configuration option determines which part of the IP address is network address?
3. How are the contents of the Hosts file used for name resolution?
4. Which TCP/IP tools can you use to view the configuration of TCP/IP?
5. How are reservations and exclusions used when configuring a DHCP server?

Real-world Issues and Scenarios

- A newly deployed PC is able to communicate with computers on the local subnet but not on remote subnets. Which TCP/IP configuration option is likely configured incorrectly?
- A computer is configured with the IP address 172.16.87.43 and the subnet mask 255.255.255.0. What is the network address of the computer?
- As part of configuring a new application server, you have created a host record for the server. During your testing you realized that the host record was pointing at an incorrect IP address. You have just modified the incorrect host record on your company DNS server, but are still unable to communicate with the new application server. Why are you still unable to communicate with the new application server?

Best Practices

- Supplement or modify the following best practices for your own work situations:
- Use DHCP to assign IP addresses to client computers.
- Assign static IP addresses to network servers and other devices
- Use exclusions to prevent DHCP from leasing out IP addresses that have been statically assigned.
- Clearly document all IP addresses that have been statically assigned.
- Use a consistent convention for assigning static IP addresses. For example, the first 50 addresses on a network could be reserved allocation as static addresses.

Tools

Tool	Use for	Where to find it
DNS	<ul style="list-style-type: none"> • Create DNS records and zones 	Administrative Tools
DHCP	<ul style="list-style-type: none"> • Configure and manage DHCP servers 	Administrative Tools
IPConfig	<ul style="list-style-type: none"> • View IP configurations • Flush the DNS resolver cache • Release and renew dynamic IP addresses 	Command Prompt
NETStat	<ul style="list-style-type: none"> • Display protocol statistics • Display network connections 	Command Prompt
NBTStat	<ul style="list-style-type: none"> • Display NetBIOS information 	Command Prompt
Netsh	<ul style="list-style-type: none"> • Configure and monitor network configuration 	Command Prompt
NSLookup	<ul style="list-style-type: none"> • View DNS records 	Command Prompt

NOT FOR STUDENT USE ONLY. STUDENT USE PROHIBITED

Module 4

Fundamentals of Communication Technologies

Contents:

Lesson 1: Network Content Types

4-3

Lesson 2: Packet Delivery Method

4-8

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Network Content Types
- Packet Delivery Methods

Multiple types of content can be delivered over a computer network by using various delivery methods. You need to understand both the content types and delivery methods to manage a Windows Server® 2008 network.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 1

Network Content Types

- What Is Static Content?
- What Is Dynamic Content?
- What Is Streaming Content?
- Demonstration: Network Content Types

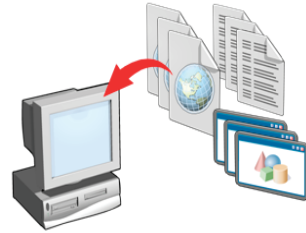
Content can be transmitted to computers over a network by using unicast, multicast, or broadcast delivery. Understanding when these delivery methods are used is essential for troubleshooting and designing your network.

What Is Static Content?

Static content is the same for all users that view it

Examples of static content are:

- Basic HTML Web pages
- Word documents
- PowerPoint slides



Key Points

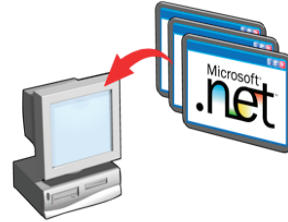
Static content is data that is the same for all users that view it. It does not change based on where the users connect from or which user is connected. This is the most common type of data on computer networks.

Question: Are most Web pages static content?

What Is Dynamic Content?

Dynamic content is

- Generated by the server at the time it is accessed
- Can vary for each user
- ASP and ASP.NET



Examples:

- A Web page that includes a user's name in the upper right corner when logged on
- A Web page that displays the IP address of a user accessing content
- A Web page that changes content to match the demographics of a user

Key Points

Dynamic content is data that can be different each time it is accessed by a user. This content can change depending on variables such as which user is accessing the content, or the user's location. This type of content is most commonly found in Web sites and Web-based applications.

Question: What are some administrator concerns about dynamic content?

USE PROHIBITED

What Is Streaming Content?

Streaming content is

- Delivered at the speed required for playback
- Provided by Windows Media Services



Examples:

- Online radio station
- Viewing online videos

Key Points

Streaming content is data that is delivered to users at the speed required for playback. Non-streaming content is delivered to users at the fastest possible speed that the client, servers, and network can support. This can lead to increases in network traffic and cause network congestion. Windows Server 2008 and Microsoft Windows® Media Services provide support for streaming content.

Question: Can a Word document be delivered as streaming content?

Demonstration: Viewing Network Content Types

In this demonstration, you will see static and dynamic content

Question: What is the relationship between the content of a Web page and what the client receives?

USE PROHIBITED

Lesson 2

Packet Delivery Method

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is Unicast Packet Delivery?
- What Is Broadcast Packet Delivery?
- Scenarios for Broadcast Packet Delivery
- What Is Multicast Packet Delivery?
- Scenarios for Multicast Packet delivery
- Demonstration: Viewing of Packet Delivery Methods

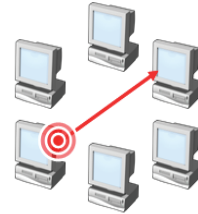
A computer network is used to deliver content to hosts. Understanding the characteristics of the various content types will allow you to plan your network appropriately.

What Is Unicast Packet Delivery?

Unicast packet delivery is performed directly between two hosts

Unicast packet delivery is used for:

- DNS lookups
- Accessing Web sites
- File transfers
- Logons



Key Points

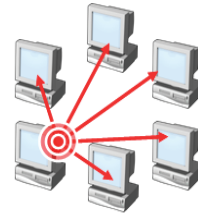
Unicast packet delivery is the delivery of a packet from one host to only one other host. This is the most common type of packet delivery on networks, as most communication is the delivery of data between two computers.

Question: Can you think of other examples where unicast packet delivery is used?

What Is Broadcast Packet Delivery?

Broadcast packet delivery is from one host to all hosts on a network

- The last IPv4 address on a network is the broadcast address
- Broadcasts are not forwarded by routers
- In special cases, a broadcast can be sent to a remote network



Examples:

- 255.255.255.255 – broadcast on local network
- 192.168.1.255 – broadcast on 192.168.1.0 network

Key Points

Broadcast packet delivery is from one host to all other hosts on a network. The destination IP address of a broadcast packet is the last available IP address on the network. This IP address is recognized by all hosts as being the broadcast address and all hosts listen for packets addressed to this IP address.

Question: Why is it important that packets addressed to 255.255.255.255 are not forwarded by routers?

Scenarios for Broadcast Packet Delivery

Some common scenarios for broadcast packet delivery are:

- DHCP
- NetBIOS name resolution
- ARP

Key Points

Broadcast packet delivery is used when an application needs to communicate with many hosts at once or when the IP address of the destination host is unknown.

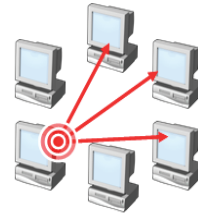
Question: Do DHCP renewals use broadcast packets?

USE PROHIBITED

What Is Multicast Packet Delivery?

Multicast packet delivery is from one host to a group of hosts

- All computers in a multicast group use the same multicast IPv4 address
- IPv4 address range: 224.0.0.0-239.255.255.255
- Hosts can have multiple multicast addresses
- Multicast addresses are selected by the applications using the address
- Routers can be configured to route multicast packets



Key Points

Multicast packet delivery is from one host to a group of hosts. The hosts in the destination group do not all need to be on the same subnet. Multicasting allows the forwarding of multicast packets by routers. However, many routers do not forward multicast packets by default. Routers on the Internet do not forward multicast packets.

Question: Why are multicast packets better to use than broadcast packets?

Scenarios for Multicast Packet Deliver

Common scenarios for multicast packet delivery are:

- Windows Deployment Services
- Windows Media Services

Key Points

Multicast packet delivery allows a single packet of data to be delivered to a group of computers. This is much more efficient than unicast delivery to a group of computers where the packet must be delivered one time to each computer.

Question: Are there any limitations when using multicast packets to deliver content from Windows Media Services?

USE PROHIBITED

Demonstration: Viewing Packet Delivery Methods

In this demonstration, you will see how packet delivery methods vary when viewed by using Network Monitor

Question: Why would you use Network Monitor 3.0 to view network communication?

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools

Review Questions

1. How does streaming content prevent network congestion?
2. Where is a packet delivered when it is addressed to 255.255.255.255?

Real-world Issues and Scenarios

- Your network consists of a head office and two branch offices connected by wide area network (WAN) links. In the head office, there are four subnets. You have configured a new computer running Windows Server 2008 and have installed Windows Media Services. You want to deliver multimedia presentations in the head office by using multicast delivery. However, you are concerned that the multimedia presentations will overwhelm your WAN links and interfere with network traffic to the branch offices. How can you prevent multicast packets from traversing the WAN links?

You are responsible for maintaining the Web server that hosts the external Web site for your organization. The original Web site was developed on 2001 and has been running exceptionally well. The memory and processor utilization on the server have been very low. A new version of the Web site has been developed by a third party, and now processor and memory utilization are very high. What is the likely cause of the increased utilization?

Tools

Tool	Use to	Where to find it
Network Monitor 3.0	Troubleshooting by viewing network packets	http://blogs.technet.com/netmon/

Module 5

TCP/IPv4 Fundamentals

Contents:

Lesson 1: Overview of IPv4 Communication

5-3

Lesson 2: Subnetting Overview

5-9

Lesson 3: Subnetting for Complex Networks

5-14

Lab: Creating IPv4 Address Spaces

5-19

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Overview of IP Communication
- Overview of Subnetting
- Subnetting for Complex Networks

Large organizations begin their network design with a large Internet Protocol version 4 (IPv4) address space that must be subdivided into smaller portions for each location. This module describes how to subdivide an IPv4 address space based on factors such as the number of hosts in each location.

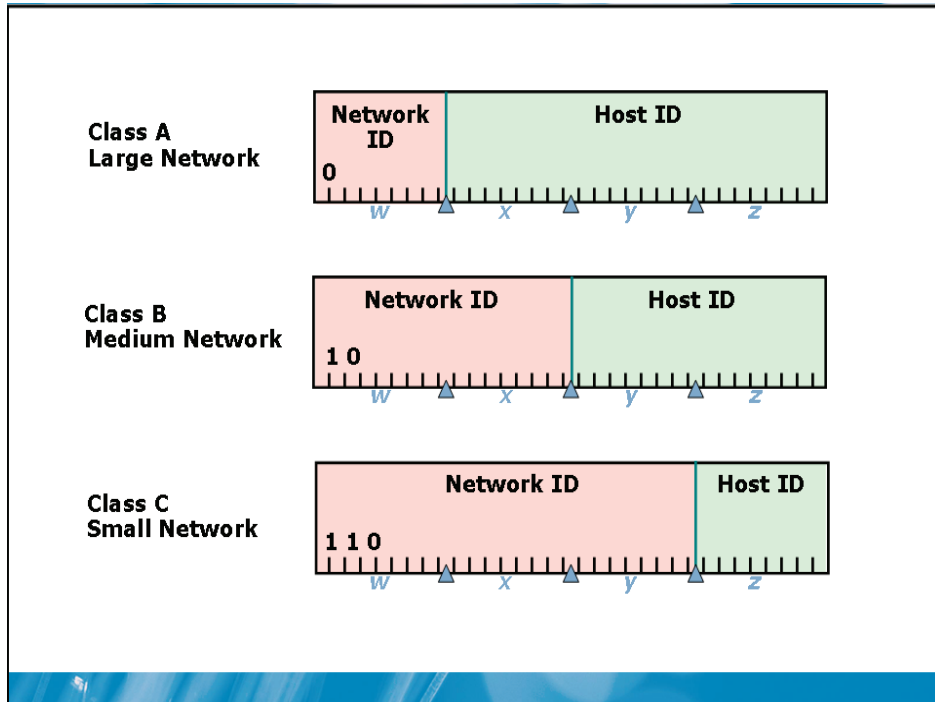
Lesson 1

Overview of IPv4 Communication

- What Are the IPv4 Address Classes?
- What Is ARP?
- IPv4 Communication within a Single Network
- IPv4 Communication Between Networks
- Demonstration: Using ARP

When you subdivide a large IPv4 address space into smaller portions, you must decide how many smaller networks to create. Your decision is guided by the requirements for controlling communication between computers on your network. Understanding the IP communication process, as well as the IPv4 address classes, will help you make the appropriate decisions when subdividing large IPv4 address spaces.

What Are the IPv4 Address Classes



Key Points

IP addresses are organized into classes. You obtain registered addresses through an Internet service provider (ISP). Your ISP obtains addresses from a regional Internet registry. The number of hosts on your network determines the class of addresses that are required.

Question: Why is it important to know the IPv4 address classes?

What Is ARP?

The ARP protocol:

- Resolves IPv4 addresses to MAC addresses
- Provides MAC addresses for IP frames
- Dynamically stores MAC addresses in the ARP cache

The ARP tool:

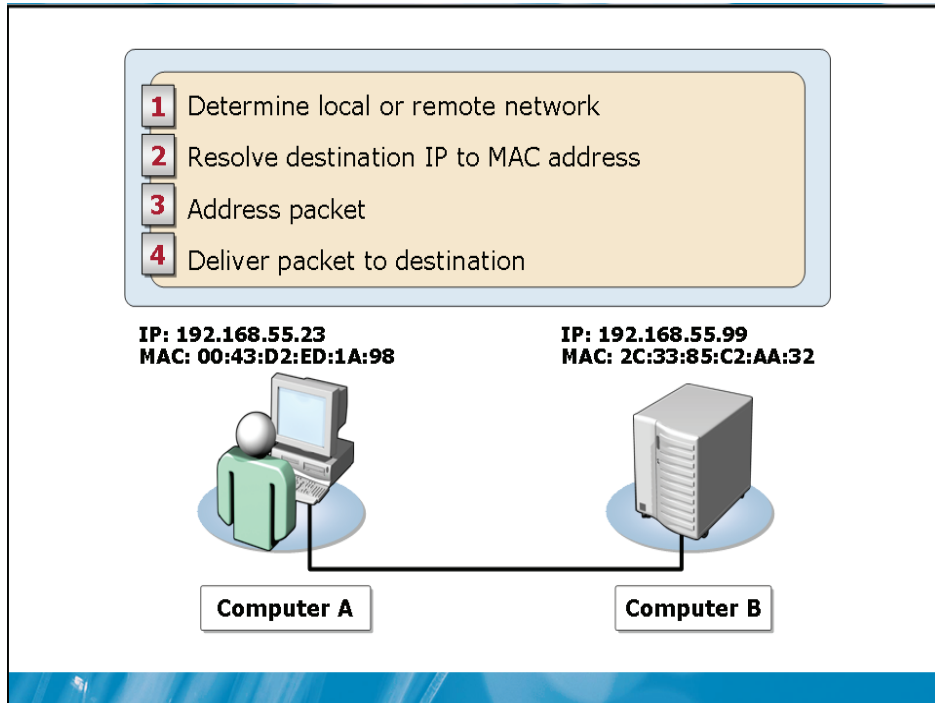
- Displays the ARP cache
- Removes entries from the ARP cache
- Adds static entries to the ARP cache

Key Points

Address resolution protocol (ARP) is used to refer to both a protocol and a tool. The ARP protocol is used to resolve IP addresses to media access control (MAC) addresses during packet creation. The ARP tool is used to manage the ARP cache used by the ARP protocol.

Question: What is the difference between the ARP protocol and the ARP tool?

IPv4 Communication within a Single Network

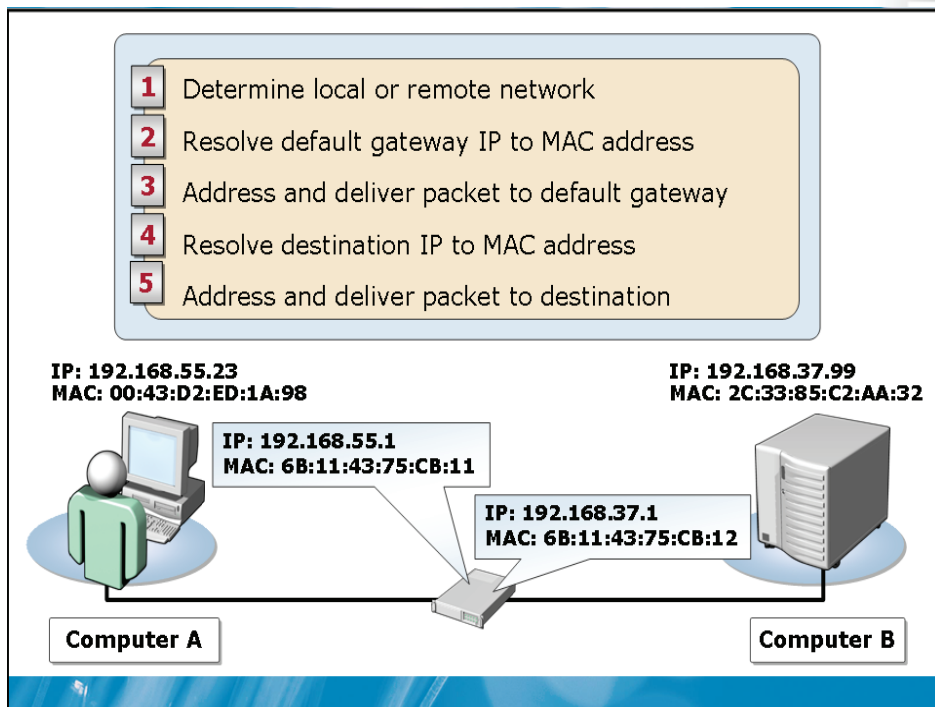


Key Points

On a single network, each computer can deliver packets to the destination without the use of a router. The sending computer resolves the destination IP address to a MAC address and sends the packet on to the network.

Question: What effect will an incorrectly configured default gateway have on communication within a single network?

IPv4 Communication Between Networks



Key Points

Packets delivered between networks use a default gateway. The default gateway moves packets from one network to another. The sending computer delivers packets to the default gateway, and the default gateway delivers the packets to the destination.

Question: Why does a computer use its own subnet mask to determine that the destination computer is on a different network?

Demonstration: Using ARP

In this demonstration, you will see how to use ARP

Question: Why was pinging NYC-SRV1 unsuccessful after adding the static entry to the ARP cache?

Lesson 2

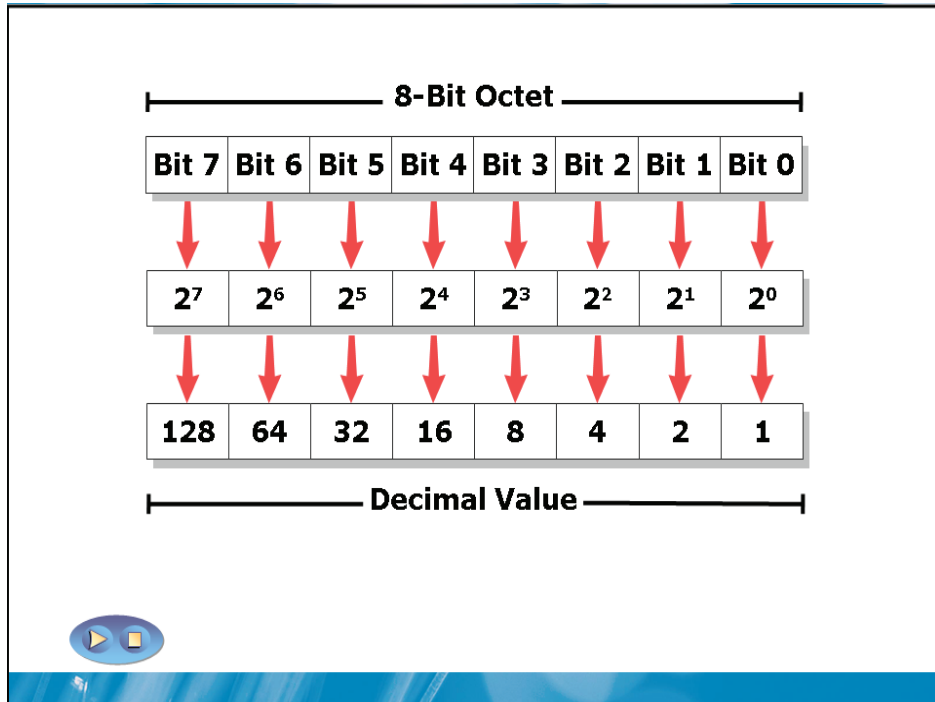
Subnetting Overview

- How Dotted Decimal Notation Relates to Binary Numbers
- What Is a Subnet?
- How Bits Are Used in a Subnet Mask
- How the Computer Determines Whether an IP Address is Local or Remote

In complex networks, subnet masks may not be simple combinations of 255 and 0. Complex networks may require that one octet in a subnet mask is subdivided with some bits used for the network ID and some bits used for the host ID. This requires you to understand how binary numbers are used during subnetting.

MOORE & ASSOCIATES COURSEWARE COURSE PROHIBITED

How Dotted Decimal Notation Relates to Binary Numbers

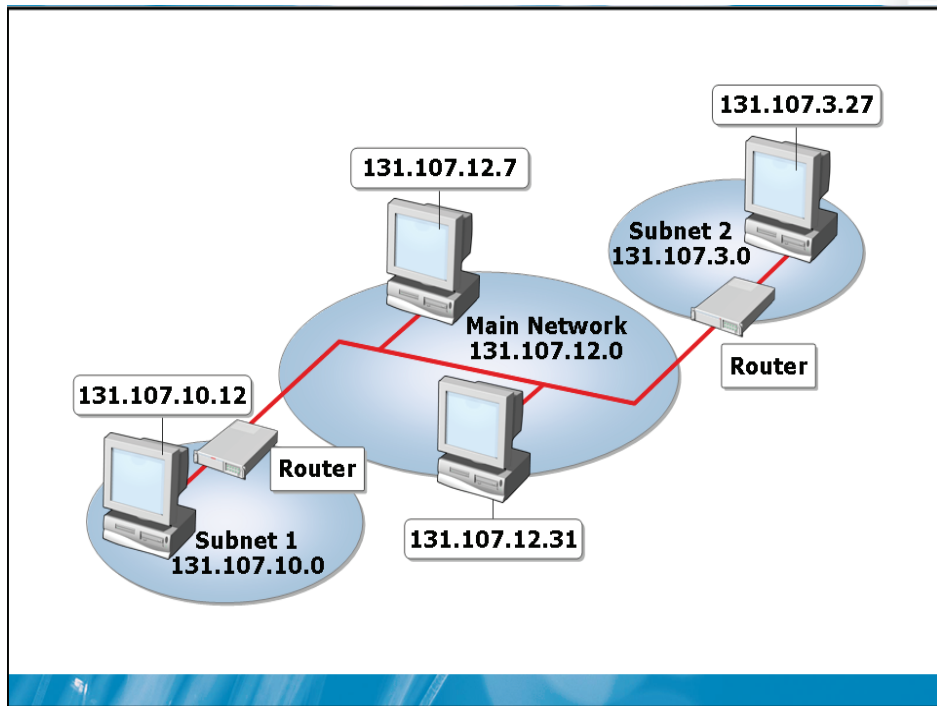


Key Points

When you assign IP addresses, you use dotted decimal notation, which is based on the decimal number system. However, in the background, computers use IP addresses in binary. To understand how to choose a subnet mask for complex networks, you must understand IP addresses in binary.

Question: Why should you understand the binary representation of IP addresses?

What Is a Subnet?



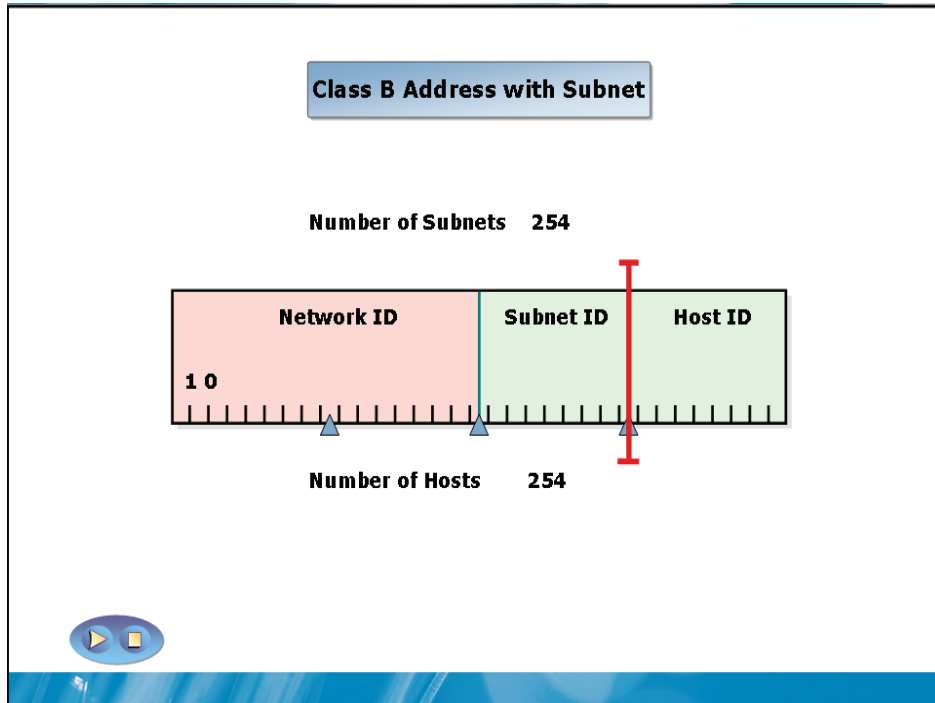
Key Points

A subnet is a physical segment of a network that is separated from the rest of the network by a router or routers. When a Class A, B, or C network is assigned to your organization, it must often be subdivided to match the physical layout of your network or design specifications. A larger network is subdivided into subnets.

Question: What is the minimum number of subnets required for a company with three physical locations?

USE PROHIBITED

How Bits Are Used in a Subnet Mask



Key Points

Before you define a subnet mask, you must estimate the number of segments and hosts per segment that you may require in the future. This enables you to use the appropriate number of bits for the subnet mask.

Question: Which is more important, allowing the number of hosts to grow or allowing the number of subnets to grow?

How the Computer Determines Whether an IP Address Is Local or Remote

Local and destination hosts' IP addresses are each ANDed with their subnet masks

- **1 AND 1 = 1**
- **Other combinations = 0**
- **If ANDed results of source and destination hosts match, the destination is local**

IP Address	10011111	11100000	00000111	10000001
Subnet Mask	11111111	11111111	00000000	00000000
Result	10011111	11100000	00000000	00000000

Key Points

When an IP network routes a data packet, it must determine whether the destination IP address is on a local network or on a remote network. Understanding how an IP network makes this determination will help you isolate issues associated with IP addressing.

Question: Do you need to know binary math to understand subnetting?

Lesson 3

Subnetting for Complex Networks

MCT USE ONLY. STUDENT USE PROHIBITED

- Determining the Number of Subnet Bits
- Determining the Number of Host Bits
- Determining Network IDs
- Demonstration: Subnetting

After you determine the required number of subnets and hosts, you must create a subnet mask that will support the configuration of the hosts. To do this, you determine the number of bits in the subnet mask that are required for the network ID and the host ID. After you establish the subnet mask, you can calculate the networks IDs and begin to configure network hosts.

Determining the Number of Subnet Bits

You should:

- Choose the number of subnet bits based on the number of subnets required
- Use 2^n to determine the number of subnets available from n bits

For five locations, three subnet bits are required

- 5 locations = 5 subnets required
- $2^2 = 4$ subnets (not enough)
- $2^3 = 8$ subnets

Key Points

To subnet a large IP address range into multiple smaller networks, you must determine how many bits in the host ID will be allocated to the network ID. This calculation is the number of subnet bits.

Question: On a class B network, how many bits are available for subnetting?

Determining the Number of Host Bits

You should:

- Choose the number of host bits based on the number of hosts required on each subnet
- Use $2^n - 2$ to determine the number of hosts available on each subnet available from n bits

For subnets 100 hosts, seven host bits are required

- $2^6 - 2 = 62$ hosts (not enough)
- $2^7 - 2 = 126$ hosts

Key Points

You must also determine the number of bits required to support hosts on a subnet. You calculate the number of host bits required by using the formula $2^n - 2$, where n is the number of bits. When the value n is placed in the formula $2^n - 2$, the result must be at least the number of hosts that are required for your network.

Question: Why are two hosts subtracted from each network when calculating the valid number of hosts?

Calculating Network Addresses

To determine the Network IDs:

- 172.16.0.0 will be subnetted using three bits
- The subnet mask is 255.255.11100000.0
- The lowest value bit in the subnet mask is the network ID increment

The network IDs increment by 32

- | | |
|--|---|
| <ul style="list-style-type: none">• 172.16.0.0• 172.16.32.0• 172.16.64.0• 172.16.96.0 | <ul style="list-style-type: none">• 172.16.128.0• 172.16.160.0• 172.16.192.0• 172.16.224.0 |
|--|---|

Key Points

You can calculate network addresses by using binary numbers and converting those numbers to dotted decimal notation. However, this can be a cumbersome process. A faster way to determine network addresses is by using the lowest value bit in the subnet mask.

Question: Why do you use the lowest value bit in the subnet mask to determine the valid network addresses?

Demonstration: Subnetting

In this demonstration, you will see how to perform subnetting

Scenario

Your organization is designing a new network with three locations, which may later increase to four. You need to subnet the network 172.30.0.0 to support four locations, with up to 3000 hosts in each location.

Lab: Creating IPv4 Address Spaces

- Exercise 1: Defining the Subnet Mask for a WAN
- Exercise 2: Defining the Hosts for a Network

Estimated time: 60 minutes

Scenario

You are a network consultant with several clients that require the design of IPv4 networks. You must determine the subnet masks and network addresses based on their business requirements.

USE PROHIBITED

Exercise 1: Defining the Subnet Mask for a WAN

Your client is designing an integrated WAN for eight locations using a Class B network (172.23.0.0). The IP structure for the WAN should include room for future growth of at least four additional locations, and maximize the number of hosts on each subnet. Each location must have its own subnet. Use the following table to define the subnets.

Description	Binary	Decimal
Original network	10101100.00010111.00000000.00000000	172.23.0.0
Original subnet mask	11111111.11111111.00000000.00000000	255.255.0.0
New subnet mask		
Subnet 1		
Subnet 2		
Subnet 3		
Subnet 4		
Subnet 5		
Subnet 6		
Subnet 7		
Subnet 8		

Exercise 2: Defining the Hosts for a Network

Your client has been assigned four class C networks for a single location. To reduce complexity on the network, you have decided to combine all four networks into a single, supernetted network. To do this, you must remove bits from the network ID and allocate them to the host ID. Use the following table to define the first host, last host, and broadcast addresses for the supernetted network.

Description	Binary	Decimal
Original network 1	11000000.10101000.11001100.00000000	192.168.204.0
Original network 2	11000000.10101000.11001100.00000000	192.168.205.0
Original network 3	11000000.10101000.11001100.00000000	192.168.206.0
Original network 4	11000000.10101000.11001100.00000000	192.168.207.0
Original subnet mask	11111111.11111111.11111111.00000000	255.255.255.0
Supernetted Network	11000000.10101000.11001100.00000000	192.168.204.0
New subnet mask	11111111.11111111.11111100.00000000	255.255.252.0
First host		
Last host		
Broadcast		

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Real-world Issues and Scenarios
- Best Practices

Review Questions

1. What is the default subnet mask for a class C network?
2. Which IP configuration components are used when determining whether a destination IP addresses is local or remote?
3. Which formula is used to calculate the number of possible hosts based on the number of bits allocated to the host ID?

Real-world Issues and Scenarios

1. You are a networking consultant with a client that is expanding to a new physical location. Your client is using a private class C address and has 200 hosts in the current location. How should you design the IPv4 network structure?

2. You are a networking consultant with a client that has eight physical locations. Each location has a maximum of 150 hosts. In the past, each location has used the private IP network 192.168.1.0. This prevented the locations from being connected. You are designing a new IPv4 network structure for your client. What is the simplest way to design the IPv4 structure for this network?

Best Practices for Subnetting

- Distill and summarize the best practices from the module and invite students to supplement or modify the best practices for their own work situations.
- Supplement or modify the following best practices for your own work situations:
 - Allocate at least one subnet for each location.
 - Allocate additional subnets based on the need to control network traffic.
 - Use the formula 2^n to determine the number of subnet bits required.
 - Use the formula 2^{n-2} to determine the number of host bits required.
 - Whenever possible, allocate for future growth by using more bits than are required for both subnets and hosts.
 - Calculate the network IDs of subnets quickly by using the lowest value bit in the subnet mask.

Module 6

IPv6 Fundamentals

Contents:

Lesson 1: Introduction to IPv6

6-3

Lesson 2: Unicast IPv6 Addresses

6-11

Lesson 3: Configuring IPv6

6-17

Lab: Configuring IPv6

6-23

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Introduction to IPv6
- Unicast IPv6 Addresses
- Configuring IPv6

Internet Protocol version 6 (IPv6) is a significant update to the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. The address space is significantly expanded and various types of addresses can be used. Windows Server® 2008 installs the IPv6 driver by default.

Lesson 1

Introduction to IPv6

- IPv4 Limitations
- IPv6 Improvements
- IPv6 Address Space
- IPv6 Address Syntax
- IPv6 Address Types
- Neighbor Discovery

The new features and functionality in IPv6 are designed to address many of the limitations in IPv4. IPv6 enhancements are intended to allow easier and more secure communication on the Internet and corporate networks.

MOUSE PROHIBITED

IPv4 Limitations

The limitations of IPv4 are:

- Limited number of addresses
- Routing difficult to manage
- Host configuration is complex
- No built in security
- Limited Quality of Service

Key Points

IPv4 was introduced in 1981 as RFC 791 and has not been significantly updated since that time. It has worked well up to this point, but it has some serious shortcomings for future networking needs.

Question: Which of these IPv4 limitations has affected you the most?

IPv6 Improvements

Improvements in IPv6 include:

- Larger address space
- More efficient routing
- Simpler host configuration
- Built-in security
- Better prioritized delivery support
- Redesigned headers for efficient processing and extensibility

Key Points

IPv6 was once known as IP-The Next Generation (IPng). It has been introduced to address the shortcomings in IPv4.

Question: Which of these improvements is most important to you?

USE PROHIBITED

Discussion: IPv6 Challenges

What are some of the challenges of implementing IPv6?

IPv6 Address Space

The IPv6 address space is:

- 128 bits
- Extremely large
- Allows routing flexibility

Key Points

The IPv6 address space is 128 bit as compared to the 32 bits used in the IPv4 address space. This allows for significantly more addresses in than IPv4. However, this address space is also designed for routing flexibility. As a result, the addresses are not allocated very efficiently.

Question: How does allocating 64 bits for host ID result in less efficient addressing?

UNAUTHORIZED USE PROHIBITED

IPv6 Address Syntax

IPv6 addresses are:

- Displayed in hexadecimal
- Can use zero compression
- Use a prefix to define the network portion of the address rather than a subnet mask

Examples:

2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A/64

2001:DB8:0:0:2AA:FF:FE28:9C5A/64

2001:DB8::2AA:FF:FE28:9C5A/64

Key Points

IPv6 does not use the dotted decimal notation that is commonly used when expressing IPv4 addresses. To compress the addresses and make them shorter, IPv6 uses hexadecimal to express addresses with a colon between each set of four digits. Each hexadecimal digit represents four bits.

Question: Why can zero compression be used only once in each address?

IPv6 Address Types

IPv6 addresses types include:

Type	Description
Unicast	Equivalent to IPv4 unicast
Multicast	Additional unicast address types
Anycast	Equivalent to IPv4 multicast

Key Points

IPv6 address types are similar to, but not the same as IPv4 address types.

Neighbor Discovery

Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes

Some of the ND functions are:

- Router discovery
- Prefix discovery
- Parameter discovery
- Address auto-configuration
- Address resolution
- Duplicate address detection

Key Points

The Neighbor Discovery (ND) protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (nodes on the same link). ND replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with more efficient multicast and unicast ND messages.

Question: Is there any benefit to using ND for address resolution rather than ARP?

Lesson 2

Unicast IPv6 Addresses

- Interface Identifiers
- What Are Global Unicast Addresses?
- What Are Link-Local Addresses?
- What Are Unique Local Unicast Addresses?
- Special IPv6 Addresses

In IPv4, a single host is typically assigned a single unicast address. However, in IPv6 multiple unicast addresses are assigned to each host for various purposes. You should understand what each of these addresses is used for to ensure that you can verify communication processes on your network.

Interface Identifiers

An interface identifier is:

- The last 64 bits of an IPv6 address
- Used as a media access control (MAC) address is in IPv4

An interface identifier can be:

- An EUI-64 address
- A randomly generated temporary identifier
- A randomly generated permanent identifier
- A manually assigned identifier

Key Points

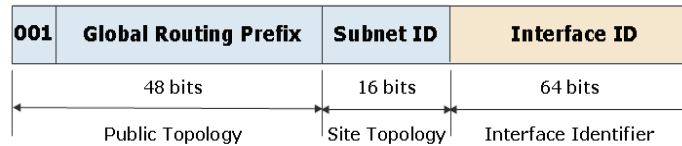
The last 64 bits of an IPv6 address are the interface identifier. This is equivalent to the host ID in an IPv4 address. Each interface on an IPv6 network must have a unique interface identifier. Because the interface identifier is unique to each interface, it is used by IPv6 in place of media access control (MAC) addresses to uniquely identify hosts.

Question: Why would you use a randomly generated interface identifier to protect privacy?

What Are Global Unicast Addresses?

Global unicast addresses are:

- Equivalent to public IPv4 addresses
- Globally routable on the Internet
- Designed for hierarchical routing



Key Points

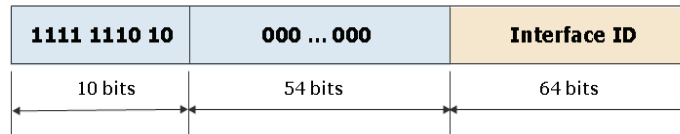
Global unicast addresses are equivalent to public IPv4 addresses. They are globally routable and reachable on the IPv6 portion of the Internet. Unlike the current IPv4-based Internet, which is a mixture of both flat and hierarchical routing, the IPv6-based Internet has been designed from its foundation to support efficient, hierarchical addressing and routing.

Question: On each subnet, how many hosts are supported?

What Are Link-local Addresses?

Link-local addresses are:

- Equivalent to APIPA IPv4 addresses
- Unique on the local network
- Required for Neighbor Discovery
- Always automatically configured for an interface
- Begin with FE80::/64



Key Points

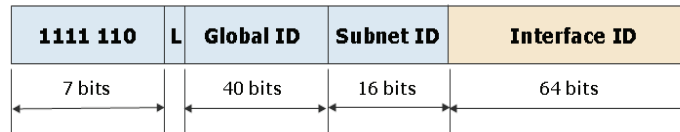
Link-local addresses are used by nodes when communicating with neighboring nodes on the same link. For example, on a single link IPv6 network with no router, link-local addresses are used to communicate between hosts on the link. IPv6 link-local addresses are equivalent to IPv4 link-local addresses, as defined in RFC 3927, that use the 169.254.0.0/16 prefix. IPv4 link-local addresses are known as Automatic Private IP Addressing (APIPA) addresses.

Question: Why are link local addresses important for IPv6 communication?

What Are Unique Local Unicast Addresses?

Unique local unicast addresses:

- Are equivalent to IPv4 private IP addresses
- Have a 40 bit Global ID you should use for your entire organization
- Have 16 bits designated for subnetting
- Replace site local addresses



Key Points

Unique local unicast addresses are the equivalent of IPv4 private address spaces such as 10.0.0.0/8. All unique local unicast addresses have the prefix FD00::/8 which defines the first eight bits. The next 40 bits are used to define a global ID.

Question: Why would your organization use unique local unicast addresses rather than global unicast addresses?

Special IPv6 Addresses

Unspecified address:

- 0:0:0:0:0:0:0:0 or ::
- Equivalent to IPv4 address 0.0.0.0
- Only ever used as a source address

Loopback address:

- 0:0:0:0:0:0:0:1 or ::1
- Equivalent to IPv4 address 127.0.0.1
- Used for testing the local IPv6 stack

Key Points

IPv6 includes two special addresses that can be used by applications:

- **Unspecified address (0:0:0:0:0:0:0:0 or ::).** This address is equivalent to the IPv4 address 0.0.0.0. It is used only as a source address to indicate the absence of an address. This is typically used during duplicate address detection before an address is confirmed to be unique.
- **Loopback address (0:0:0:0:0:0:0:1 or ::1).** This address is equivalent to the IPv4 address 127.0.0.1. It is used to send packets to the local host and for testing the IPv6 stack.

Question: Can you think of another instance when the address :: may be used when configuring an application?

Lesson 3

Configuring IPv6

- IPv6 Addresses Assigned to a Host
- Demonstration: Configuring IPv6
- Address Autoconfiguration
- The Autoconfiguration Process
- What Is DHCPv6?

Each IPv6 interface is configured with multiple IPv6 addresses. Some of these addresses are assigned automatically. Others can be configured manually if desired. DHCPv6 is one of the methods that can be used to configure IPv6 hosts with and address automatically.

IPv6 Addresses Assigned to a Host

Unicast addresses:

- A link local address for each interface
- A unique local unicast address or global unicast address
- A loopback interface with ::1

Multicast addresses:

- The interface-local scope all-nodes multicast address (FF01::1)
- The link-local scope all-nodes multicast address (FF02::1)
- The solicited-node address for each unicast address on each interface
- The multicast addresses of joined groups on each interface

Key Points

An IPv6 host is assigned multiple unicast and multicast addresses.

Question: Which of these addresses can you configure for an interface?

Demonstration: Configuring IPv6

In this demonstration, you will see how to configure IPv6 with a static address

Question: Is it less likely that you will use manual configuration for IPv6 than for IPv4?

USE PROHIBITED

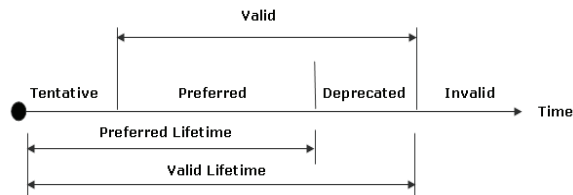
Address Autoconfiguration

Address autoconfiguration can be:

- Stateful
- Stateless

Autoconfigured address states:

- Tentative
- Valid
- Preferred
- Deprecated
- Invalid

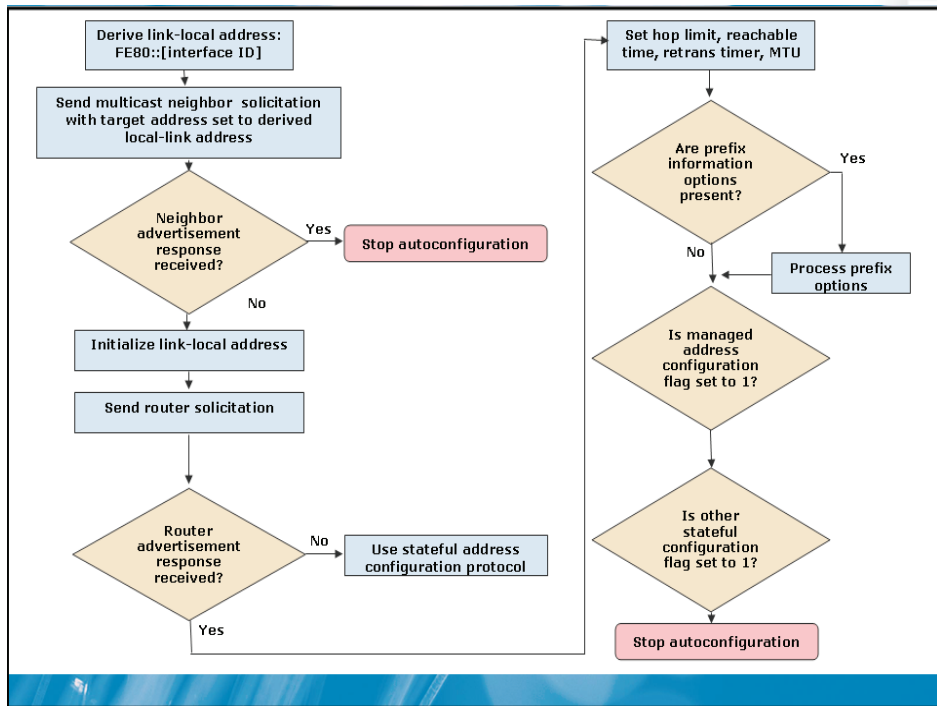


Key Points

Autoconfiguration is a way to automatically assign an IPv6 address to an interface. Autoconfiguration can be stateful or stateless. Stateful autoconfiguration is performed by DHCPv6. Stateless configuration is performed based on router advertisements.

Question: If the IPv6 address of a host has entered the deprecated state, can it continue to communicate on the network?

The Autoconfiguration Process



Key Points

The part of autoconfiguration is the generation of a link-local address that is used to communicate with other hosts on the same network. This is required to perform further autoconfiguration tasks. When the link-local address is generated by the host, duplicate address detection is performed to ensure that it is unique.

Question: Who configures the router advertisements?

USE PROHIBITED

What Is DHCPv6?

- 1 Client sends a Solicit message
- 2 Server sends an Advertise message
- 3 Client sends a Request message
- 4 Server sends a Reply message

Key Points

DHCPv6 is a service that provides stateful autoconfiguration of IPv6 hosts. It can automatically configure IPv6 hosts with an IPv6 address and other configuration information such as DNS servers. This is equivalent to DHCPv4 for IPv4 networks.

Question: When is only configuration information requested by clients?

Lab: Configuring IPv6

- Exercise 1: Defining IPv6 Networks for Internal Use
- Exercise 2: Configuring a Static IPv6 Address on a Server

Logon information

Virtual machine	NYC-DC1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are the server administrator for an organization with 10 physical locations and 100 users in each location. Your organization is planning an IPv6 implementation and you are on the project team.

Exercise 1: Defining IPv6 Networks for Internal Use

Your organization has determined that unique local unicast addresses will be used to implement IPv6. One subnet must be created for each of the ten physical locations. You must help the team determine an appropriate addressing scheme.

- Task 1: Define IPv6 networks for internal use
1. Determine the prefix for unique local unicast addresses:
 - The prefix for unique local unicast addresses is 8 bits long
 - Review the module to determine the correct prefix
 - Enter the prefix in the table below using 2 hexadecimal digits
 2. Select a random 40-bit number:
 - Each hexadecimal digit represents 4 bits
 - Create a 10 digit hexadecimal number, and enter it in the table below
 3. Select subnet IDs for each of ten locations:
 - The subnets can be contiguous
 - Enter ten 16-bit subnet IDs in the table below using four hexadecimal digits each.

Description	Prefix	Global ID	Subnet ID
Subnet 1			
Subnet 2			
Subnet 3			
Subnet 4			
Subnet 5			
Subnet 6			
Subnet 7			
Subnet 8			
Subnet 9			
Subnet 10			

Exercise 2: Configuring a Static IPv6 Address on a Server

The subnets for each location in your network have been defined. The team will configure the DNS server in each location with a static IPv6 address to make it easier to configure clients and test during troubleshooting. You must configure the DNS server with a static IPv6 address. The DNS server will use the network identifier of `::5` and the gateway will be `::1`

- ▶ Task 1: View the IPv6 addresses that are configured by default
 1. On NYC-DC1, log on as Administrator with a password of Pa\$\$w0rd.
 2. Open a command prompt.
 3. Run the `ipconfig /all` command to view the current addresses.
 4. Write down the following addresses:
 - Link-local IPv6 Address: _____
- ▶ Task 2: Configure a static IPv6 address
 1. On NYC-DC1, open the properties of Local Area Connection.
 2. In the properties of Internet Protocol Version 6 (TCP/IPv6), enter the following:
 - IPv6 address: `FD55:5555:5555:1::5`
 - Subnet prefix length: 64
 - Default gateway: `FD55:5555:5555:1::1`
 - Preferred DNS server: `::1`
- ▶ Task 3: Verify the new IPv6 configuration
 1. On NYC-DC1, open a command prompt.
 2. Run the `ipconfig /all` command to view the current addresses
 3. Use the `ping` command to test the configuration of the IPv6 address.

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Real-world Issues and Scenarios
- Best Practices

Review Questions

1. What are some of the limitations of IPv4 that are addressed by IPv6?
2. How is the interface identifier used in IPv6 different from the host ID used in IPv4?
3. Which unicast addresses are assigned to a host?

Real-world Issues and Scenarios

1. You are a network administrator for an organization with five physical locations. Each location has approximately 500 computers. You are planning an IPv6 implementation using global unicast addresses. How many subnets will you need to obtain from an ISP?

2. You are a network administrator for a small organization that is planning the implementation of IPv6 on your network. All concerns about interoperability between IPv4 and IPv6 have been addressed already by the project team. The final decision remaining is how to configure servers with IPv6 addresses and options. Should the servers be configured manually or be autoconfigured?

Best Practices for Using Unique Local Unicast Addresses

Supplement or modify the following best practices for your own work situations:

- Use unique local unicast addresses rather than site local addresses for internal networks that are not accessible from the Internet.
- Use only one 40-bit global ID for your organization.
- Randomly generate the global ID to prevent duplication and make it easier to merge networks.
- Use the 16-bit subnet ID to create subnets within your organization.

Module 7

Fundamentals of Administering Windows Server 2008

Contents:

Lesson 1: Introduction to IPv6	7-3
Lesson 2: Unicast IPv6 Addresses	7-10
Lesson 3: Configuring IPv6	7-17
Lesson 4: Using Remote Desktop for Administration	7-24
Lesson 5: Configuring Security for Server Administration	7-30
Lab: Configuring IPv6	7-36

MCT USE ONLY. STUDENT USE PROHIBITED

Module Overview

- Windows Server 2008 Administrative Tools
- Monitoring Performance
- Monitoring Events
- Using Remote Desktop for Administration
- Configuring Security for Server Administration

Windows Server® 2008 operating system includes several administrative tools for managing the operating system. Reliability and Performance Monitor is included to monitor system performance. Event Viewer is included to monitor system status. Remote Desktop for Administration allows management to be performed from a remote computer rather than the server console.

Lesson 1

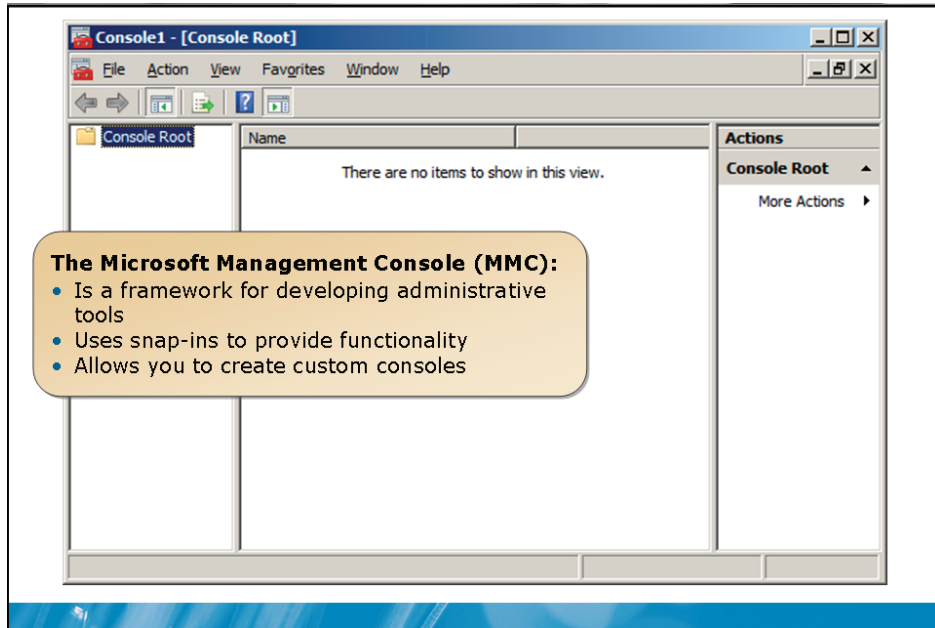
Using Windows Server 2008 Administrative Tools

- Microsoft Management Console
- Problem Reports and Solutions
- Server Manager
- Computer Management
- Device Manager
- Demonstration: Using Windows Server 2008 Administrative Tools

Each administrative tool included with Windows Server 2008 is used to manage different system components. Administrative tools include:

- Microsoft Management Console
- Problem Reports and Solutions
- Server Manager
- Computer Management
- Device Manager

Microsoft Management Console

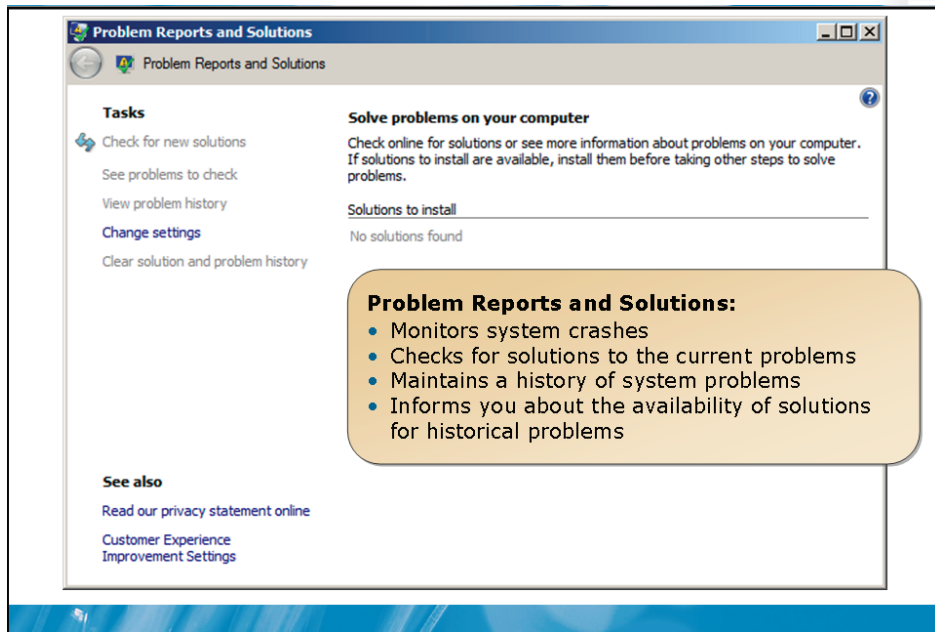


Key Points

The Microsoft Management Console (MMC) is a framework for administrative tools. Snap-ins are added to the MMC to provide administrative capabilities.

Question: Question: Will you create customized consoles for most of your management tasks?

Problem Reports and Solutions



Key Points

Problem Reports and Solutions is a utility for monitoring and resolving system problems. Problem Reports and Solutions records the details of a system problem, and then contacts Microsoft for a resolution of the problem.

Question: How does Problem Reports and Solutions improve upon the Dr. Watson utility found in previous versions of Microsoft Windows® operating system?

Server Manager

Server Manager is an MMC console with several snap-ins for managing your server

You can:

- Add or remove server roles
- Add or remove server features
- Monitor system events
- Manage devices
- Schedule tasks
- Manage local users and groups
- Configure Windows Firewall
- Configure storage
- Perform a backup

Key Points

Server Manager is an MMC with several snap-ins for managing your server. Combining frequently used snap-ins into a single console simplifies administration of your server.

Question: Why is it beneficial to combine frequently used snap-ins into a single console?

Device Manager

Device Manager is a snap-in that is used to view and manage hardware information

You can:

- View device status and information
- View device resources
- Configure device settings
- Enable and disable devices
- Update driver software

Key Points

Device Manager is a snap-in that is used to view and manage hardware information. You can use Device Manager to view the status of any device in your system. This includes information about the resources a device is using, such as memory addresses or interrupt requests. You can also use Device Manager to enable and disable devices during troubleshooting or to configure device settings.

Question: Why would you update a device driver if a device appears to be working properly?

Demonstration: Using Windows Server 2008 Administrative Tools

In this demonstration, you will see how to use:

- Problem Reports and Solutions
- Server Manager
- Computer Management
- Device Manager

Question: Which of the administrative tools demonstrated will you use most often?

Lesson 2

Monitoring Performance

MCT USE ONLY. STUDENT USE PROHIBITED

- Task Manager
- Resource Overview
- Performance Monitor
- Reliability Monitor
- Data Collector Sets
- Demonstration: Using Reliability and Performance Monitor

Monitoring server performance is an essential part of system administration. By monitoring server performance, you can determine when components need to be upgraded before users are affected by performance problems. For example, by monitoring memory utilization over time, you can see when free memory is becoming limited and add additional memory or move applications to a different server.

Task Manager

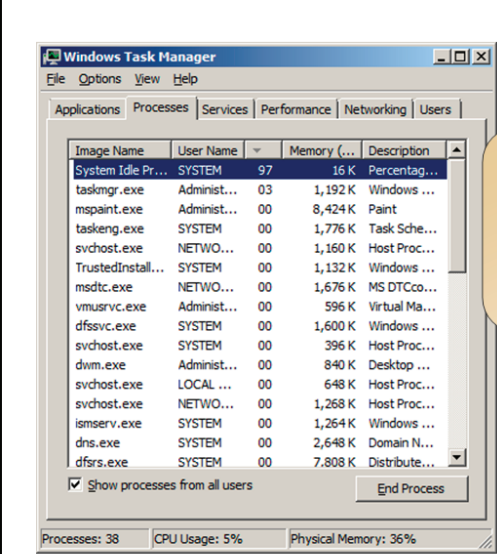


Image Name	User Name	PID	Private Memory	Description
System Idle Pr...	SYSTEM	0	16 K	Percentag...
taskmgr.exe	Administ...	03	1,192 K	Windows ...
mspaint.exe	Administ...	00	8,424 K	Paint
taskeng.exe	SYSTEM	00	1,776 K	Task Sche...
svchost.exe	NETWO...	00	1,160 K	Host Proc...
TrustedInstall...	SYSTEM	00	1,132 K	Windows ...
msdtc.exe	NETWO...	00	1,676 K	MS DTCco...
vmusrvc.exe	Administ...	00	596 K	Virtual Ma...
dfssvc.exe	SYSTEM	00	1,600 K	Windows ...
svchost.exe	SYSTEM	00	396 K	Host Proc...
dwm.exe	Administ...	00	840 K	Desktop ...
svchost.exe	LOCAL ...	00	648 K	Host Proc...
svchost.exe	NETWO...	00	1,268 K	Host Proc...
ismserv.exe	SYSTEM	00	1,264 K	Windows ...
dns.exe	SYSTEM	00	2,648 K	Domain N...
dfers.exe	SYSTEM	00	7,808 K	Distribute...

Show processes from all users

End Process

Processes: 38 CPU Usage: 5% Physical Memory: 36%

Task Manager monitors:

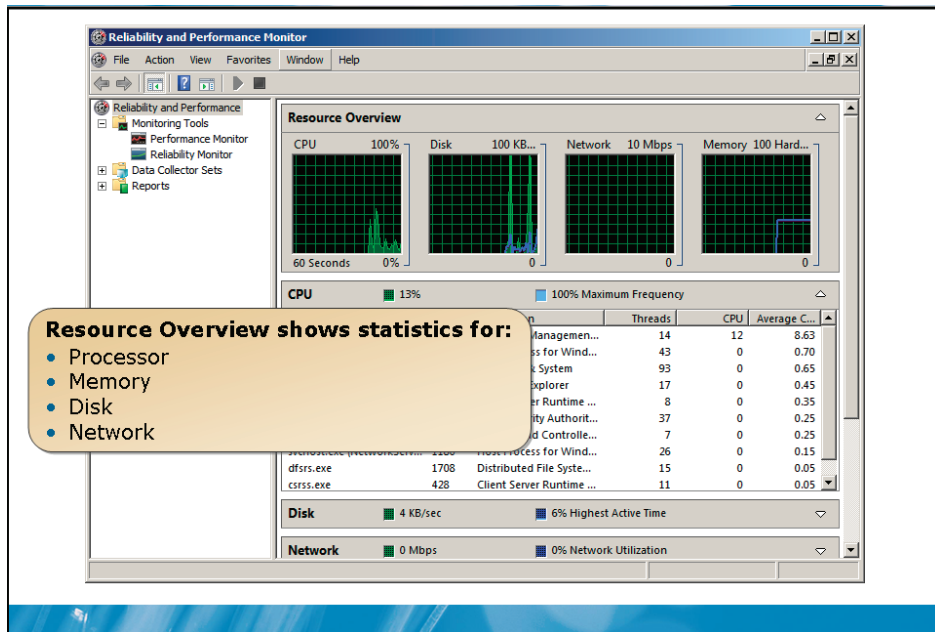
- Applications
- Processes
- Services
- Basic CPU and memory statistics
- Basic networking performance
- Connected users

Key Points

Task Manager is a simple utility that gives you an overview of system performance. It has several tabs with different information on each tab:

Question: What is the most common task you will perform with Task Manager?

Resource Overview



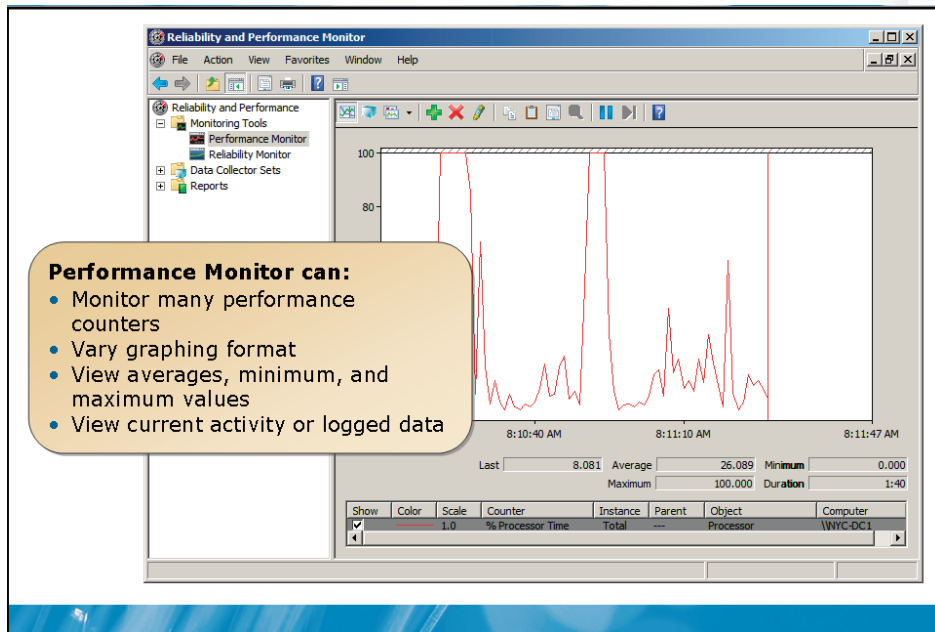
Key Points

Resource Overview is a part of Reliability and Performance Monitor that shows commonly monitored statistics.

In addition to the summary statistics, you can view detailed statistics for individual processes. This allows you to view CPU, disk, network, and memory information for individual processes when troubleshooting.

Question: How do the summary statistics provided by Resource Overview compare with the process information provided by Task Manager?

Performance Monitor



Key Points

Performance Monitor allows you to select performance counters that you want to monitor. After the counters are selected, you can choose how the data is displayed.

Question: What are the benefits of Performance Monitor over Resource Overview?

BETA COURSEWARE. EXPIRES 5/16/2008

Reliability Monitor

Reliability Monitor tracks system stability over time and generates a System Stability Index

Recorded events include:

- Software installation
- Application failures
- Hardware failures
- Windows failures
- Miscellaneous changes and failures

Key Points

Reliability Monitor tracks system stability over time.

Question: How can you use Reliability Monitor for troubleshooting?

Demonstration: Using Reliability and Performance Monitor

In this demonstration, you will see how to monitor server performance by using Reliability and Performance Monitor

Question: How are reports more useful than viewing performance data in Performance Monitor?

Lesson 3

Monitoring Events

- Event Viewer
- Windows Logs
- Applications and Services Logs
- Custom Views
- Advanced Event Viewer Features
- Demonstration: Using Event Viewer

You can use Event Viewer to monitor events generated by Windows Server 2008, applications, and services. Events are organized in to Windows logs and Applications and Services logs. A new feature in Windows Server 2008 is the ability to query events across multiple log files.

Event Viewer

Event viewer:

- Is a utility for viewing event logs
- Displays XML events in an easy to read format
- Can display raw XML of events

Event levels:

- Error
- Warning
- Information
- Audit Success
- Audit Failure

Key Points

Event Viewer is a utility for viewing the event located in log files. These events are generated by Windows components and applications. The events are stored in logs in an XML format. When you view an event, you can display it in either the XML format or a more readable format.

Question: For what purposes will you use Event Viewer?

Applications and Services Logs

Applications and Services logs:

- Are new in Windows Server 2008 and Windows Vista
- Divide events into more specific logs
- Can have multiple log types per service or application

Log type	Contents
Admin	Events that indicate a problem and well-defined solution
Operational	Events for general information and problems without specific solutions
Analytic	Events that describe program operation and problems that cannot be resolved by user intervention
Debug	Events used by developers to troubleshoot problems

Key Points

Applications and Services Logs are a new category of event logs in Windows Server 2008. These logs store events from a single application or component, rather than events that have system-wide impact. For each application or component, there can be multiple logs.

Question: Why are multiple logs for events beneficial for server administrators?

Advanced Event Viewer Features

Subscriptions:

- Collect copies of events from multiple computers
- Allow centralized analysis of events

Integration with Task Scheduler:

- Tasks can be triggered based on events
- Used for troubleshooting

Key Points

Event Subscriptions

Subscriptions are used to centralize event logs for analysis. This allows you to troubleshoot problems that involve several servers. Subscriptions also allow you to quickly scan the event logs of multiple servers to see if any errors are occurring.

Task Scheduler Integration

In Windows Server 2008, Event Viewer allows you to attach a task to an event. This allows you to run a task when this event occurs again.

Question: Which task action would you use to restart a stalled print spooler?

Demonstration: Using Event Viewer

In this demonstration, you will see how to use Event Viewer to monitor Windows Server 2008

Question: Why would you use the XML view of an event?

BETA COURSEWARE. EXPIRES 5/16/2008
COPYRIGHT USE PROHIBITED

Lesson 4

Using Remote Desktop for Administration

MCT USE ONLY. STUDENT USE PROHIBITED

- Remote Desktop for Administration
- Benefits of Remote Desktop for Administration
- Demonstration: Remote Desktop Client Configuration
- Securing Remote Desktop for Administration
- Demonstration: Using Remote Desktop for Administration

Remote Desktop for Administration is widely used by most organization to access servers remotely and to perform system maintenance. There are many configuration options you can use for controlling security of the connections and other connection characteristics.

Remote Desktop for Administration

Remote Desktop for Administration:

- Allows access to the server desktop remotely
- Is limited to two connections
- Sends only screen updates and keystrokes between server and client
- Uses port 3389 by default

Key Points

Remote Desktop for Administration is a service that allows administrators to access the desktop of a computer running Windows Server 2008 remotely. This service can be used to access a server from a corporate desktop or a remote location.

Question: What concerns are there about allowing a server administrator to use Remote Desktop for Administration from home?

Benefits of Remote Desktop for Administration

The benefits of Remote Desktop for Administration are:

- Run server administrative tools without installing them on a workstation
- Run server administrative tools that cannot be installed on a workstation
- Works well over slow links
- May avoid the need to travel to remote locations
- May avoid the need to return to the office after hours
- Manage server core installations

Key Points

Remote Desktop for Administration is a useful tool with several benefits.

Question: Can Remote Desktop for Administration result in cost savings for an organization?

Demonstration: Remote Desktop Client Configuration

In this demonstration you will see how to configure the Remote Desktop Client

Question: Why would you disable client features such as local drives and printers?

BETA COURSEWARE. EXPIRES 5/16/2008
STUDENT USE PROHIBITED

Securing Remote Desktop for Administration

Remote Desktop for Administration is secured by:

- Enabling and disabling Remote Desktop for Administration
- Controlling members of the Remote Desktop Users group

RDP security settings:

- Security layer
- Encryption level
- Require authentication before allowing RDP connections to this computer

Key Points

The first level of securing Remote Desktop for Administration is controlling who can use it. Remote Desktop for Administration is disabled by default. You can leave it disabled for high security installations. When enabled, access can be controlled by making users members of the Remote Desktop Users group. Members of the Local Administrators group are allowed to connect by default.

Question: Why should you not use the low encryption level?

Lesson 5

Configuring Security for Server Administration

MCT USE ONLY. STUDENT USE PROHIBITED

- What Are the Local Built-in Groups?
- What Are the Domain Built-in Groups?
- What Are User Rights?
- How to Elevate Privileges for Administration
- Demonstration: Configuring Security for Server Administration

Within Active Directory® Domain Services (AD DS) and the local security database of computers running Windows Server 2008, there are built-in security groups. These security groups are used to control access to system management through system rights. You can add members to these groups to delegate administrative privileges. You can also create custom groups and grant administrative rights to the custom groups.

What Are the Local Built-in Groups?

Local built-in groups include:

- Administrators
- Backup Operators
- Event Log Readers
- Guests
- Network Configuration Operators
- Performance Log users
- Performance Monitor users
- Power Users
- Print Operators
- Users

Key Points

Member servers in a domain have a local security database that contains user accounts and group accounts. The local users and groups can be assigned permissions only on the local computer.

Question: Which built-in group do you use to grant a user full administrative rights to the server?

What Are the Domain Built-in Groups?

Domain built-in groups include the local built-in groups, except for Power Users

Additional groups include:

- Account Operators
- Incoming Forest Trust Builders
- Pre-Windows 2000 Compatible Access
- Terminal Server License Servers
- Windows Authorization Access Group

Key Points

Domain controllers do not have a local security database. Therefore, the built-in groups required by domain controllers are located in AD DS. When given a membership in a domain built-in group, the user is given rights to all domain controllers in the domain.

Question: What is the primary difference between domain built-in groups and local built-in groups?

What Are User Rights?

User rights:

- Control the ability to perform system tasks
- Can be configured in the local security policy
- Can be configured by Group Policy

Key Points

User rights control the ability of specific users and groups to perform system tasks. The built-in groups are assigned user rights by default during installation. However, you can modify the rights that are assigned to the built-in groups. You can also create your own custom groups and assign users to those groups.

Question: Why would you use Group Policy to assign user rights rather editing the local security policy?

How to Elevate Privileges for Administration

To elevate privileges for administration:

- In a graphical interface: Run As Administrator
- At a command prompt: `runas`

Key Points

It is a security best practice to log on as a standard user for most tasks. When you need to perform administrative tasks, you can log in with a user account with additional administrative privileges. Using this best practice limits the ability of malicious software (also called malware) to damage or control your computer systems. Malicious software includes viruses, root kits, and other unauthorized software.

Question: Why does logging on as a standard user limit malicious software?

Demonstration: Configuring Security for Server Administration

In this demonstration, you will see how to configure security for server administration

Question: Which tools are used to configure local built-in groups and domain built-in groups?

Microsoft Security Use Prohibited

Lab: Administering Windows Server 2008

MCT USE ONLY. STUDENT USE PROHIBITED

- Exercise 1: Joining a server to the domain
- Exercise 2: Configuring Remote Desktop for Administration
- Exercise 3: Centralizing event logging
- Exercise 4: Resolving a performance issue by using Reliability and Performance Monitor

Logon information

Virtual computer	NYC-DC1, NYC-SVR1, NYC-CL1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

You are the server administrator for Woodgrove Bank. Your organization has just implemented two computers running Windows Server 2008. You must complete the configuration of these servers before they are put into production.

Exercise 1: Joining a server to the domain

- ▶ Task 1: Verify the current configuration
 1. On NYC-DC1, log on as Administrator with a password of Pa\$\$w0rd.
 2. In Active Directory Users and Computers, verify that the NYC-SVR1 computer account does not exist.
 3. On NYC-SVR1, log on as Administrator with a password of Pa\$\$w0rd.
 4. In Local Users and Groups, verify that Domain Admins is not a member of the local administrators group.

- ▶ Task 2: Join the domain
 1. On NYC-SVR1, open System Properties.
 2. Change the settings for the domain, and join the woodgrovebank.com domain.
 3. When prompted, log on as Administrator with a password of **Pa\$\$w0rd**.
- ▶ Task 3: Verify domain membership
 1. On NYC-DC1, in Active Directory Users and Computers, verify that the NYC-SVR1 computer account exists.
 2. On NYC-SVR1, log on as Woodgrovebank\Administrator with a password of Pa\$\$w0rd.
 3. In Local Users and Groups, verify that Domain Admins is a member of the local administrators group.

Exercise 2: Configuring Remote Desktop for Administration

The server NYC-SVR1 is being used to run a new application for loan applications. The person responsible for monitoring this application needs access to NYC-SVR1 remotely because he is not authorized to enter the data center. You need to enable Remote Desktop for Administration for Axel Delgado with the highest level of security possible.

- ▶ Task 1: Enable Remote Desktop for Administration
 1. On NYC-SVR1, open Remote settings in System Properties.
 2. Allow connections only if Network Level Authentication is used.
- ▶ Task 2: Grant Axel Delgado access to Remote Desktop for Administration on NYC-SVR1
 1. On NYC-SVR1 in Remote Settings, Add Axel Delgado as a user allowed to connect remotely.

- ▶ Task 3: Configure security for Remote Desktop for Administration
 1. On NYC-SVR1, open Terminal Service Configuration.
 2. In the properties of RDP-Tcp configure:
 - Security layer: **SSL (TLS1.0)**
 - Encryption level: **High**
 - Allow connections only from computers running Remote Desktop with Network Level Authentication.
- ▶ Task 4: Give Axel rights to run Reliability and Performance Monitor
 - On NYC-SVR1, use Local Users and Groups to add Axel Delgado as a member of Performance Log Users.
- ▶ Task 5: Verify Remote Desktop for Administration Functionality
 1. On NYC-CL1, open Remote Desktop Connection.
 2. Log on using the following information:
 - Computer: **NYC-SVR1.woodgrovebank.com**
 - User name: **woodgrovebank\Axel**
 - Password: **Pa\$\$w0rd**
 3. Open Reliability and Performance Monitor. Notice that Resource Overview is not available to Axel Delgado.
 4. Verify that Axel can view information in Performance Monitor.

Exercise 3: Centralizing event logging

Woodgrove bank has implemented centralized event logging for all computers running Windows Server 2008. At this time, only the system event logs are collected centrally for analysis. Events are collected on NYC-DC1. You need to configure an event log subscription for NYC-SVR1.

- ▶ Task 1: Configure NYC-SVR1 to forward events
 1. On NYC-SVR1, run the following at a command prompt:
 - `winrm quickconfig`
 2. Use Local Users and Groups to add NYC-DC1 as a member of Administrators.

- ▶ Task 2: Create a subscription on NYC-DC1
 1. On NYC-DC1, open Event Viewer.
 2. At the Subscriptions node, create a new subscription with the following information:
 - Enable the Windows Event Collector Service
 - Name: **NYC-SVR1**
 - Collector initiated
 - Computer: **NYC-SVR1**
 - Query Filter:
 - Event levels: **Critical, Warning, Verbose, Error, Information**
 - By log
 - Windows Logs: **System**
 - Advanced:
 - Event delivery optimization: **Minimize latency**
- ▶ Task 3: Create events in the System log on NYC-SVR1
 - On NYC-SVR1, run the following at a command prompt:
 - **Net stop spooler**
 - **Net start spooler**
- ▶ Task 4: Create a custom view for service management events
 1. On NYC-DC1, view the runtime status of the NYC-SVR1 subscription. The subscription is active because it is fully configured.
 2. View events in the Forwarded Events log.
 3. Create a new custom view with the following settings:
 - Event levels: **Critical, Warning, Verbose, Error, Information**
 - By log
 - Windows Logs: **Forwarded Events**
 - Event sources: **Service Control Manager Eventlog Provider**
 - Name: **Service Management**

Exercise 4: Resolving a Performance Issue by Using Reliability and Performance Monitor

Axel Delgado has called to you indicate that there is a problem with NYC-SVR1. One component of the new load application software is unstable and begins to use 100 percent of the available CPU cycles. The application vendor has promised a fix will be available in the next few weeks.

In the meantime, Axel has asked you if there is a way to automatically end the process for this component when CPU utilization stays at 100 percent for more than 1 minute. In this exercise, you need to configure an alert that can automatically end the process `loanapp.exe` when CPU utilization stays at 100 percent for more than 1 minute.

- ▶ Task 1: Start the faulty application
 1. On NYC-SVR1, start `\\NYC-DC1\DS\Mod07\Labfiles\cpustres.exe`.
 2. Configure Thread 1 with maximum activity.
- ▶ Task 2: View application performance
 1. Open Task Manager.
 2. Verify that status of the application CPU Stress is running.
 3. Verify that the `cpustres.exe` process has used most of the CPU time.
 4. Verify that the CPU utilization is 100 percent.
 5. Open Reliability and Performance Monitor.
 6. Verify that CPU utilization is the same as noted in Task Manager.
 7. View the details of the CPU utilization by expanding the CPU summary bar.

- ▶ Task 3: Create a task to stop the faulty application
 1. On NYC-SVR1, open Task Scheduler.
 2. Create a basic task with the following settings:
 - Name: StopApp
 - Task Trigger: Daily
 - Daily: default settings
 - Action: Start a program
 - Program/script: C:\Windows\System32\taskkill.exe
 - Arguments: /IM cpustres.exe
 3. Edit the StopApp task and remove the Daily trigger.

- ▶ Task 4: Create an alert for 100 percent CPU utilization
 1. On NYC-SVR1, in Reliability and Performance Monitor, create a new user defined data collector set with the following settings:
 - Name: 100% CPU
 - How to create: Create Manually (Advanced)
 - Type of data: Performance Counter Alert
 - Counter: %Processor Time
 - Alert when: Above 99%
 2. Configure the alert DataCollector01:
 - Task to run: StopApp
 - Alert action: Log an entry in the application event log
 3. Start the 100% CPU Data Collector Set.
 4. Wait approximately 30 seconds for the alert to trigger the task.

- ▶ Task 5: Verify that the application is stopped
 1. On NYC-SVR1, verify that the application is not running in Task Manager.
 2. Verify an event for the alert appears in the Diagnosis-PLA Operational log in Event Viewer.

► Task 6: Verify system health

1. On NYC-SVR1, open Reliability and Performance Monitor.
2. Start the System Diagnostics Data Collector Set. This runs for about one minute.
3. After the System Diagnostics Data Collector Set is complete, view the most recent diagnostic report.

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools

Review Questions

1. Which administrative tool tracks system crashes and attempts to resolve them?
2. When monitoring performance, which tools can you use to track CPU utilization over time?
3. Which feature in Event Viewer can you use to centralize analysis of event logs?
4. Which group is used to control the users allowed to remotely connect to a server by using the Remote Desktop client?
5. What rights does the Account Operators group have for a domain?

Real-world Issues and Scenarios

1. You are the lead server administrator for your location in a large organization. There are 4000 users in your location, with seven server administrators. You would like to configure administrative tools for the server administrators that you manage. Each administrative tool would have all the options required for them to perform their job tasks. How can you create these custom tools?

MCT USE ONLY. STUDENT USE PROHIBITED

2. A computer running Windows Server 2008 has been in your organization for about two months. It has been running perfectly until last week. Since last week, it has been crashing once or twice a day. How can you determine the cause of this problem?
3. You are the server administrator for a small organization with 100 users and three computers running Windows Server 2008. Your IT manager would like to respond more quickly to support calls after business hours. Currently, you drive into the office when required. This takes up to an hour. How can you avoid the need to return to the office to perform support tasks after hours? And how will you address security concerns?

Tools

Tool	Use to	Where to find it
Microsoft Management Console	<ul style="list-style-type: none"> • Add snap-ins to perform administrative tasks • Create custom consoles 	Command prompt
Problem Reports and Solutions	<ul style="list-style-type: none"> • Track solutions to system problems 	Administrative Tools
Server Manager	<ul style="list-style-type: none"> • Add or remove server roles and features • Perform diagnostics • Manage server configuration • Manage server storage 	Administrative Tools
Computer Management	<ul style="list-style-type: none"> • Share folders • Access system tools • Manage server storage • Manage services • Manage Routing and Remote Access 	Administrative Tools
Device Manager	<ul style="list-style-type: none"> • Configure devices • Update drivers 	Administrative Tools, Computer Management, Server Management
Task Manager	<ul style="list-style-type: none"> • View applications and processes • View basic performance information 	Ctrl+Alt+Del, right-click taskbar, Ctrl+Shift+Esc
Reliability and Performance Monitor	<ul style="list-style-type: none"> • Resource Overview • Performance Monitor • Reliability Monitor • Data Collector Sets 	Administrative Tools
Event Viewer	<ul style="list-style-type: none"> • View events in logs • Collect events at a single computer • Query events 	Administrative Tools, Computer Management, Server Management
Remote Desktop for Administration	<ul style="list-style-type: none"> • Remotely connect to servers and perform administrative tasks 	Control Panel > System > Remote settings

MCT USE ONLY. STUDENT USE PROHIBITED

Terminal Services Configuration	<ul style="list-style-type: none">• Configure Remote Desktop for Administration	Administrative Tools
Local User and Computers snap-in	<ul style="list-style-type: none">• Used to manage local users and groups	Computer Management, Server Management
Active Directory Users and Computers	<ul style="list-style-type: none">• Used to manage domain user accounts and groups	Administrative Tools
Run As Administrator	<ul style="list-style-type: none">• Elevate privileges of a program	Context menu when right-clicking an application shortcut
runas	<ul style="list-style-type: none">• Elevate privileges of a program	Command prompt

Module 8

Security Fundamentals


Contents:

Lesson 1: Defense-in-Depth	8-3
Lesson 2: Securing Access to Web Content	8-13
Lesson 3: Securing Access to Files	8-20
Lesson 4: Data Encryption	8-27
Lab: Configuring Data Security	8-33

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Defense-in-Depth
- Securing Access to Web Content
- Securing Access to Files
- Data Encryption



Security is an integral part of any computer network and needs to be considered from many perspectives. Data security for Web content and files accessed on network shares are common concerns. In addition to file and share permissions, data encryption can also be used to restrict data access.

Lesson 1

Defense-in-Depth

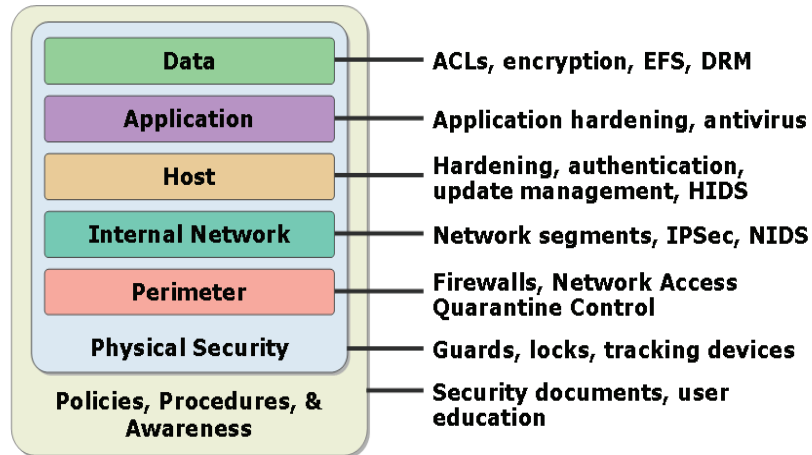
- What Is Defense-in-Depth?
- Policies, Procedures, and Awareness
- Physical Layer Security
- Perimeter Layer Security
- Internal Network Layer Security
- Host Layer Security
- Application Layer Security
- Data Layer Security
- Discussion: How to Protect Computer Systems

There are various ways to approach security design for computers. Defense-in-depth is one model for analyzing and implementing security for computer systems. The model uses layers to describe different areas of security.

What Is Defense-in-Depth?

Defense-in-depth uses a layered approach to security, which:

- Reduces an attacker's chance of success
- Increases an attacker's risk of detection



Key Points

Defense-in-depth is a layered model for analyzing and implementing computer system security. Each layer in the model represents a specific area that needs to be considered. This model also emphasizes the need to combine multiple security layers.

Question: How many layers of the defense-in-depth model should be secured?

Policies, Procedures, and Awareness

Policies, procedures, and awareness refers to the organizational policies and procedures implemented to help prevent security incidents

Sources of compromise include:

- Users unaware of rules
- Users viewing rules as unnecessary
- Social engineering

Key Points

Security is not only a technology-based solution. Organizations also implement policies, procedures, and awareness programs to help prevent security incidents. Security relies on staff and users following policies and procedures.

Question: What are some examples of policies and procedures being compromised and affecting computer system security?

USE PROHIBITED

Physical Layer Security

Physical layer security refers to helping prevent physical access and harm to IT infrastructure

Physical access to systems allows:

- Physical destruction
- Software installation
- Data modification
- Theft

Key Points

Physical layer security refers to preventing physical access and harm to IT equipment. This is one of the most commonly overlooked areas of securing computers systems.

Question: What are some examples of compromises when physical layer security is not in place?

Perimeter Layer Security

Perimeter layer security refers to connectivity between your network and other untrusted networks

Perimeter layer compromise includes:

- Attacks on resources in a perimeter network
- Attacks on remote clients
- Attacks on business partners

Key Points

Perimeter layer security refers to connectivity between your network and other untrusted networks. The most commonly considered untrusted network is the Internet.

Question: In what way could a business partner be a risk?

USE PROHIBITED

Internal Network Layer Security

Internal network layer security refers to events on the internally controlled network including WANs

Internal Network layer compromise includes:

- Unauthorized network communication
- Unauthorized network hosts
- Unauthorized packet sniffing



Key Points

Internal network layer security refers to events on the internally controlled network, including local area networks (LANs) and wide area networks (WANs). This layer is easier to secure because you have control of the devices on these networks.

Question: Why is wireless communication more at risk for packet sniffing than wired communication?

Host Layer Security

The host layer refers to the individual computers on the network

Host layer compromise can be:

- Exploiting operating system flaws
- Exploiting default operating system configurations
- Accomplished by a virus

Key Points

The host layer refers to the individual computers on the network. This includes the operating system, but not application software. Operating system services, such as a Web server, are included in host layer security.

Question: What is an example of host layer security being compromised?

Application Layer Security

The application layer refers to the applications running on the hosts

Application layer compromise can be:

- Exploiting application flaws
- Exploiting application default configurations
- Viruses introduced by a user

Key Points

The application layer refers to applications running on the hosts. This includes additional services, such as mail servers, and desktop applications, such as Microsoft Office.

Question: Give an example of malicious applications that may be installed by a user.

Data Layer Security

The data layer refers to the data stored on your computers

Data layer compromise can be:

- Unauthorized access to data files
- Unauthorized access to Active Directory
- Modification of application files

Key Points

The data layer refers to data stored on your computers. This includes data files, application files, databases, and Active Directory® Directory Services (AD DS).

Question: Give an example of a data-layer compromise.

NT USE PROHIBITED

Discussion: How to Protect Computer Systems

Discuss how to help protect a computer system at each layer of the defense in depth model:

- Policies, procedures and awareness
- Physical security
- Perimeter
- Internal network
- Host
- Application
- Data

Question: For each layer of the defense-in-depth model, how can a computer system be protected?

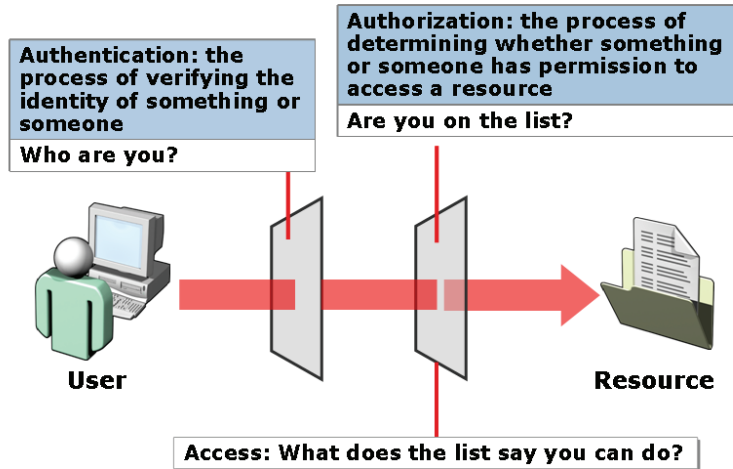
Lesson 2

Securing Access to Web Content

- What Are Authentication, Authorization, and Access?
- Process for Accessing Web Content
- IIS Authentication Methods
- IIS Authorization and Access Methods
- Other IIS Security Methods
- Demonstration: Securing Access to Web Content

The fundamental considerations when controlling access to data are authentication, authorization, and access. When securing access to Web content you must be aware of how Internet Information Services (IIS) is capable of performing these tasks. Provide a brief introduction to this lesson in normal text. A module must have at least two lessons.

What Are Authentication, Authorization, and Access?

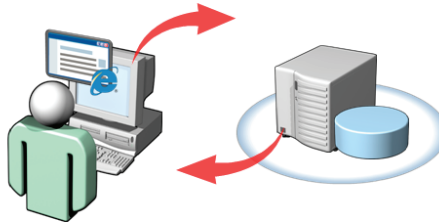


Key Points

Authentication is the process used to confirm your identity when accessing a computer system. The most common authentication method used to control access to resources is a username and password.

Question: Is it possible to have authorization and access without authentication?

Process for Accessing Web Content



- 1 The client requests content from the server
- 2 The server requests authentication credentials from the client
- 3 The client provides authentication credentials
- 4 The server verifies the client is allowed access to the content
- 5 The server sends the content to the client

Key Points

The typical process for accessing Web content is five steps.

Question: How will this process vary for anonymous access to Web content?

IIS Authentication Methods

IIS authentication methods include:

Authentication Type	Description
Basic	Sends credentials in clear text
Windows	Sends protected workstation credentials
Digest	Sends protected credentials
Client certificate mapping	Uses certificates as user credentials
IIS client certificate mapping	Better performing version of certificate mapping



Key Points

IIS supports multiple authentication methods for accessing Web content. The method selected must also be supported on the Web browser that is being used to access the content.

Question: What is the difference between basic authentication with SSL and digest authentication?

IIS Authorization and Access Methods

NTFS permissions:

- User access is based on the NTFS permissions of the file being accessed
- Anonymous access uses IUSR as a proxy user

URL Authorization: Allow or deny access to URLs

Sample code:

```
<authorization>
  <add accessType= "allow" users= "Vik_Malhotra" />
  <add accessType= "deny" roles= "administrators" />
  <add accessType= "deny" users= "*" />
</authorization>
```

Key Points

There are two methods used for controlling authorization and access to Web content when using IIS: NTFS permissions and URL Authorization

Question: When securing Web content will you use NTFS permissions or URL Authorization?

Other IIS Security Methods

Other IIS security methods include:

Security Method	Description
Request filtering	Filters all incoming requests based on rules configured by the Administrator
IP and domain restrictions	Enable and deny access to content based on originating IP address or domain name

Key Points

Request filtering is a system that restricts access requests based on the URL being requested. If the URL matches characteristics specified by the server administrator, then the request is denied.

IP and domain restrictions control access to Web content based on the source IP address of the computer requesting the content.

Question: Why are IP address restrictions not typically used for controlling access to Internet Web sites?

Demonstration: Securing Access to Web Content

In this demonstration, you will see how to secure access to Web content




Question: Which option is selected in IIS Manager to configure URL Authorization?

CONTENT USE PROHIBITED

Lesson 3

Securing Access to Files

- Windows Authentication Methods
- What Are Share Permissions?
- What Are NTFS Permissions?
- What Is Permissions Inheritance?
- How to Determine Effective Permissions
- Demonstration: Securing Access to Files



The most common way that users access data is from file shares on the network. Controlling access to files shares is done with file share permissions and NTFS permissions. Understanding how to determine effective permissions is essential to securing your files. Provide a brief introduction to this lesson in normal text. A module must have at least two lessons.

Windows Authentication Methods

Windows authentication methods include:

Windows Authentication Method	Description
Kerberos version 5 protocol	Capable of authenticating users and computers
NTLM	Used for backward compatibility with computers running pre-Windows 2000 operating systems and some applications
Certificate mapping	Certificates are used as authentication credentials

Key Points

When accessing files over the network, you must be authenticated to verify your identity. This is done during the network logon process. Windows Server® 2008 operating system includes the authentication methods shown above for network logons.

Question: Which authentication method is used when a client computer running the Windows Vista® operating system logs on to AD DS?

What Are Share Permissions?

Share permissions:

- Control access to folders shared over the network
- Do not control local access to files and folders
- Can be allowed or denied

Permission	Description
Full Control	Allows all permissions including the ability to change permissions
Read	Allows users to read existing files
Change	Allows users to create new files or delete, modify, and read existing files

Key Points

To make files accessible over a network, the folder must be shared. This makes files in that folder and subfolders accessible. Share permissions are a way to control who is able to access the share contents and what can be done with the share contents.

Question: In what situation would you allow users only read access to a folder?

What Are NTFS Permissions?

NTFS permissions:

- Are assigned per file or directory
- Can always be set by the file or folder owner
- Are much more flexible than share permissions

The basic permissions are:

- Full control
- Modify
- Read and execute
- List folder contents
- Read
- Write

Key Points

NTFS permissions are used to control which users or groups can access or modify files and folders on NTFS formatted partitions. These permissions are much more flexible than share permissions because they can be assigned individually for each file or folder as required.

Question: What NTFS permission will you assign for most users?

NTFS USE PROHIBITED

What Is Permissions Inheritance?

Permissions inheritance:

- Allows permissions set on a folder to be applied automatically to files in that folder and subfolders
- Simplifies assignment of NTFS permissions
- Can be blocked



Key Points

Permissions Inheritance allows the NTFS permissions set on a folder to be applied automatically to files in that folder and subfolders. This means that NTFS permissions for an entire folder structure can be set at a single point. And if modification is required, modification needs to be done only at a single point.

Question: Why is permissions inheritance a benefit for administrators?

How to Determine Effective Permissions

When determining effective permissions:

- User and group permissions are combined
- Deny permissions override allow permissions
- The most restrictive of NTFS and share permissions apply

Key Points

Effective permissions are the permission any user has to a file or folder. This is different from the permissions that are assigned or granted to a specific user. User and group permissions are combined to determine effective permissions.

Question: How does granting the Everyone group Full Control share permissions simplify the management of permissions?

NT USE PROHIBITED

Demonstration: Securing Access to Files

In this demonstration, you will see how to secure access to files



Question: How does simple file sharing differ from advanced file sharing?

Lesson 4

Data Encryption

- Types of Encryption
- What Is EFS?
- What Is BitLocker?
- Demonstration: Using EFS

NTFS permissions and share permissions help prevent users from accessing files over the network or through the operating system. However, if a hard disk is placed in a different computer, it is easy to retrieve the data off of it regardless of the permissions that have been assigned. Encryption provides more advanced protection for data. Provide a brief introduction to this lesson in normal text. A module must have at least two lessons.

Types of Encryption

Encryption converts data into a format that cannot be read directly

Types of encryption:

- Symmetric
- Asymmetric
- Hash

Encrypted content is referred to as ciphertext

Encryption is a system that converts data into a format that cannot be read directly. Data that is unencrypted is known as cleartext or plaintext. Data that has been encrypted is known as ciphertext. The mathematical formula used to encrypt the data is known as an algorithm. A key is a large number that is used with the algorithm as part of the encryption process.

There are three types of encryption:

Symmetric encryption uses the same key to encrypt and decrypt the data. This type of encryption is strong and fast. However, it is difficult to securely pass the key between computers during the initial configuration.

Asymmetric encryption uses two different keys. What is encrypted by one key can only be decrypted by the other key. This type of encryption is slower and weaker than symmetric encryption but avoids the problem of securely passing the key.

Hash encryption is one-way encryption. After data is encrypted with hash encryption, it cannot be decrypted back to plaintext. This type of encryption is used to compare two pieces of data. For example, hash encryption is used to send passwords over the network during authentication so that there is no risk of the password being intercepted.

Note: Asymmetric encryption is also known as public key encryption (PKI).

MCT USE ONLY. STUDENT USE PROHIBITED

What Is EFS?

EFS is a system for encrypting files

EFS:

- File contents are protected by a symmetrical key
- The symmetrical key is protected by asymmetrical encryption
- Enabled in the properties of a files
- Requires a user certificate
- Can be used on shared files
- Can be configured with a recovery agent in case user certificates are lost

Key Points

Encrypting Files System (EFS) is a system for encrypting data files that is included as part of Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. EFS generates a unique symmetrical encryption key to encrypt each file. The symmetrical key is stored in the file header.

Question: How does asymmetric encryption avoid the problem of securing the encryption between the two computers?

What Is BitLocker?

BitLocker is a system that encrypts the entire operating system drive and potentially data volumes

Types of encryption:

- Helps protect data on the operating system drive
- Helps protect the operating system from modification
- Access to the operating system drive is controlled by encryption keys

Key Points

BitLocker is a system that encrypts the entire operating system volume. Encryption of additional data volumes is also an option. Encryption keys are handled automatically in the background with little overhead.

Question: In what scenario would BitLocker be useful on a server?

INTENSE PROHIBITED

Demonstration: Using EFS

In this demonstration, you will see how to use EFS



Question: How is EFS enabled for a file?

Lab: Configuring Data Security

- Exercise 1: Creating a Simple Share
- Exercise 2: Creating an Advanced Share
- Exercise 3: Configuring Web Content for Anonymous Access
- Exercise 4: Securing Web Content

Logon information

Virtual computer	NYC-DC1, NYC-SVR1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are a server administrator for Woodgrove Bank. A new computer running Windows Server 2008 is being deployed. This server has data copied to it, but the data is not yet shared or secured in the way it needs to be. You need to appropriately secure the data.

Exercise 1: Creating a Simple Share

The security for marketing department data needs to be configured as a share with a single set of permissions that are inherited throughout the entire folder structure. There is not variation of security from one folder to the next. All marketing users have Modify permission to all files. You have determined that simple file sharing is an appropriate way to configure this share.

- ▶ Task 1: Verify the current configuration
 1. On NYC-DC1, use Active Directory Users and Computers to view the members of the Marketing Group.
 2. Browse to D:\Mod08\Labfiles\Marketing and open the Properties of the Marketing folder.
 3. View the default NTFS permissions on the Marketing folder by selecting the Security tab.
- ▶ Task 2: Create a simple share
 1. On NYC-DC1, open the **Properties** of the Marketing folder.
 2. Create a simple share by clicking the Share button on the Sharing tab.
 3. Define the following permissions:
 - **Administrator**: Owner
 - **Marketing**: Contributor
 4. Take note of the UNC path for the share.
- ▶ Task 3: Review the configuration changes
 1. On NYC-DC1, open the **Properties** of the Marketing folder.
 2. View the NTFS permissions for the Marketing folder.
 3. Click the **Advanced Sharing** button to review the share permissions for the Marketing folder.
- ▶ Task 4: Test the configuration changes
 1. On NYC-CL1, log on as Kim with a password of **Pa\$\$w0rd**.
 2. Verify that Kim is able to access and modify the file \\NYC-DC1\Marketing\Marketing Document.doc
 3. Log off as Kim and log on as Paul with a password of **Pa\$w0rd**.
 4. Verify that Paul cannot access the file \\NYC-DC1\Marketing\Marketing Document.doc.

Exercise 2: Creating an Advanced Share

The customer service department would like all customer service data accessible through a single share. The permissions for users vary depending on the folder. Consequently simple sharing is not an appropriate way to configure permissions. You must create an advanced share and set NTFS permissions appropriately for each group.

- ▶ Task 1: Verify the current configuration
 1. On NYC-DC1, use Active Directory Users and Computers to view the members of the following groups:
 - **CSRRetail**
 - **CSRCommercial**
 - **CSRManagement**
 2. View the NTFS permissions configured on the following folders:
 - D:\Mod08\Labfiles\Customers
 - D:\Mod08\Labfiles\Customers\Commercial
 - D:\Mod08\Labfiles\Customers\Retail
- ▶ Task 2: Configure NTFS permissions
 1. On NYC-DC1, remove inherited permissions from the Customers folder in the Advanced Security settings.
 2. Assign the following NTFS permissions to the Customers folder:
 - **Administrators**: Allow Full control
 - **CSRManagement**: Allow Modify
 - **CSRRetail**: Allow List folder contents
 - **CSRCommercial**: Allow List folder contents
 3. Assign the following NTFS permission to the Commercial folder:
 - **CSRCommercial**: Allow Modify
 - **CSRRetail**: Deny List folder contents
 4. Assign the following NTFS permission to the Retail folder:
 - **CSRRetail**: Allow Modify
 - **CSRCommercial**: Deny List folder contents

- ▶ Task 3: Create and configure the CSR share
 1. On NYC-DC1, open the properties of the Customers folder.
 2. Create an Advanced Share using the following information:
 - **Share name:** CSR
 - **Permissions:** Full control for Everyone
- ▶ Task 4: Test the permission changes
 1. On NYC-CL1, log on as Tamara with a password of **Pa\$\$w0rd**.
 2. Verify that Tamara is able to access and modify the file \\NYC-DC1\CSR\Commercial\Commercial Loan Document.doc.
 3. Verify that Tamara is able to access and modify the file \\NYC-DC1\CSR\Retail\Retail Loan Document.doc.
 4. Log on as Lori with a password of **Pa\$\$w0rd**.
 5. Verify that Lori is able to access and modify the file \\NYC-DC1\CSR\Commercial\Commercial Loan Document.doc.
 6. Verify that Lori is not able to access and modify the file \\NYC-DC1\CSR\Retail\Retail Loan Document.doc.
- ▶ Task 5: Limit list folder contents permission
 1. On NYC-DC1, modify the advanced security permissions of the Customers folder to apply List folder contents permission to this folder and files for the following groups:
 - **CSRCommercial**
 - **CSRRetail**
- ▶ Task 6: Test the limiting of list folder contents permission
 1. On NYC-CL1, log on as Lori with a password of **Pa\$\$w0rd**.
 2. Verify that Lori is able to list the contents of the \\NYC-DC1\CSR\Commercial folder.
 3. Verify that Lori is not able to list the contents of the \\NYC-DC1\CSR\Retail folder.

Exercise 3: Configuring Web Content for Anonymous Access

Woodgrove Bank has decided to make all company promotional materials available on the company Web site. To do this, a new virtual directory must be created on the Web site. The promotional materials should be available to users without authentication.

- ▶ **Task 1: Create a new virtual directory for Web content**
 1. On NYC-DC1, open Internet Information Services Manager
 2. Add a virtual directory to the Default Web Site with the following options:
 - **Alias:** public
 - **Physical path:** D:\Mod08\Labfiles\WebContent\Public

- ▶ **Task 2: View the configuration for anonymous authentication**

On NYC-DC1 in Internet Information Services Manager, open the Authentication settings for the public virtual directory.

Edit the settings for Anonymous Authentication to verify that the specific user is IUSR.

- ▶ **Task 3: Configure NTFS permissions for anonymous access to Web content**
 1. Edit the NTFS permissions on the public folder:
 - Block inherited permissions and copy the existing permissions
 - Remove all permissions for the Users group
 - Add **IUSR** with Read & Execute Permissions
 - Add **NETWORK SERVICE** with Read & Execute Permission

- ▶ **Task 4: Test anonymous access to Web content**
 1. On NYC-CL1, log on as Lori with a password of **Pa\$\$w0rd**.
 2. Verify that anonymous access is functioning by using Internet Explorer to open <http://nyc-dc1.woodgrovebank.com/public/promotional document.txt>
 3. Verify that the access is anonymous by using Internet Explorer to open <http://nyc-dc1.woodgrovebank.com/public/user.aspx>

Exercise 4: Securing Web Content

The marketing department would like some files to be available on a Web site. This will allow them to download the files when they are away from the office. The data does not include company secrets, but should be secured by requiring authentication. Only users from the marketing group should have access. When in the office, users should not be prompted for authentication credentials.

- ▶ Task 1: Create a new virtual directory for marketing data
 1. Open Internet Information Services (IIS) Manager.
 2. Add a virtual directory to the Default Web Site with the following options:
 - **Alias:** marketing
 - **Physical path:** D:\Mod08\Labfiles\WebContent\Marketing
- ▶ Task 2: Configure Basic authentication
 1. On NYC-DC1 in Internet Information Services Manager, open the Authentication settings for the marketing virtual directory.
 2. Disable Anonymous Authentication.
 3. Enable Basic Authentication.
 4. Edit the settings for Basic Authentication to use woodgrovebank as the default domain.
- ▶ Task 3: Restrict access to Web content with URL authorization
 1. On NYC-DC1 in Internet Information Services Manager, open the Authorization Rules for the marketing virtual directory.
 2. Add a rule to allow access for the Marketing group.
 3. Remove the rule that allows access for all users.
- ▶ Task 4: Test Basic authentication to Web content
 1. On NYC-CL1, log on as **Kim** with a password of **Pa\$\$w0rd**.
 2. Verify that members of the Marketing group are allowed access by using Internet Explorer to open [http://nyc-dc1.woodgrovebank.com/marketing/marketing staff directory.txt](http://nyc-dc1.woodgrovebank.com/marketing/marketing%20staff%20directory.txt).
 3. When prompted, log on as **Kim** with a password of **Pa\$\$w0rd**. Kim is a member of the marketing group.

4. Close Internet Explorer.
 5. Verify that non-members of the Marketing group are not allowed access by using Internet Explorer to open <http://nyc-dc1.woodgrovebank.com/marketing/marketing staff directory.txt>.
 6. When prompted, log on as **Mark** with a password of **Pa\$\$w0rd**. Mark is not a member of the marketing group.
 7. Close Internet Explorer.
- ▶ Task 5: Configure Windows authentication for Web content
1. On NYC-DC1 in Internet Information Services Manager, open the Authentication settings for the marketing virtual directory.
 2. Disable **Basic Authentication**.
 3. Enable **Windows Authentication**.
- ▶ Task 6: Test Windows authentication
1. On NYC-CL1, prepare Internet Explorer for Windows Authentication by adding the intranet site by selecting the **Security** tab in **Internet Options**:
 - <http://nyc-dc1.woodgrovebank.com>
 2. Verify that Windows authentication is functional by using Internet Explorer to open <http://nyc-dc1.woodgrovebank.com/marketing/marketing staff directory.txt>.
 3. Verify the user credentials for authentication by using Internet Explorer to open <http://nyc-dc1.woodgrovebank.com/marketing/user.aspx>.

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Real-world Issues and Scenarios
- Best Practices
- Tools

Review Questions

1. Why is it important to implement security at multiple layers of the defense-in-depth model?
2. To allow access for anonymous Web site visitors, which user account should be given access to files?
3. How are share permissions and NTFS permissions combined to create effective rights?
4. Which type of encryption is the strongest and fastest?

Real-world Issues and Scenarios

1. The research and development department in your organization would like to encrypt some data that is particularly sensitive. All data is stored on a single server and you want to encrypt only the necessary files. Which Windows Server 2008 encryption technology is appropriate for this scenario?

2. Your organization has decided to increase security by implementing smart cards for logon authentication. In addition to obtaining the smart cards and the smart card readers, what else must be obtained for each user?
3. You have implemented a new Web-based application for internal users on a computer running Windows Server 2008. The application uses the authentication methods built into IIS. The installation instructions provided the steps to configure basic authentication secured by SSL. However, the users are complaining about having to enter authentication credentials each time they open the application. How can you resolve this?

Best Practices for Securing Files

- Distill and summarize the best practices from the module and invite students to supplement or modify the best practices for their own work situations.
- Supplement or modify the following best practices for your own work situations:
- Consider permissions inheritance when designing the file system structure.
- Assign permissions to groups rather than individual users whenever possible.
- Use Deny permission to restrict a user or a few users from accessing a file or folder.
- When there is a risk of physical access to a hard disk, use encryption to protect files.
- Use EFS to encrypt files and folders.
- Use BitLocker to encrypt entire data volumes.

Tools

Tool	Use to	Where to find it
Internet Information Services (IIS) Manager	<ul style="list-style-type: none"> • Manage Web sites 	Administrative Tools

Module 9

Fundamentals of Securing Network Communication

Contents:

Lesson 1: Public Key Infrastructure

Lesson 2: Using Certificates

Lab: Securing Web Communication

MCT USE ONLY. STUDENT USE PROHIBITED

9-3

9-10

9-17

Module Overview

- Public Key Infrastructure
- Using Certificates

Securing communication is the process of encrypting data while it is in transit over the networks. When securing network communication, certificates can be used for authentication and encryption. The system for issuing and managing certificates is a public key infrastructure (PKI).

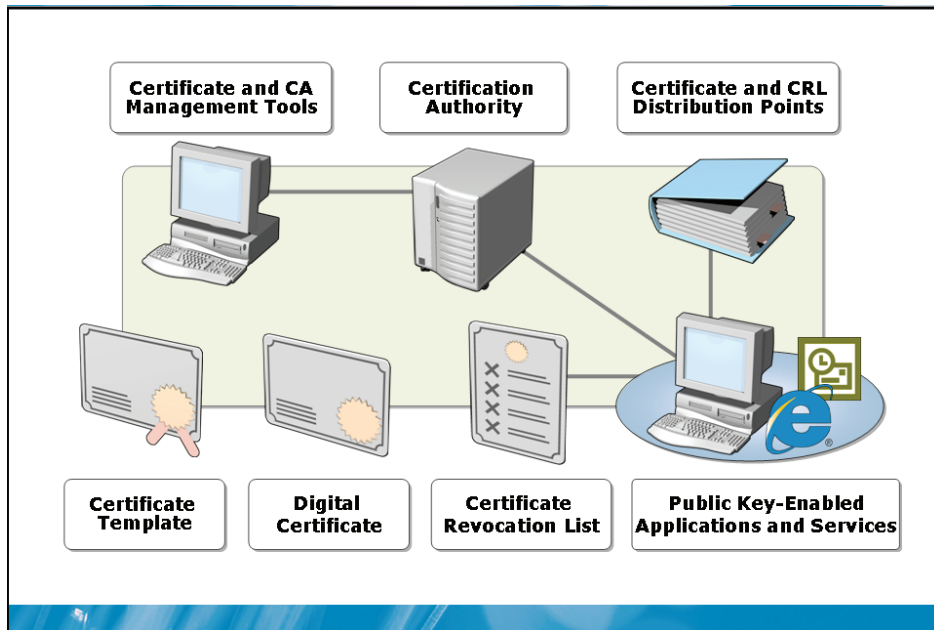
Lesson 1

Public Key Infrastructure

- Components of Public Key Infrastructure
- Selecting a Certification Authority
- What Is a Certificate?
- Types of Certificates
- What Is a Certificate Template?
- New Certificate Features in Windows Server® 2008

Certification authorities (CAs) are a critical component of a PKI. They are responsible for issuing certificates to users and computers. Certificate templates can be used to control what types of certificates are issued by a CA and to which devices or users.

Components of Public Key Infrastructure



Key Points

The components of a PKI work together to distribute and validate certificates.

Question: Can you think of a situation where certificates can be used without being issued by a CA?

Selecting a Certification Authority

Internal CAs:

- Generate certificates free of charge
- Are trusted by internal computers
- Are not trusted by computers outside the organization

External CAs:

- Require a fee for each certificate
- Are trusted by internal and external computers

Key Points

You can obtain certificates from either an internal CA or an external CA. An internal CA is controlled by your organization and managed internally on one of your servers. An external CA is a third-party organization that issues certificates to other organizations.

Question: Which type of CA would you use to secure access to a Web server?

What Is a Certificate?

A digital certificate:

- Can be used to verify identity
- Contains a public key
- Contains information about the issuer and the subject
- Is signed by a CA

Key Points

A certificate is collection of information that can be used for identification or encryption. Certificates can be issued to users, computers, or other devices.

Question: How does a certificate uniquely identify a subject?

Types of Certificates

Certificates can be for limited uses:

Certificate Type	Description
User	Assigned to users for performing actions such as file encryption
Computer	Assigned to computers for performing actions such as domain communication
CA	Assigned to certification authorities to authorize the issuing of certificates

Key Points

There are multiple types of certificates. Each certificate type has a range of allowed uses.

Question: Why is it important to understand the multiple types of certificates?

BETA COURSEWARE. USE PROHIBITED

What Are Certificate Templates?

Certificate templates include:

Certificate Template	Description
Administrator	Allows trust list signing and user authentication
Basic EFS	Used by Encrypting File System (EFS) to encrypt data
Computer	Allows a computer to authenticate itself on the network
Domain Controller	All-purpose certificates held by domain controllers
IPSec	Used by IP Security (IPSec) to digitally sign, encrypt, and decrypt network communication
User	Certificate to be used by users for e-mail, EFS, and client authentication
Web Server	Proves the identity of a Web server

Key Points

Certificate templates are used to simplify the management of certificate issuance. A certificate template defines the certificate characteristics required for specific situation. The certificate template also defines how a certificate can be issued.

Question: Why are certificate templates useful?

New Certificate Services Features in Windows Server 2008

New certificate services features include:

New Feature	Description
Enterprise PKI	A tool for monitoring your PKI environment.
Network Device Enrolment Service	Allows routers and switches to obtain X.509 certificates
Online certificate status protocol	Allows queries to view the validity of certificates
Policy settings	Updated with addition features for managing certificated by using Group Policy
Web enrolment	Updated to use a new DLL for enrolment control
Cryptography Next Generation	A set of APIs for performing cryptographic operations.
Restricted Enrolment Agent	An authorized individual that can approve certificate requests for specific security groups

Key Points

The Windows Server® 2008 operating system includes a number of new and updated features. These features include increased security and improved performance.

NT USE PROHIBITED

Lesson 2

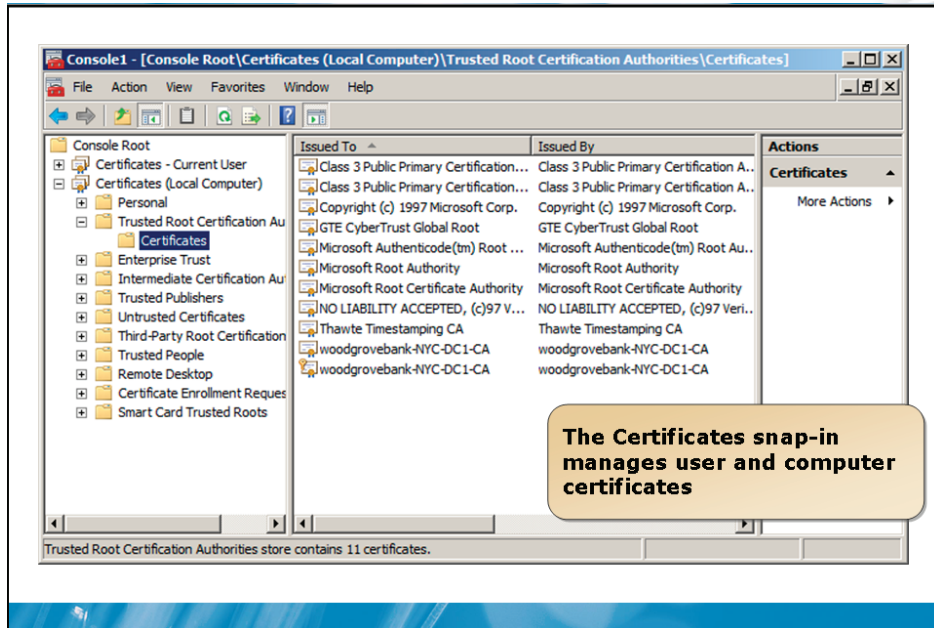
Using Certificates

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is the Certificates Snap-in?
- What Is SSL?
- What Is IPSec?
- What Is S/MIME?
- How Certificates Are Used for Remote Access
- Demonstration: Obtaining a User Certificate

Certificates are used as part of the process for securing network communication. They are used to secure VPN connections, communication with Web servers, and e-mail. The Certificates snap-in is used to manage the certificates on a computer running Windows Server 2008.

What Is the Certificates Snap-in?



Key Points

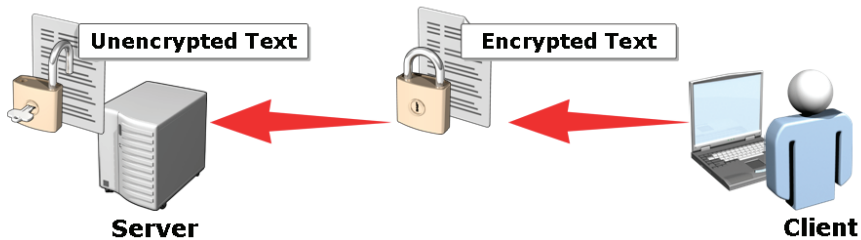
The Certificates snap-in is the utility used to manage user certificates and computer certificates in Windows Server 2008 and the Windows Vista® operating system.

Question: In what situation should you verify existing certificates?

What Is SSL?

Secure Sockets Layer (SSL):

- Encrypts communication between a client and server
- Requires no client configuration
- Is commonly used with basic authentication
- Uses asymmetric encryption to establish a secure channel
- Uses symmetric encryption to secure data in transit



Key Points

Secure Sockets Layer (SSL) is a protocol used to encrypt communication between a client and server. It is commonly used with basic authentication to encrypt the authentication credentials, as well as the data being transmitted over the network. When the URL for a Web site uses the HTTPS protocol, it is using SSL to secure communication.

Question: What makes SSL easier to implement than some other encryption systems?

What Is IPSec?

IPSec:

- Secures communication between two hosts
- Authenticates both hosts
- Is configured by using Windows Firewall with Advanced Security
- Can use multiple authentication types:
 - Pre-shared key
 - Kerberos version 5 protocol
 - Certificates

Key Points

IPSec is a method for encrypting network communication between hosts. It is also used to digitally sign packets to ensure that they are not modified during transit. You control the data encryption by Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port numbers and host addresses.

Question: Why would you use TCP/UDP ports to control the data encrypted by IPSec?

What Is S/MIME?

Secure Multipurpose Internet Mail Extensions (S/MIME):

- Is a standard for helping to secure e-mail communication
- Can encrypt e-mail messages
- Can digitally sign e-mail messages
- Is supported by most e-mail clients
- Requires coordination between senders

Key Points

Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard that uses certificates to secure e-mail. The messages can be encrypted, digitally signed, or both. Encrypting a message prevents unauthorized users from reading the message. Digitally signing a message verifies the sender and ensures that the message was not modified during delivery.

Question: To use S/MIME, what configuration must be completed by an email sender in addition to importing a certificate into the e-mail client?

How Certificates Are Used for Remote Access

When certificates are used for remote access:

- The certificates are used as an authentication method
- Security is increased over using a username and password
- Can be placed on a smart card for additional security

Key Points

Certificates are used as an authentication method for remote access such as a VPN connection.

Question: Why is a certificate more secure than a user name and password?

CONTENT USE PROHIBITED

Demonstration: Obtaining a User Certificate

In this demonstration, you will see how to obtain a user certificate.

Question: What is the benefit of obtaining a certificate through the Certificates snap-in rather than the Web interface snap-in?

Lab: Securing Web Communication

- Exercise 1: Verifying the Trusted Root CA
- Exercise 2: Securing a Web site by using SSL

Logon information

Virtual computer	NYC-DC1, NYC-DC1-CA
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

Woodgrove bank has several Web sites that are accessible from outside the organization. These Web sites require users to log on by using their network credentials. It is essential that the credentials are protected during authentication and that the data is encrypted while in transit. To do this, you must implement basic authentication with SSL for your Web site.

Exercise 1: Verifying the Trusted Root CA

Woodgrove Bank has recently implemented an Enterprise CA on Windows Server 2008. You would like to view the configuration of the CA and verify that the CA is trusted by workstations.

- ▶ Task 1: View CA properties by using the Certification Authority administrative tool
 1. On NYC-DC1, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Open the Certification Authority administrative tool.
 3. Verify the name of the CA is WoodgroveBank-NYC-DC1-CA.
 4. View the properties of the CA certificate on the General tab in the properties of WoodgroveBank-NYC-DC1-CA.
 5. View the certificate templates that are available.
- ▶ Task 2: View CA status by using the Enterprise PKI snap-in
 1. On NYC-DC1, open an empty MMC console.
 2. Add the Enterprise PKI snap-in to the MMC console.
 3. View the status of all CAs.
 4. View the detailed status of WoodgroveBank-NYC-DC1-CA.
- ▶ Task 3: View Trusted Root CAs on a client
 1. On NYC-CL1, log on as Dana with a password of Pa\$\$w0rd.
 2. Open an empty MMC console.
 3. Add the Certificates snap-in to the MMC console.
 4. Verify that WoodgroveBank-NYC-DC1-CA is listed as a trusted root certification authority.

Exercise 2: Securing a Web site by using SSL

To secure the authentication and data transfer from a Web site, you must obtain and install a certificate for a Web server. SSL must also be enabled on the Web site.

► Task 1: Verify Web site functionality

1. On NYC-CL1, use Internet Explorer and attempt to access <http://nyc-dc1.woodgrovebank.com>.
2. On NYC-CL1, use Internet Explorer and attempt to access <http://nyc-dc1.woodgrovebank.com>.

This is unsuccessful.

► Task 2: Obtain a new certificate for the Web server

On NYC-DC1, open the Internet Information Services (IIS) Manager administrative tool.

1. View the Server Certificates for NYC-DC1.
2. Create a domain certificate with the following settings:
 - Common name: NYC-DC1.woodgrovebank.com
 - Organization: Woodgrove Bank
 - Organizational unit: IT
 - City/locality: New York
 - State/province: New York
 - Country/region: US
 - Online Certification Authority: WoodgroveBank-NYC-DC1-CA
 - Friendly name: Web SSL Certificate

- ▶ Task 3: Configure SSL on the Web site
 1. On NYC-DC1 in Internet Information Services (IIS) Manager, edit the bindings for Default Web Site.
 2. Add the following binding:
 - Type: https
 - IP address: All Unassigned
 - Port: 443
 - SSL certificate: Web SSL Certificate
 - In the SSL settings for Default Web site, configure the Web site to require SSL.
- ▶ Task 4: Verify encryption for the Web site
 1. On NYC-CL1, use Internet Explorer and attempt to access <http://nyc-dc1.woodgrovebank.com>.

This is unsuccessful.

2. On NYC-CL1, use Internet Explorer and attempt to access <http://nyc-dc1.woodgrovebank.com>.

This is successful.

3. On NYC-CL1, use Internet Explorer and attempt to access <http://nyc-dc1.woodgrovebank.com>.

This is unsuccessful and a warning displays.

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Best Practices
- Tools

Review Questions

1. Which component of a PKI lists certificates that have been invalidated before their expiry date?
2. How are certificates used with IPSec?

Real-world Issues and Scenarios

1. Your organization uses Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) to retrieve and send e-mail when outside the organization. A recent security audit has determined that all remote e-mail is being transmitted in clear text and can be read by anyone with a packet sniffer. Even the usernames and passwords are being transmitted in clear text. How can you resolve this problem?
2. Your organization would like to implement smart cards for authentication. To ease the management burden, you would like to authorize specific individuals to configure smart cards for a geographical location. How can this be implemented

Best Practices for Obtaining and Generating Certificates

- Distill and summarize the best practices from the module and invite students to supplement or modify the best practices for their own work situations.
- For applications with external users, obtain certificates from an external CA to ensure that the certificates are trusted.
- For applications with internal users only, obtain certificates from an internal CA to reduce costs.
- Use certificate templates to allow automation of certification issuance.
- Use certificate templates to control certificate issuance based on Active Directory users.
- Use certificate templates to simplify the issuance of certificates with a consistent configuration.
- Use a Restricted Enrollment Agent to control the issuance of certificates for specific security groups.
- Use Group Policy to automate the issuance of certificates whenever possible.

Tools

Tool	Use for	Where to find it
Certification Authority	<ul style="list-style-type: none"> • Manage CA • Approve certificate requests 	Administrative Tools
Enterprise PKI	<ul style="list-style-type: none"> • Monitoring multiple CAs 	MMC snap-in
Certificates	<ul style="list-style-type: none"> • View certificates issued to users and computers • Request new certificates • Export/import certificates 	MMC snap-in
Active Directory Certificate Services Web Site	<ul style="list-style-type: none"> • Request certificates • Download certificates 	http://CAservername/certsrv

Module 10

Windows Firewall and Caching Fundamentals

Contents:

Lesson 1: Overview of Perimeter Security	10-2
Lesson 2: Windows Firewall Overview	10-8
Lesson 3: Creating Windows Firewall Rules	10-15
Lesson 4: Monitoring and Troubleshooting Windows Firewall	10-22
Lab: Using Windows Firewall	10-29

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

MCT USE ONLY. STUDENT USE PROHIBITED

- Overview of Perimeter Security
- Windows Firewall Overview
- Creating Windows Firewall Rules
- Monitoring and Troubleshooting Windows Firewall

Firewalls are commonly used to create perimeter networks to protect computers on a private network. However, there are also host-based firewalls that protect an individual computer. Windows Firewall is a host-based firewall that is included with Windows Server 2008. You can configure firewall rules and monitor Windows Firewall.

Lesson 1

Overview of Perimeter Security

- Discussion: Security Concerns for a Perimeter Network
- What Is A Proxy Server?
- What Is a Reverse Proxy Server?
- What Is a Host-based Firewall?

Perimeter security is used to protect your network from external attackers. Some of the tools you can use to protect a perimeter network are proxy servers and firewalls.

Microsoft
USE PROHIBITED

Discussion: Security Concerns for a Perimeter Network

- What are some of the resources located in a perimeter network?
- Why is a perimeter network more at risk than an internal network?
- What are some of the specific risks to perimeter network resources?

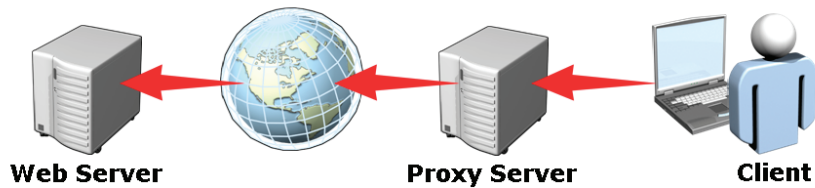
Key Points

Answer the questions in a classroom discussion.

What Is A Proxy Server?

A proxy server:

- Accepts request on behalf of a client
- Isolates clients from resources
- Requires clients to be configured to use the proxy server
- Uses caching to increase data access speed
- Can evaluate contents of packets not just port numbers



Key Points

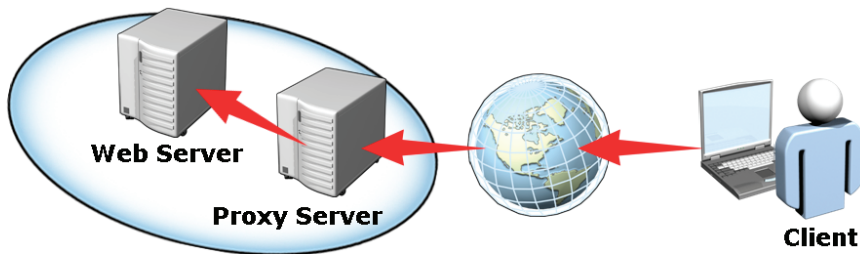
A proxy server is a server that forwards requests from clients to other servers. Proxy servers are typically located in the same physical location as the clients. Clients are configured to use the proxy server. For example, an organization may have a proxy server to filter Web requests. Internet Explorer must be configured to use the proxy server.

Question: How does caching reduce Internet link utilization?

What Is a Reverse Proxy Server?

A reverse proxy:

- Accepts requests on behalf of a server
- Isolates servers from clients
- Points to a single server
- Requires no client configuration
- Uses caching to reduce load on a server



Key Points

Similar to a proxy server, a reverse proxy server forwards requests from clients to servers. However, a reverse proxy server is placed at the same physical location as the server to provide protection from clients.

Question: How does a reverse proxy server protect a Web server?

What Is a Host-based Firewall?

A host-based firewall:

- Is a software firewall on the operating system
- Is effective on the internal network
- Allows software-based exceptions in addition to IP- and port-based exceptions

Key Points

A traditional firewall is basically a router that applies rules to packets as they are forwarded to a network. The firewall functions as a gateway device to control packets going in and out of the network.

Question: Are host-based firewalls a replacement for traditional firewalls?

Lesson 2

Windows Firewall Overview

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is Windows Firewall?
- New Features in Windows Firewall
- Windows Firewall Administration Tools
- Options Available Through Basic Firewall Configuration
- Default Windows Firewall Configuration
- Demonstration: Basic Firewall Configuration

Windows Firewall in Windows Server 2008 has many improvements from the previous version in Windows Server 2003. In addition to using the basic interface in the previous version of Windows Firewall, you can also perform administration by using Windows Firewall with Advanced Security.

What Is Windows Firewall?

Windows Firewall is:

- A host-based firewall
- Enabled by default
- Automatically configured when new roles and features are installed

Key Points

Windows Firewall is a host-based firewall included with Windows Server 2008. It is enabled by default to ensure that a server is protected from the time of installation.

As a part of the operating system, the configuration of Windows Firewall is integrated with the installation of operating system roles and features. When you install new roles or features, the rules in Windows Firewall are updated automatically as necessary. This simplifies the administrative tasks required for configuring a host-based firewall.

Question: Why is it beneficial to update firewall rules automatically when new roles and features are added?

New Features in Windows Firewall

New features in Windows Firewall include:

Feature	Description
Outbound rules	<ul style="list-style-type: none">• Rules that control packets leaving the host• Disabled by default
Integration of IPSec rules	<ul style="list-style-type: none">• Control the creation of IPSec connections• Replaces IPSec policies
Network profile integration	<ul style="list-style-type: none">• Rules can apply to public, private, and/or domain networks

Key Points

Windows Firewall in Windows Server 2008 has the same features as Windows Firewall in Windows Vista.

Question: Can you think of a situation where network profile integration would be useful for a server?

Windows Firewall Administration Tools

Basic firewall configuration:

- Available through Control Panel
- Does not control outbound rules or IPSec
- Is similar to previous versions of Windows Firewall

Windows Firewall with Advanced Security:

- Allows complete configuration of Windows Firewall
- Allows configuration of IPSec rules

Key Points

Basic firewall configuration in Windows 2008 is similar to the Windows Firewall configuration tool in previous versions of Windows. The basic firewall configuration tool is available in Control Panel. However, this tool is limited to the functions available in previous versions of Windows Firewall and cannot configure advanced features such as outbound rules or IPSec.

Question: When would you use the basic firewall configuration tool instead of Windows Firewall with Advanced Security?

BETA COURSEWARE. USE PROHIBITED

Options Available Through Basic Firewall Configuration

Basic firewall configuration options include:

- Enable or disable
- Block all incoming connections
- Configure exceptions
- Specify enabled adapters

Key Points

The basic firewall configuration tool has a limited set of configuration options.

Question: Why would you disable Windows Firewall for a specific network adapter?

Default Windows Firewall Configuration

The default Windows Firewall configuration is:

- All inbound connections are blocked
- All outbound connections are allowed
- Inbound exceptions are automatically modified for new roles and features

Key Points

It is important to understand the default configuration for Windows Firewall because you may need to modify the configuration to suit your business needs.

Demonstration: Basic Firewall Configuration

In this demonstration, you will see how to perform basic firewall configuration

Key Points

Question: Which tasks can you use the basic firewall configuration tool to perform?

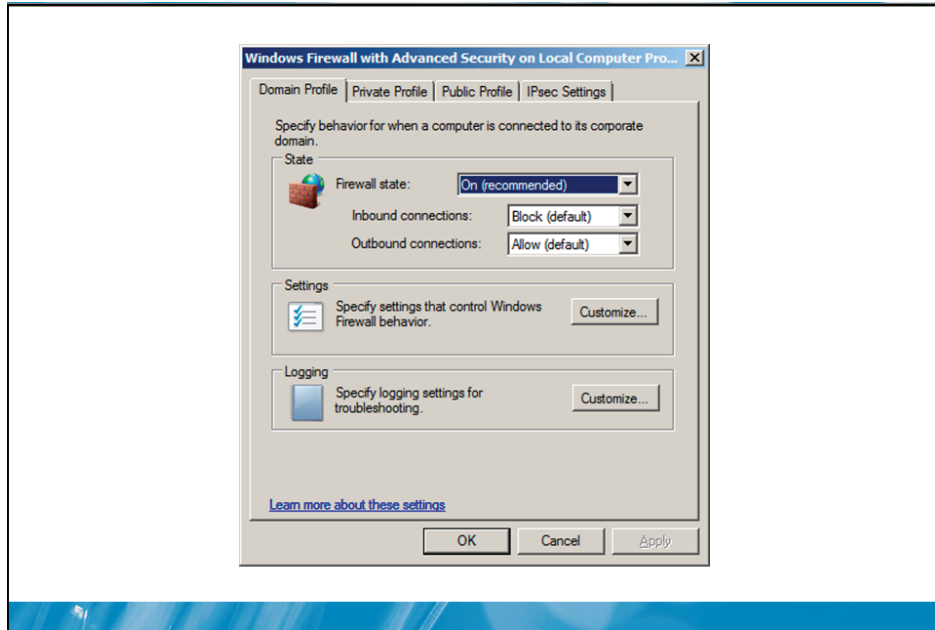
Lesson 3

Creating Windows Firewall Rules

- What Are Profiles?
- What Are Rules?
- What Are Rule Types?
- Rule Configuration Options
- What Are Connection Security Rules?
- Demonstration: Creating a Rule

Windows Firewall rules can be configured for inbound and outbound traffic. Each rule can also be assigned to a profile, which applies rules based on the type of network. Also, you can create connection security rules to control the use of IPSec.

What Are Profiles?



Key Points

A profile is a set of configuration options that specify the behavior of Windows Firewall when connected to a specific type of network. For each network type there is a profile.

Question: Why would you specify the type of data that is logged?

What Are Rules?

Inbound rules:

- Prevent incoming connections from other hosts
- Reduce the attack surface

Outbound rules:

- Prevent outgoing connections from this host
- Stop unauthorized software from communicating outside

Key Points

Windows Firewall in Windows Server 2008 has both inbound and outbound rules. These rules allow you to control network communication that is initiated by other hosts, or initiated by software on the local host.

Question: Why do outbound rules increase the administrative effort that is required to maintain servers?

What Are Rule Types?

Rule types include:

Rule type	Description
Program	Creates a rule for a specific executable file
Port	Creates a rule for a TCP or UDP ports
Predefined	Creates a rule for a well known Windows program or service
Custom	Creates a rule with options that are unavailable when creating other rule types

Key Points

To simplify the creation of rules in Windows Firewall, a wizard allows you to select a rule type during creation. This gives you access to the most commonly used options when creating rules of a specific type. After creation, you can edit a rule and have access to options that were not available in the wizard.

Question: What is the benefit of using a program rule instead of a port rule?

Rule Configuration Options

Rule configuration options include:

Configuration option	Description
Action	Used to allow, block, or secure a connection
Users and Computers	Limit connections to specific users or computers
Scope	Limits rule application to specific local and/or remote IP addresses
Profiles	Specifies to which profiles the rule applies
Interface types	Specifies to which interface types this rule applies
Edge Traversal	Specifies that Teredo should be used for traffic matching this rule to avoid NAT

Key Points

During the rule creation process, only specific options are presented to you. After creation, you can edit the rule and view all rule configuration options.

Question: How does the action specified for a rule relate to the profile settings for a network type?

What Are Connection Security Rules

Connection security rules define the authentication process for IPSec rules

Connection security rule type	Description
Isolation	Restricts connections based on criteria such as domain membership or health certificates
Authentication exemption	Designates a computer or IP addresses for which authentication is not required
Server-to-server	Restricts communication between two computers or groups of computers
Tunnel	Configures a secure tunnel between two computers that can be used by other computers
Custom	Allows rule configurations not available through other rule types

Key Points

Connection security rules define the authentication process for IPSec. These rules do not define whether data is secured or not. The security of data is defined in inbound and outbound rules. Connection security rules work with inbound and outbound rules to provide data security.

Question: Which type of connection security rule would you implement on a computer acting as a router for a secure connection to another location over the Internet?

Demonstration: Creating a Rule

In this demonstration, you will see how to create a rule

Key Points

Question: When creating a new rule on a member server, which profile should you assign?

Microsoft Security Use Prohibited

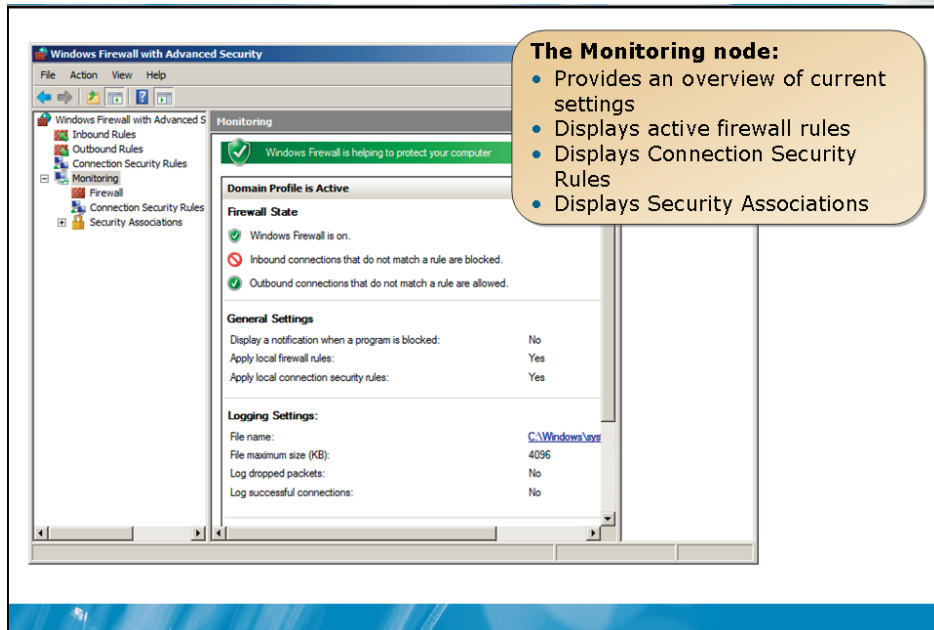
Lesson 4 Monitoring and Troubleshooting Windows Firewall

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is the Monitoring Node?
- Logging Options for Windows Firewall
- Restoring Windows Firewall Configuration Settings
- What Is the Windows Firewall Service?
- Troubleshooting Windows Firewall
- Demonstration: Monitoring Windows Firewall

Problems in network communication can occur when Windows Firewall is configured incorrectly. Problems are typically caused by a new rule having unexpected consequences. To help determine the cause of a problem in Windows Firewall, you can use the Monitoring node in Windows Firewall with Advanced Security or logging. If necessary, you can recover the configuration of Windows Firewall from a backup.

What Is the Monitoring Node?



Key Points

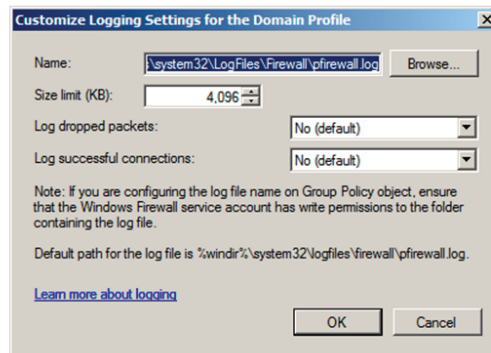
The Monitoring node of Windows Firewall with Advanced Security allows you to quickly review the current configuration of Windows Firewall.

Question: When is the Monitoring node useful?

Logging Options for Windows Firewall

Logging options include:

- File name and location
(%windir%\system32\logfiles\firewall\pfirewall.log)
- Size limit (4 MB default)
- Log dropped packets (default: no)
- Log successful connections (default: no)



Key Points

Windows Firewall includes the option to perform logging. The options you select for logging will depend on your goals for logging. If your goal is to monitor malicious activity on the network, then you can enable logging for dropped packets. If your goal is audit activity, you can also log successful connections. By default, no logging is performed.

Question: Why would you change the default location of the log file?

Restoring Windows Firewall Configuration Settings

Configuration setting options include:

Option	Description
Import Policy	Imports a saved Windows Firewall configuration from file
Export Policy	Exports the current Windows Firewall configuration to file
Restore Defaults	Resets the Windows Firewall configuration to default settings

Key Points

Windows Firewall includes option for restoring configuration settings. These are useful when performing troubleshooting.

Question: Why should you backup Windows Firewall settings before making changes?

What Is the Windows Firewall Service?

Windows Firewall Service:

- Is the service that controls Windows Firewall
- Must be running to protect the local computer
- Can be stopped and started if experiencing problems
- Must have write access to the location of log files

Key Points

The Windows Firewall service is the service that controls Windows Firewall. When the Windows Firewall service is stopped, then Windows Firewall is not functional. When Windows Firewall is enabled, the Windows Firewall service is configured to start automatically.

Question: When should you start and stop the Windows Firewall service manually?

Discussion: Troubleshooting Windows Firewall

What steps would you take to troubleshoot Windows Firewall?

Key Points

Answer the question in a classroom discussion.

MOCKUP ONLY. NOT FOR USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Demonstration: Monitoring Windows Firewall

In this demonstration, you will see how to monitor Windows Firewall

Question: Why should you increase the default size of the log file for Windows Firewall?

Lab: Using Windows Firewall

- Exercise 1: Limiting Access to a Web Application
- Exercise 2: Distributing Windows Firewall Rules by Using Group Policy

Logon information

Virtual machine	NYC-DC1, NYC-CL1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

Woodgrove bank has completed a review of security requirements and there are two recommendations that use Windows Firewall. The first recommendation is limiting access to a Web application to users with a specific range of authorized IP addresses. The second recommendation is to block Internet Explorer from accessing network resources on all domain controllers.

Exercise 1: Limiting Access to a Web Application

The recent security audit has recommended that access to a Web application be restricted to only IP addresses that are authorized. You must configure Windows Firewall to allow a specific range of IP address to communicate with the Web server. Connectivity for other services on the same server must not be affected

- ▶ Task 1: Verify connectivity to a Web application
 1. On NYC-CL1, log on as **Dana** with a password of **Pa\$\$w0rd**.
 2. Use Internet Explorer to verify that you can access <http://nyc-dc1.woodgrovebank.com>.
- ▶ Task 2: View the current client IP address
 - On NYC-CL1, use ipconfig to view the current IP address.
- ▶ Task 3: Configure Windows Firewall to limit access to the Web service
 1. On NYC-DC1, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Open the Windows Firewall with Advanced Security administrative tool.
 3. Edit the inbound rule World Wide Web Services (HTTP Traffic-In) to limit the scope to the IP address range 10.10.0.100 to 10.10.0.150.
 4. Edit the inbound rule World Wide Web Services (HTTPS Traffic-In) to limit the scope to the IP address range 10.10.0.100 to 10.10.0.150.
- ▶ Task 4: Verify rule functionality
 1. On NYC-CL1, use Internet Explorer to verify that you cannot access <http://nyc-dc1.woodgrovebank.com>.
 2. Open Network Sharing Center.
 3. View the detailed status of Local Area Connection. Note that the IP address is not in the allowed scope for the rules modified in the previous task.
 4. Open the Properties of Local Area Connection.
 5. Modify the IPv4 address to be 10.10.0.100.
 6. Use Internet Explorer to verify that you can access <http://nyc-dc1.woodgrovebank.com>

Exercise 2: Distributing Windows Firewall Rules by Using Group Policy

The recent security audit has recommended that all Web browser access on domain controllers should be blocked. To accomplish this you will create a rule the block network access for Internet Explorer. To simplify configuration of all domain controllers, you will distribute the Windows Firewall rule by using Group Policy.

- ▶ **Task 1: Create a new rule in a Group Policy**
 1. On NYC-DC1, open the Group Policy Management administrative tool.
 2. View the group policy objects that are linked to the Domain Controllers OU in the WoodgroveBank.com domain.
 3. Edit the Default Domain Controllers Policy.
 4. Browse to **Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Outbound Rules**.
 5. Create a new outbound rule named **Block Internet Explorer** that blocks the program %ProgramFiles%\Internet Explorer\iexplore.exe.

- ▶ **Task 2: Verify distribution of the new rule**
 1. On NYC-DC1, open a command prompt and run gpupdate.
 2. Open the Windows Firewall with Advanced Security administrative tool.
 3. View the active firewall rules in the Monitoring node.
 4. View the details of the Block Internet Explorer rule.

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Real-world Issues and Scenarios
- Best Practices

Review Questions

1. How is a reverse proxy server different from a proxy server?
2. Are Outbound Rules enabled or disabled by default?
3. How can Windows Firewall control network communication for an application regardless of the TCP or UDP port number that it is using?
4. Why would you use the Export Policy option in Windows Firewall with Advanced Security?

Real-world Issues and Scenarios

1. Your organization has chosen to implement Windows Firewall on all servers running Windows Server 2008. The implementation of infrastructure servers running as domain controllers and DNS servers has been completed without any problems. Application servers running applications designed for Windows Server 2008 are also functioning properly. However, after moving an older application to a computer running Windows Server 2008, the application is not working properly. What is the likely cause of the problem?

2. Your organization would like to increase the security of Web servers located in your perimeter network. You have determined that the best way to do this is to implement a reverse proxy server. Describe the configuration steps that are necessary to implement a reverse proxy server.
3. Your organization has hired a new security auditor. One of the tasks the security auditor is responsible for is monitoring Windows Firewall logs. However, the security auditor does not have administrative rights to the servers and is unable to read the firewall log in the default location. Describe the steps required to move the firewall log location and allow the security auditor access to the file.

Best Practices for Troubleshooting Windows Firewall

Supplement or modify the following best practices for your own work situations:

- Disable Windows Firewall to confirm that firewall rules are causing a problem
- Export the policy before making changes
- Test one change at a time
- Verify that required rules are active

Module 11

Remote Access Fundamentals

Contents:

Lesson 1: Remote Access Overview	11-3
Lesson 2: RADIUS Overview	11-8
Lesson 3: Network Policy Server	11-14
Lesson 4: Troubleshooting Remote Access	11-20
Lab: Implementing Remote Access	11-24

MCT USE ONLY
STUDENT USE PROHIBITED

Module Overview

- Remote Access Overview
- RADIUS Overview
- Network Policy Server
- Troubleshooting Remote Access

As workforces become more mobile, remote access to corporate resources becomes a more important part of network infrastructure. Users expect to be able to work from outside the office at anytime. Remote Authentication Dial In User Service (RADIUS) and Network Policy Server (NPS) provide part of the solution for authenticating remote users.

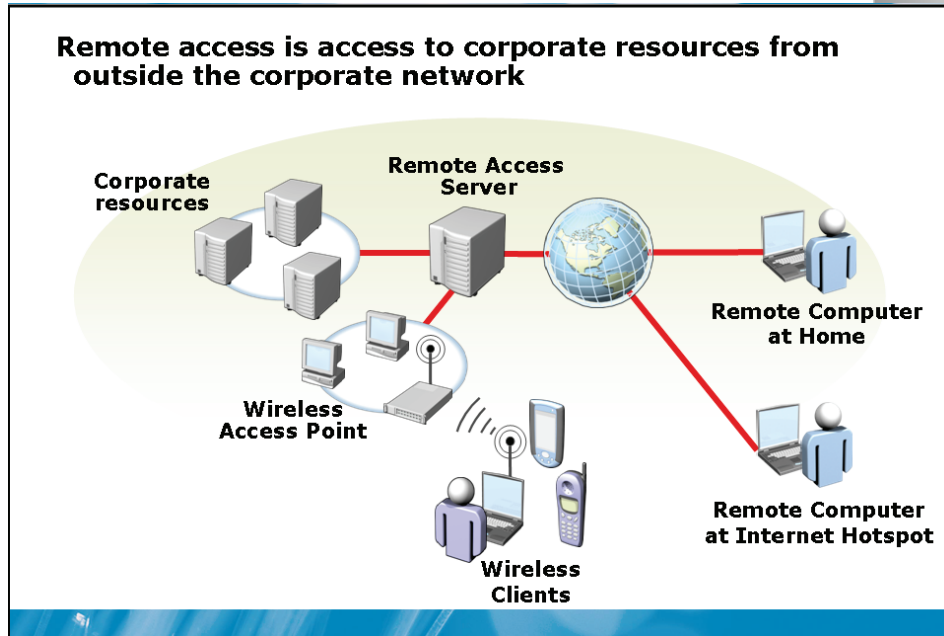
Lesson 1

Remote Access Overview

- What Is Remote Access?
- Discussion: Characteristics of VPN and Dial-up Connections
- VPN Protocols
- What Is RRAS?

Remote access can mean accessing data from a home, a hotel room, or a mobile device. From these locations, you may be using a virtual private network (VPN) or dial-up connection. When a VPN connection is used, you must select the appropriate protocol based on your needs. Windows Server 2008 includes Routing and Remote Access Service (RRAS) to act as a remote access server accepting dial-up and VPN connections.

What Is Remote Access?



Key Points

Remote access enables users to access corporate resources from outside the corporate network. Situations that may require remote access include:

- Staff working from home in the evenings
- Staff telecommuting
- Working from hotels during business trips
- Wireless clients for accessing data on road

Question: What are some examples of security concerns for data that is accessed remotely?

Discussion: Characteristics of VPN and Dial-up Connections

What are the characteristics of VPN and Dial-up connections?

Key Points

Answer the questions in a classroom discussion.

NT USE PROHIBITED

VPN Protocols

VPN connections can use various protocols to provide encryption

VPN Protocol	Description
Point-to-point tunneling protocol (PPTP)	<ul style="list-style-type: none">• Widely supported in clients• Traverses NAT easily• Easy to configure
Layer 2 tunneling protocol (L2TP)	<ul style="list-style-type: none">• Uses IPSec to encrypt data• Increased security over PPTP• More difficult to configure
Secure socket tunneling protocol (SSTP)	<ul style="list-style-type: none">• Uses SSL to encrypt data• Can pass through proxy servers on port 443• Easy to configure

Key Points

VPN connections can use various protocols to provide encryption. Each protocol requires different configuration and has different characteristics.

Question: Why is SSTP less likely to have problems traversing firewalls than other VPN protocols?

What Is RRAS?

Routing and Remote Access is a component that allows Windows Server 2008 to act as a router and/or remote access server

Router:

- Typically used on small networks
- Less expensive than hardware-based routers
- Network Address Translation (NAT) for Internet access

Remote Access server:

- VPN server
- Dial-up server
- Demand dial connection to secure connectivity between two locations

Key Points

Routing and Remote Access Server (RRAS) is a component that allows Windows Server 2008 to act as a router or remote access server. The remote access server functionality is more commonly used than the routing functionality.

NT USE PROHIBITED

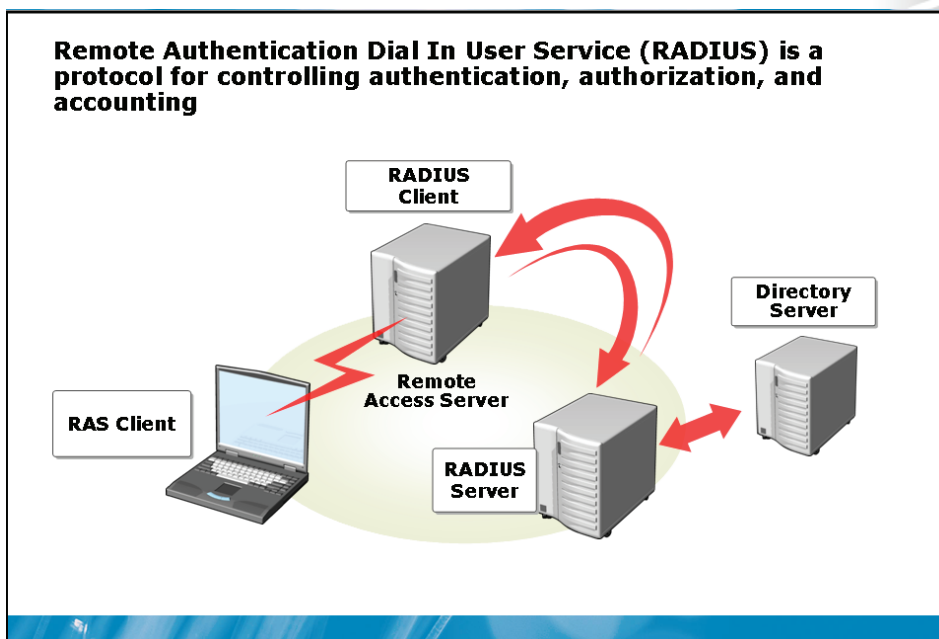
Lesson 2

RADIUS Overview

- What Is RADIUS?
- How RADIUS Works for Remote Access
- How RADIUS Works for 802.1X Connections
- Benefits of RADIUS
- What Is A RADIUS Proxy?

RADIUS is a standard protocol for authentication that is used on the Internet and corporate networks. RADIUS is used to authenticate remote access connections for users and network connections for network devices. In complex situations, a RADIUS proxy is used to direct authentication requests to the appropriate RADIUS server.

What Is RADIUS?



Key Points

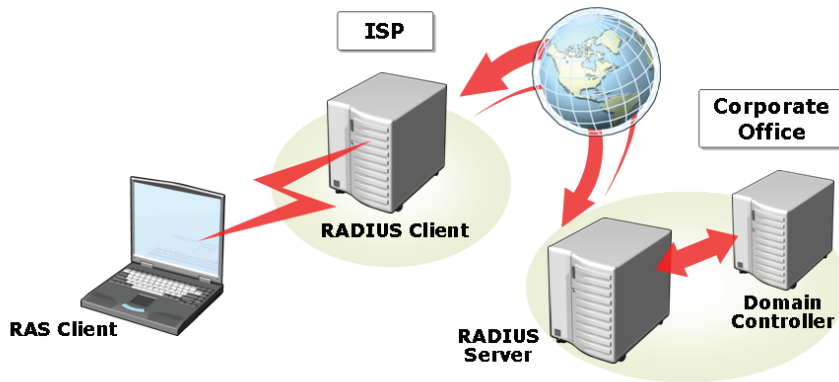
RADIUS is a protocol for controlling authentication, authorization, and accounting. RADIUS is an open standard defined by the Internet Engineering Task Force (IETF).

Question: Why is it beneficial to use an open standard such as RADIUS for remote authentication?

How RADIUS Works for Remote Access

For remote access, RADIUS:

- Allows an ISP to authenticate users against a corporate directory such as Active Directory
- Allows accounting for all remote access to centralized in a single location



Key Points

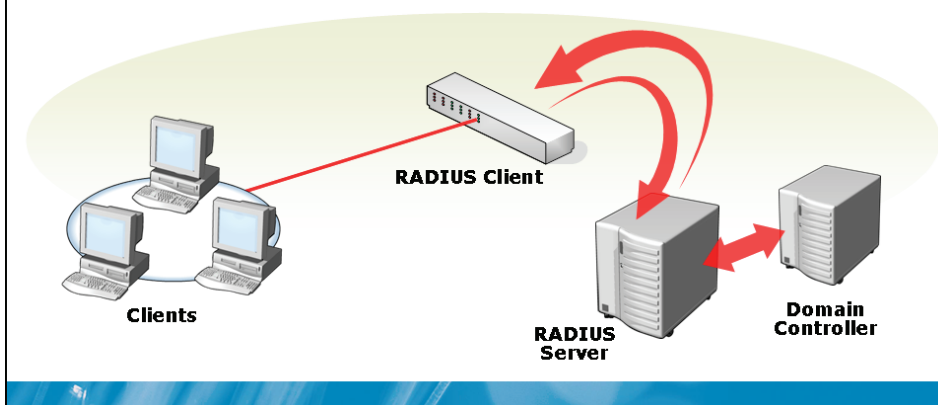
One common scenario for using RADIUS is dial-up authentication through an Internet Service Provider (ISP). When using RADIUS for authentication through an ISP, the RADIUS client is the dial-up server at the ISP. User credentials are sent over the Internet from the RADIUS client to the RADIUS server.

Question: Describe a scenario where 802.1X could prevent a network problem?

How RADIUS Works for 802.1X Connections

For 802.1X, RADIUS:

- Authenticates network connections
- Can be used for wired or wireless connections



Key Points

The 802.1X protocol is used to authenticate devices before they access the network. Implementing 802.1X increases network security by preventing unauthorized devices to access the network. This system can be less administration than controlling network access based on the MAC address of computers.

Question: What are the benefits of using RADIUS?

Discussion: Benefits of RADIUS

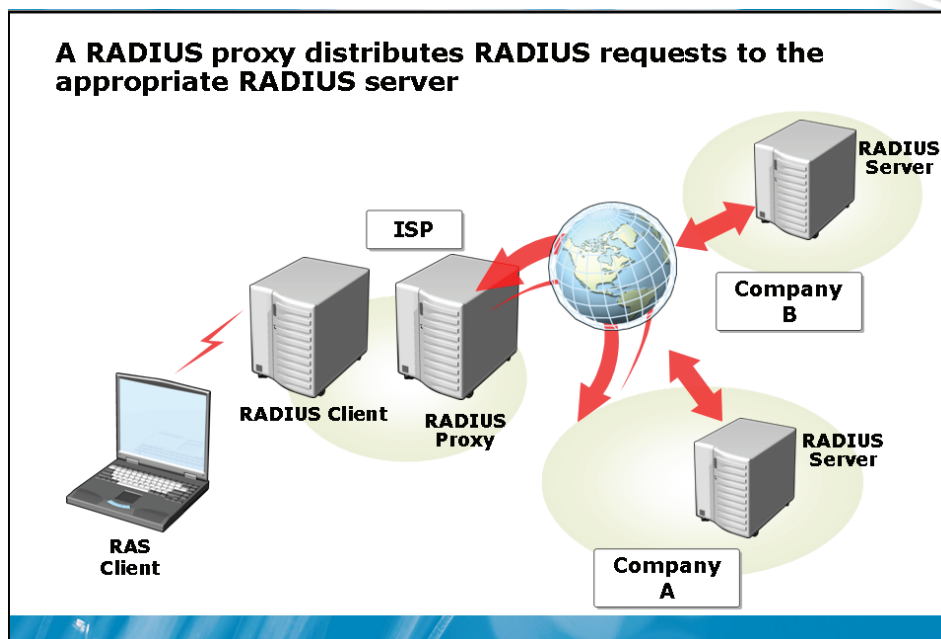
What are the benefits of using RADIUS?

Key Points

Answer the questions in a classroom discussion.

MCT USE ONLY. STUDENT USE PROHIBITED

What Is A RADIUS Proxy?



Key Points

A RADIUS proxy distributes RADIUS request to the appropriate RADIUS server. This is required when a RADIUS client authenticates connections for multiple RADIUS servers. In a typical configuration, a RADIUS client is configured to communicate with a single RADIUS server.

Question: Why is using a RADIUS proxy simpler than using a separate RADIUS client for each RADIUS server?

Lesson 3

Network Policy Server

- What Is Network Policy Server?
- What Is Network Access Protection?
- What Are Connection Request Policies?
- What Are Network Policies?
- Demonstration: Configuring NPS Policies

NPS is the Windows Server 2008 implementation of a RADIUS server and RADIUS proxy. NPS is also a Network Access Protection (NAP) server. When NPS evaluates RADIUS authentication requests, connection request policies are used to control processing. Provide a brief introduction to this lesson in normal text. A module must have at least two lessons.

MCT USE ONLY. STUDENT USE PROHIBITED

What Is Network Policy Server?

Network Policy Server is a role service that can function as a:

- RADIUS server
- RADIUS proxy
- Network Access Protection server

Network Policy Server replaces IAS from previous versions of Windows

Key Points

NPS is a role service in the Network Policy and Access Services role in Windows Server 2008.

Question: What component in Windows Server 2003 had similar functionality to NPS?

What Is Network Access Protection?

Network Access Protection is a system that:

- Enforces client health before allowing access to the network
- Does not block intruders or malicious users
- Has various enforcement mechanisms

Enforcement mechanisms include:

- IPSec
- 802.1X
- VPN
- DHCP
- RADIUS

Key Points

NAP is a system that enforces client health before allowing clients access to the network. Client health can be based on characteristics such as antivirus software status, Windows Firewall status, or the installation of security updates. The monitored characteristics are based on which system health agents are installed.

Question: Which NAP enforcement method would you use to ensure that remote access users have the most recent operating system updates installed?

What Are Connection Request Policies?

Are part of the RADIUS proxy functionality in NPS that:

- Determine whether authentication of connection requests is performed locally or passed to another RADIUS server.
- Contain conditions and settings
- Must be configured for NAP with 802.1X or VPN even when processed locally

Some potential conditions:

- User Name
- Client IPv4 address
- Service Type
- Client Vendor
- Tunnel Type
- Called Station ID
- Day and Time Restrictions

Key Points

Question: Why would you use settings in a connection request policy?

NT USE PROHIBITED

What Are Network Policies?

Network policies control remote access requests, replacing remote access policies in previous versions of Windows

Network Policy component	Description
Conditions	Determine whether this policy is used to evaluate a connection request
Access permission	Determine whether access is allowed, denied, or determined by user dial-in properties
Authentication methods	Determine the authentication methods that can be negotiated.
Constraints	Limits on the connection such as idle time or maximum connection time
Settings	Set characteristics of the connection such as encryption or IP filters

Key Points

Connection request policies are part of the RADIUS proxy functionality in NPS. The connection request policies are used by NPS to determine how authentication requests should be forwarded, or if they should be forwarded. The default connection request policy authenticates all requests locally. If you want NPS to act as a RADIUS proxy and forward some request to other RADIUS servers, then you must create additional connection request policies.

Question: How do network policies differ from network connection policies?

Demonstration: Configuring NPS Policies

In this demonstration, you will see how to configure:

- A connection request policy
- A network policy

Question: Are the options for conditions and settings in network policies the same as the options for conditions and settings in connection request policies?

NT USE PROHIBITED

Lesson 4

Troubleshooting Remote Access

- What Is NPS Accounting?
- Common Remote Access Issues
- Process for Troubleshooting Remote Access Issues

Remote access connections are often difficult to troubleshoot because there are so many unknown elements when users are connecting from a remote location or public computer. However, NPS accounting can help by providing centralized logs for analysis. Also, there are some common remote access issues that you can evaluate as part of the troubleshooting process.

What Is NPS Accounting?

NPS Accounting is an administration tool that:

- Is used for logging
- Applies only to locally authenticated connections
- Can be used for connection analysis and billing
- Can be used for security investigation
- Can store data in a file or SQL Database

Key Points

The Accounting node in the Network Policy Server administrative tool is used to configure authentication and accounting logging. This information is useful for security investigations, such as a security breach, or for generating billing information.

Question: In what situation would you not enable the **When disk is full delete older log files** option?

Common Remote Access Issues

Some common remote access issues are:

- Client configuration
- Firewall configuration
- Network Policy configuration

Key Points

Some of the most common issues that occur for remote access involve client, firewall, or network policy configurations.

Discussion: Process for Troubleshooting Remote Access Issues

What are some methods used to troubleshoot remote access issues?

Key Points

Answer the questions in a classroom discussion.

M

USE PROHIBITED

Lab: Implementing Remote Access

- Exercise 1: Implementing a VPN server
- Exercise 2: Implementing a RADIUS server
- Exercise 3: Implementing a RADIUS proxy

Logon information

Virtual machine	NYC-DC1, NYC-RAS NYC-CL1
User name	Administrator
Password	Pa\$\$wOrd

Estimated time: 60 minutes

Scenario

You are the remote access administrator for Woodgrove Bank. The bank does not currently have a remote access infrastructure and will build a new infrastructure using Windows Server 2008.

Exercise 1: Implementing Remote Access

The initial remote access implementation for Woodgrove Bank will have only a single VPN server in the head office. You want to control access to the VPN with a new global security group named NYC_VPNUsers. Members of this group will be granted access to use the VPN. Encryption will be required.

- ▶ Task 1: Configure RRAS as a VPN server
 1. On NYC-RAS, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Use the Routing and Remote Access administrative tool to enable routing and remote access:
 - Configuration: **Remote access (dial-up or VPN)**
 - Remote access: **VPN**
 - Network interface: Local Area Connection, do not enable security on the selected interface
 - IP Address Assignment: From a specified range of addresses,
 - Start IP address: **10.11.0.180**
 - End IP address: **10.11.0.199**
 - Use Routing and Remote Access to authenticate connection requests

- ▶ Task 2: Create a group for VPN users
 1. On NYC-DC1, log on as **Administrator** with a password or **Pa\$\$w0rd**.
 2. Use Active Directory Users and Computer to create a new NYC_VPNUsers global security group in the NYC OU.
 3. Add Dana Birkby as a member of the NYC_VPNUsers group.

- ▶ Task 3: Configure network policies
 1. On NYC-RAS, use the Network Policy Service administrative tool to create a new network policy:
 - Name: **VPN Users**
 - Type of network access server: Remote Access Server (VPN-Dial up)
 - Conditions:
 - Member of NYC_VPNUsers group in WoodgroveBank.com domain
 - Access Permission: Granted

- Authentication Methods: default
 - Constraints:
 - NAS Port Type: Virtual (VPN)
 - Encryption: Must be encrypted
2. Ensure that the VPN Users policy is evaluated first.
- ▶ Task 4: Create the VPN connection.
1. On NYC-CL1, log on as **Dana** with a password or **Pa\$\$w0rd**.
 2. Create a new connection in Network and Sharing Center:
 - Connect to a workplace
 - Use my Internet connection (VPN)
 - Configure the Internet connection later
 - Internet address: **NYC-RAS.woodgrovebank.com**
 - Destination name: Woodgrove Bank VPN
 - Leave user name and password blank
- ▶ Task 5: Test the VPN connection
1. On NYC-CL1, use the Connect To option in the Start menu to connect the Woodgrove Bank VPN connection.
 2. Log on as Axel with a password of Pa\$\$w0rd.

This is unsuccessful because Axel is not a member of the VPN Users group.

3. Attempt to log on using the Woodgrove Bank VPN connection again.
4. Log on as Dana with a password of **Pa\$\$w0rd**.

This is successful because Dana is a member of the VPN Users group.

5. Use the Connect To option in the Start menu to view the status of the Woodgrove Bank VPN connection.
6. View the IP address delivered for the VPN connection.
7. Disconnect the Woodgrove Bank VPN connection.

Exercise 2: Implementing a RADIUS server

The implementation of remote access for head office users has been very successful. Because of the success, additional VPN servers will be implemented. To simplify the maintenance of network policies, you are implementing a RADIUS server that will serve as a central point to perform all authentication.

- ▶ Task 1: Install NPS
 - On NYC-RAS, use Server Manager to install the Network Policy and Access Services server role:
 - Service role: Network Policy Server
- ▶ Task 2: Configure security on the RADIUS server
 - On NYC-DC1, use Network Policy Server to configure a new RADIUS client:
 - Friendly name: **NYC-RAS**
 - Address: **10.10.0.1**
 - Shared secret: **Pa\$\$w0rd**
- ▶ Task 3: Configure RRAS as a RADIUS client
 1. On NYC-RAS, use Routing and Remote Access to view the Security tab in the Properties of NYC-RAS.
 2. Configure NYC-RAS to use RADIUS authentication.
 3. Add a RADIUS server:
 - Server name: **10.10.0.10**
 - Shared secret: **Pa\$\$w0rd**
 4. Restart Routing and Remote Access.

- ▶ Task 4: Test the VPN connection
 1. On NYC-CL1, log on as Dana with a password of **Pa\$\$w0rd**.
 2. Use the Connect To option in the Start menu to connect the Woodgrove Bank VPN connection.
 3. Log on as Dana with a password of **Pa\$\$w0rd**.

This is not successful because no network policies have been created on the RADIUS server.

- ▶ Task 5: Configure a network policy on NYC-DC1
 1. On NYC-DC1, use the Network Policy Service administrative tool to create a new network policy:
 - Name: **RADIUS VPN Users**
 - Type of network access server: Remote Access Server (VPN-Dial up)
 - Conditions:
 - Member of NYC_VPNUsers group in woodgrovebank.com domain
 - Access Permission: Granted
 - Authentication Methods: default
 - Constraints:
 - Disconnect after maximum idle time : 30 minutes
 - NAS Port Type: Virtual (VPN)
 - Encryption: Must be encrypted
 2. Ensure that the RADIUS VPN Users policy is evaluated first.

- ▶ Task 6: Verify the network policy is working
 1. On NYC-CL1, use the Connect To option in the Start menu to connect the Woodgrove Bank VPN connection.
 2. Log on as Dana with a password of Pa\$\$w0rd.

This is now successful because a network policy has been configured.

3. Disconnect the Woodgrove Bank VPN connection.
- ▶ Task 7: View authentication events for the VPN connection
 1. On NYC-DC1, use Event Viewer to filter the security log and view Network Policy Server Events:
 - Event log: Security
 - Event sources: Microsoft Windows security auditing
 - Task category: Network Policy Server
 2. Read the most recent few events to view information about the VPN connection from NYC-CL1.

Exercise 3: Implementing a RADIUS proxy

Woodgrove bank has a large technology research area that operates independently within the bank. To allow the technology research area remote access, you are configuring a network connection policy that forwards authentication request for the technology research area users to their own RADIUS server. All users in the technology research area will append “R-“ to their logon name to identify themselves to the RADIUS proxy.

- ▶ Task 1: View the default network connection policy
 - On NYC-DC1, use the Network Policy Server administrative tool to view the default connection request policy.

- ▶ Task 2: Create a new remote RADIUS server group
 1. On NYC-DC1, use the Network Policy Server administrative tool to create a new RADIUS server group:
 - Name: **Research**
 - Server: **research.woodgrovebank.com**
 - Shared secret: **Pa\$\$w0rd**

- ▶ Task 3: Create a new connection request policy
 1. On NYC-DC1, use the Network Policy Server administrative tool to create a new connection request policy:
 - Name: **Research Proxy**
 - Type of network access server: Remote Access Server (VPN-Dial up)
 - Conditions:
 - User name: R-*
 - Forward requests to the Research remote RADIUS server group
 - Configure Settings:
 - Attribute: User-name, replace R- with blank
 2. Move Research Proxy to be the first policy evaluated.

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools

Review Questions

1. Which VPN protocol uses IPSec for encryption?
2. What type of devices or servers can be RADIUS clients?
3. Which RADIUS roles does NPS perform?
4. Which logging location supports multiple NPS servers writing information to the same location?

Real-world Issues and Scenarios

1. Your organization is implementing RRAS as a VPN server. All remote client computers that will be connecting to the VPN server will be running Windows Vista. To minimize problems with firewalls, which VPN protocol should you use?
2. Your organization would like to use RRAS to secure communication between two locations over the Internet. However, there are concerns about how the connection will be started after the RRAS server in either location is rebooted. Which feature in RRAS can be used to reconnect the VPN between two locations?
3. There has recently been a problem in your organization with an unauthorized computer being connected to the corporate network. A consultant came in and connected a laptop infected with a virus to the network. There was no protection in place on the network and the virus attempted to spread to computers on your network. Fortunately the anti-virus software on your network computers was up to date and the virus was unsuccessful in replicating itself. Which features in Windows Server 2008 can prevent this from happening again?
4. Your organization is implementing Windows Server 2008 as a RADIUS server. There is some confusion among the staff as to the relationship between network policies and network connection policies. Explain the difference between the network policies and network connection policies.

Tools

Tool	Use for	Where to find it
Routing and Remote Access	<ul style="list-style-type: none"> • Configuring Routing and Remote Access as a router, VPN server, dial-up server, or RADIUS client. 	Administrative Tools Computer Management
Network Policy Server	<ul style="list-style-type: none"> • Configure network policies for remote access • Configure network connection policies for a RADIUS proxy 	Administrative Tools

Module 12

Routing Fundamentals

Contents:

Lesson 1: Routing Overview	12-3
Lesson 2: Configuring RRAS as a Router	12-8
Lesson 3: Quality of Service	12-14
Lab: Configuring Routing	12-20

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Routing Overview
- Configuring RRAS as a Router
- Quality of Service

Routing processes control how packets are moved from one host to another in a network. The Routing and Remote Access service (RRAS) can be used to configure Windows Server 2008 as a router. Quality of Service (QoS) can be used to ensure the certain types of network traffic receive higher priority when being routed.

Lesson 1

Routing Overview

- What Are Static and Dynamic Routing?
- How the IP Protocol Selects a Route
- Demonstration: Viewing a Routing Table
- Troubleshooting Routing

Routing tables are lists of networks. The maintenance of routing tables can be either static or dynamic. Hosts and routers use routing tables to determine how a packet is delivered.

What Are Static and Dynamic Routing?

Statically configured routers:

- Do not automatically discover the IDs of remote networks
- Do not exchange information with other routers
- Are not fault tolerant

Dynamically configured routers:

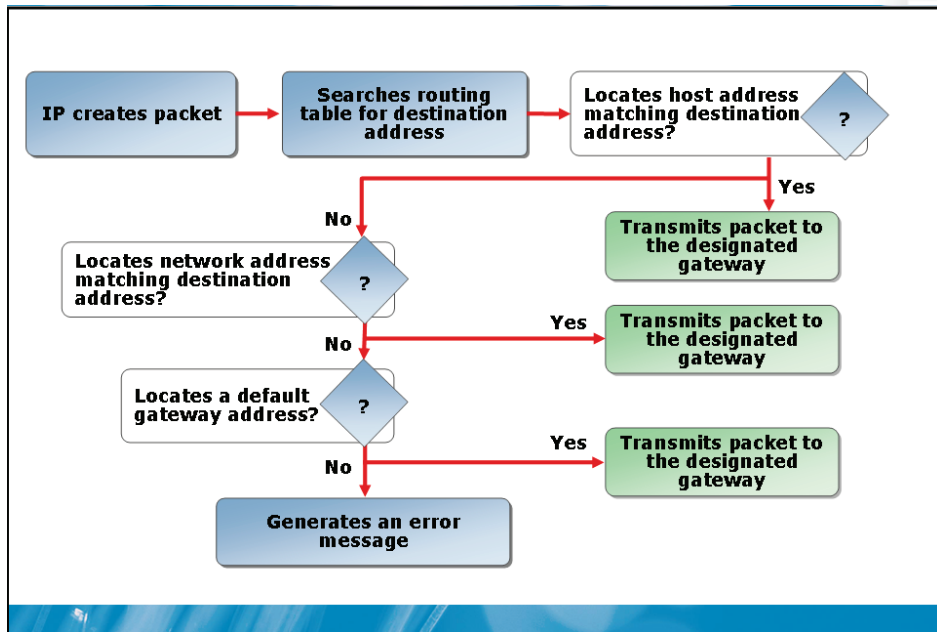
- Discover the IDs of remote networks automatically
- Use a routing protocol to exchange information with other routers
- Can be fault tolerant

Key Points

Hosts and routers maintain a list of network IDs and how to deliver packets to those networks. This list of network IDs is a routing table. Depending on the priorities of your organization, the routing table can be updated dynamically or manually.

Question: Why would you use static routing instead of dynamic routing?

How the IP Protocol Selects a Route



Key Points

To send data packets from one Internet protocol (IP) network to another, IP must select the appropriate path. When a router receives a packet, the network interface adapter passes the packet to IP. IP examines the destination address and compares it to a routing table. A routing table is a series of entries, called routes, which contain information about the location of the network IDs for the internetwork. IP then makes a decision as to how to forward the packet.

Question: Is the routing process used for IPv4 the same for IPv6?

NT USE PROHIBITED

Demonstration: Viewing a Routing Table

In this demonstration, you will see how to view a routing table

Question: Which route in the routing table represents the default gateway?

Discussion: Troubleshooting Routing

What are some tools that can be used to troubleshoot routing?

Key Points

Answer the questions in a classroom discussion.

CONTENT USE PROHIBITED

Lesson 2

Configuring RRAS as a Router

MCT USE ONLY. STUDENT USE PROHIBITED

- RRAS Routing Roles
- Routing Protocols
- Configuration Options for an Interface
- Information Available for an Interface
- Demonstration: Configuring RRAS as a LAN Router

The Routing and Remote Access administrative tool can be used to configure RRAS as a LAN router, demand-dial router, or network address translation (NAT). Depending on which role you select, various routing protocols can be configured. The Routing and Remote Access administrative tool allows you to configure routing characteristics of network interfaces and view statistics for network interfaces.

RRAS Routing Roles

Routing roles include:

Routing role	Description
LAN router	Can route IPv4 and IPv6 packets between network segments
Demand-dial	Automatically create a connection to a remote location by using dial-up networking or a VPN connection
NAT	Perform NAT and allow computers to access the Internet by sharing a single Internet addressable IPv4 address

Key Points

When RRAS is configured as a router, you can use it for LAN routing, demand-dial routing, and NAT.

Question: Why is a demand-dial connection required to configure a VPN connection over the Internet between two offices?

Routing Protocols

Routing protocols include:

Routing Protocol	Description
DHCP Relay Agent	Allows a RRAS server to relay DHCP requests to a DHCP server on a remote network.
IGMP Router Proxy	Allows a RRAS server to act as an IGMP router or proxy for multicast traffic
NAT	Allows a RRAS server to act as a NAT router to share a single IPv4 address.
RIP Version 2 for Internet Protocol	Allows a RRAS router to perform dynamic routing with other RIP routers.
DHCPv6 Relay Agent	Allows a RRAS server to relay DHCP request to a DHCPv6 server on a remote network.

Key Points

Routing protocols are rules for how routers can manipulate packets.

Question: When should you implement RIP Version 2 Internet Protocol on RRAS?

Configuration Options for an Interface

Interface configuration options include:

Configuration Option	Description
IP Router Manager	Enables or disables TCP/IP for the Interface
Router Discovery Advertisements	Clients use router discovery advertisements to dynamically discover default gateways
Inbound/Outbound filters	Filters similar to Windows Firewall
Fragmentation checking	Specifies whether filtering is performed on packet fragments
Multicast boundaries	Configures time to live for multicast traffic
Multicast heartbeat detection	Used to confirm that multicast infrastructure is functioning properly

Key Points

In the Routing and Remote Access administrative tool, there are a number of routing related settings that can be configured for each network interface.

Question: Why is the use of Inbound/Outbound filters not recommended?

CONTENT USE PROHIBITED

Information Available for an Interface

Available interface information includes:

Interface information	Description
TCP/IP Information	Statistics such as number of packets sent and received
Address Translations	Translations from IP address to physical address
IP Addresses	IP addresses that are bound to this computer
IP Routing Table	Host and network routes in the routing table of this computer
TCP connections	Active connections and listening TCP ports
UDP listener ports	A list of UDP ports listening to accept UDP packets

Key Points

The Routing and Remote Access administrative tool allows you to view a variety of statistics for each network interface and the general computer. Interface specific information is shown under the IPv4 and IPv6 nodes in the General node.

Question: Why would you view the computer summary information in the Routing and Remote Access administrative tool rather than using command-line tools such as Netstat?

Demonstration: Configuring RRAS as a LAN Router

In this demonstration, you will see how to configure RRAS as a LAN router

Question: Which option must be selected to configure RRAS as a LAN router?

CONTENT USE PROHIBITED

Lesson 3

Quality of Service

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is Quality of Service?
- Architecture of Policy-based QoS
- What Is a QoS Policy?
- Demonstration: Creating a QoS Policy

Quality of Service (QoS) is used to ensure that certain types of data packets have priority on the network. Windows uses QoS policies to delivery QoS configuration information to workstations and servers.

What Is Quality of Service?

Quality of Service (QoS):

- Prioritizes network traffic for network routing by adding a DSCP value
- Uses throttling to limit bandwidth usage on a host

Can be based on:

- Sending application
- Source or destination IPv4 or IPv6 addresses
- Protocol (TCP or UDP)
- Source or destination ports

Key Points

QoS for network communication is used to give specific network packets higher priority for delivery through the network than other packets. As each packet is created on the workstation or server, a Differentiated Services Code Point (DSCP) is embedded in the header of the packet. The DSCP value is read by routers during delivery and the packet is given priority by routers based on the DSCP value.

Question: Are there any specific requirements for routers to support QoS?

What Is a QoS Policy?

A QoS policy:

- Is defined as part of a group policy
- Can be applied to users or computers
- Can include specific IPv4 or IPv6 addresses or networks to apply to
- Allows you to define a DSCP value for network traffic
- Allows you to define a throttle rate for network traffic

Key Points

A QoS policy is how QoS settings are applied to Windows servers and workstations. The QoS policy is part of a group policy object. You cannot edit a QoS policy directly in the local security policy, it must be delivered by Group Policy. Within the QoS policy, you can define the DSCP value for specific network packets or a throttle rate.

Question: Why is applying QoS policies based on IP addresses not accurate in an environment that uses DHCP?

Discussion: QoS Scenarios

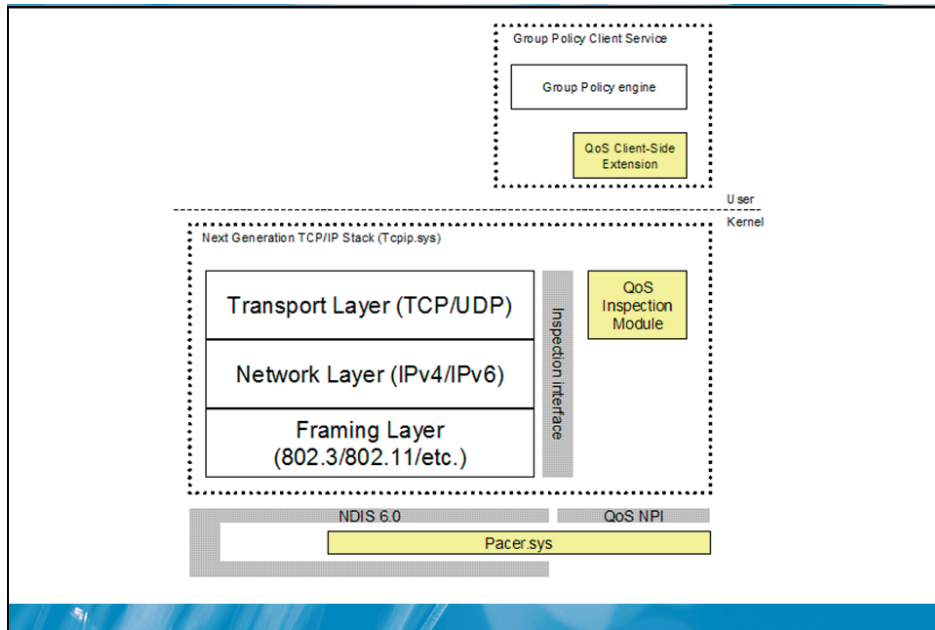
What are some scenarios where DSCP values and bandwidth throttling can be used?

Key Points

Answer the questions in a classroom discussion.

CONTENT USE PROHIBITED

Architecture of Policy-based QoS



Key Points

The implementation of QoS in Windows Server 2008 and Windows Vista uses the following components: QoS Client-Side Extension, QoS Inspection Module, and Pacer.sys.

Question: Why is it necessary for the network layer to obtain header information from Pacer.sys?

Demonstration: Creating a QoS Policy

In this demonstration, you will see how to create a QoS Policy

Question: Is it possible to create a QoS policy locally on a computer?

CONTENT USE PROHIBITED

Lab: Configuring Routing

MCT USE ONLY. STUDENT USE PROHIBITED

- Exercise 1: Configuring a LAN Router
- Exercise 2: Implementing RIPv2
- Exercise 3: Configuring a Demand-dial Router
- Exercise 4: Configuring QoS

Logon information

Virtual machine	NYC-DC1, NYC-RAS, NYC-SVR1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

You are the administrator responsible for network routing at Woodgrove bank. Most routing in the organization is performed by dedicated hardware routers because of the high performance requirements. However, you have decided to use Windows Server 2008 in some lower capacity situations, such as routing to small branch offices.

Exercise 1: Configuring a LAN Router

Woodgrove bank is adding a new remote office for administrative staff. It has been determined that using Windows Server 2008 as a router will be suitable for this location. The head office network is 10.10.0.0. The WAN link is 10.11.0.0 and the network for the remote office is 10.12.0.0. The server NYC-RAS is being configured as a router between the head office network and the WAN link.

- ▶ Task 1: Configure default gateway on NYC-DC1
 1. On NYC-DC1, use Server Manager to view connections.
 2. Open the status of Local Area Connection.
 3. Verify the IPv4 default gateway of Local Area Connection to be 10.10.0.1.
- ▶ Task 2: View IPv4 configuration on NYC-RAS
 1. On NYC-RAS, use Server Manager to view IP addresses under Computer Information.
 2. Verify the IPv4 address of Local Area Connection to be 10.10.0.1.
 2. Verify the IPv4 address of Local Area Connection 2 to be 10.11.0.1.
- ▶ Task 3: Configure IPv4 on NYC-SVR1
 1. On NYC-SVR1, use Server Manager to view connections.
 2. Open the properties of Local Area Connection.
 3. Configure Local Area Connection with the following settings:
 - IP address: **10.11.0.24**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **10.11.0.1**
 4. Open the properties of Local Area Connection 2.
 5. Configure Local Area Connection 2 with the following settings:
 - IP address: **10.12.0.24**
 - Subnet mask: **255.255.0.0**
- ▶ Task 4: Configure NYC-RAS as a router
 1. On NYC-RAS, use Server Manager to add the Network Policy and Access Service role.
 - Service role: Routing
 2. In the Routing and Remote Access administrative tool, use a custom configuration to enable Routing and Remote Access as a LAN router.

- ▶ Task 5: View the routing table on NYC-RAS
 1. On NYC-RAS in the Routing and Remote Access administrative tool, view the IP routing table from the Static Routes node.
 2. View the routing table from a command prompt by using the following command:
 - **Route print -4**
- ▶ Task 6: Test routing on NYC-RAS
 1. Open a command prompt.
 2. Test connectivity to the default gateway with the following command:
 - **Ping 10.10.0.1**
 3. Test connectivity through the router with the following command:
 - **Ping 10.11.0.24**
 4. Verify the path through the network with the following command:
 - **Tracert 10.11.0.24**

Exercise 2: Implementing RIPv2

The newly configured Windows Server 2008 routing is working well, but requires static routes to be added whenever routing changes are made. To simplify routing administration, you are implementing RIP version 2 on your routers.

- ▶ Task 1: Configure NYC-SRV1 as a LAN router
 1. On NYC-SRV1, use Server Manager to add the Network Policy and Access Service role.
 - Service role: Routing
 2. In the Routing and Remote Access administrative tool, use a custom configuration to enable Routing and Remote Access as a LAN router.

- ▶ Task 2: Test routing to the 10.12.0.0 network
 1. On NYC-RAS, view the routing table at a command prompt by using the following command:
 - **Route print -4**
 2. Verify that the 10.12.0.0 network is not listed in the routing table on NYC-RAS.
 3. On NYC-DC1, test connectivity at a command prompt with the following command:
 - **Ping 10.12.0.24**

This is not successful because the NYC-RAS does not have the necessary routing in its routing table.

- ▶ Task 3: Install RIPv2 on NYC-SRV1
 1. On NYC-SRV1, use the Routing and Remote Access administrative tool to add RIP Version 2 for Internet Protocol from the General node.
 2. Add Local Area Connection as a RIP interface.
 3. Add Local Area Connection 2 as a RIP interface.
- ▶ Task 4: Install RIPv2 on NYC-RAS
 1. On NYC-RAS, use the Routing and Remote Access administrative tool to add RIP Version 2 for Internet Protocol from the General node.
 2. Add Local Area Connection as a RIP interface.
 3. Add Local Area Connection 2 as a RIP interface.
- ▶ Task 5: Verify RIP functionality
 1. On NYC-RAS, use the Routing and Remote Access administrative tool to view RIP statistics by selecting the RIP node.
 2. Verify that the Local Area Connection 2 Interface is showing both Responses sent and Responses received.

3. Use the Static Routes node to view the IP Routing Table.
4. Verify that the network 10.12.0.0 is listed in the routing table.
5. On NYC-DC1, at a command prompt use the following command to test connectivity:
 - **Ping 10.12.0.24**

Exercise 3: Configuring a Demand-dial Router

Woodgrove bank has added a new small office. You have decided to use a demand-dial connection between the two offices to avoid the cost of a leased line. The demand-dial connection will be a VPN over the Internet.

- ▶ Task 1: Configure a demand-dial connection on NYC-RAS
 1. On NYC-RAS, use the Routing and Remote Access administrative tool to disable Routing and Remote Access.
 2. Use the Routing and Remote Access administrative tool to enable a secure connection between two private networks with the following settings:
 - Demand-dial connection
 - Specified range of IP addresses: 10.10.0.200 – 10.10.0.219
 3. In the Demand-Dial Interface Wizard:
 - Name: **Remote Router**
 - Connect using virtual private networking (VPN)
 - Type: Point to Point Tunneling Protocol (PPTP)
 - Destination server IP address: **10.11.0.24**
 - Route IP packets on this interface
 - Add a user account so a remote router can dial in

- Static Route
 - Destination: **10.12.0.0**
 - Network mask: **255.255.0.0**
 - Metric: **1**
 - Dial-In Credentials:
 - Password: **Pa\$\$w0rd**
 - Dial-Out Credentials:
 - User name: **Remote Router**
 - Domain: **NYC-SVR1**
 - Password: **Pa\$\$w0rd**
- Task 2: Configure a demand-dial connection on NYC-SVR1
1. On NYC-SVR1, use the Routing and Remote Access administrative tool to disable Routing and Remote Access.
 2. Use the Routing and Remote Access administrative tool to enable a secure connection between two private networks with the following settings:
 - Demand-dial connection
 - Specified range of IP addresses: 10.12.0.200 – 10.12.0.219
 3. In the Demand-Dial Interface Wizard:
 - Name: Remote Router
 - Connect using virtual private networking (VPN)
 - Type: Point to Point Tunneling Protocol (PPTP)
 - Destination server IP address: **10.11.0.1**
 - Route IP packets on this interface
 - Add a user account so a remote router can dial in

- Static Route:
 - Destination: **10.10.0.0**
 - Network mask: **255.255.0.0**
 - Metric: **1**
- Dial-In Credentials:
 - Password: **Pa\$\$w0rd**
- Dial-Out Credentials:
 - User name: **Remote Router**
 - Password: **Pa\$\$w0rd**

► Task 3: Configure static routes

1. On NYC-RAS in the Routing and Remote Access administrative tool, add a new static route.
 - Interface: **Remote Router**
 - Destination: **10.12.0.0**
 - Network mask: **255.255.0.0**
 - Metric: **1**
2. On NYC-SVR1 in the Routing and Remote Access administrative tool, add a new static route.
 - Interface: **Remote Router**
 - Destination: **10.10.0.0**
 - Network mask: **255.255.0.0**
 - Metric: **1**

- ▶ Task 4: Test the demand-dial connection
 1. On NYC-RAS in the Routing and Remote Access administrative tool, use the Static Routes node to verify that there is a static route to the network 10.12.0.0.
 2. On NYC-DC1, test connectivity at a command prompt by using the following command:
 - **Ping 10.12.0.24**
 3. On NYC-RAS in the Routing and Remote Access administrative tool, use the Network Interfaces node to verify that the Remote Router demand-dial connection is connected.

Exercise 4: Configuring QoS

Woodgrove bank has implemented a new VoIP application on user computers. The packets generated by this application need to have higher priority on the network to ensure voice quality when communicating with customers. You are implementing a QoS policy to give the VoIP application higher priority on the network.

- ▶ Task 1: Create a new group policy for the domain
 1. On NYC-DC1, use the Group Policy Management administrative tool to create a new GPO in the WoodgroveBank.com domain and link it there.
 - Name: **QoS**
 2. Edit the QoS GPO and create a new QoS policy under Computer Configuration > Windows Settings > Policy-based QoS,
 - Policy name: **VoIP**
 - DSCP value: **50**
 - Application name: **%ProgramFiles%\VoIP\VoIP.exe**
 - Source IP address: **Any**
 - Destination IP address: **Any**
 - Protocol: **TCP and UDP**

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Common Issues and Troubleshooting Tips
- Real-world Issues and Scenarios
- Tools

Review Questions

1. When multiple routes in a routing table match the destination network, how is the route selected?
2. Which routing protocol is used by Windows Server 2008 LAN routers to perform dynamic routing?
3. What is added to the header of a packet to support QoS?

Common Issues related to Troubleshooting Routing

- When the default gateway is configured incorrectly on a computer, the computer will be able to communicate on the local network, but not other networks.
- When the subnet mask is configured incorrectly on a computer, the computer may not be able to communicate with all computers on the local network.

- Many routers and firewalls drop the ICMP packets that are used by Ping and Tracert. No -response to Ping does not always indicate that the host is down. However, response to ping always indicates that a host is up.
- Network troubleshooting tools such as Ping cannot verify the functionality of applications on a host.

Real-world Issues and Scenarios

1. You have recently been hired to administer one location in the network of a mid-size organization. The network has three locations with five subnets in each. The routers are configured manually. In the past, there have been issues with network changes not being properly entered in the routing table in all locations. This resulted in downtime for some users and a significant cost for the organization. What can you do to reduce the chances of incorrect information being entered in the routing tables?
2. Your organization has recently added a new location. To provide secure communications to the new location, you are using a demand-dial connection to create a VPN connection between the two locations. You are able to manually start the VPN connection between the two locations, but it is not starting automatically, even when there are packets that need to be delivered to the remote location. What additional routing configuration is required?
3. Your organization wants to implement QoS on the network to support a new VoIP application that runs on Windows Vista. However, the VoIP application randomly selects port numbers when initiating a call. How can you create a QoS policy that ensures the VoIP traffic has sufficient priority on the network?

Tools

Tool	Use for	Where to find it
Routing and Remote Access	<ul style="list-style-type: none">Configuring Routing and Remote Access as a router, VPN server, dial-up server, or RADIUS client.	Administrative Tools Computer Management
Route	<ul style="list-style-type: none">Views and modifies the routing table	Command prompt
Ping	<ul style="list-style-type: none">Verifying host availability and reachability	Command prompt
Tracert	<ul style="list-style-type: none">Use to verify router status on a network path	Command prompt
Pathping	<ul style="list-style-type: none">Use to verify router status on a network path	Command prompt
Group Policy Management Console	<ul style="list-style-type: none">Edit group policy objectsCreate QoS policies	Administrative Tools

Module 13

Network Load Balancing Fundamentals

Contents:

Lesson 1: Server Availability and Scalability Overview	13-3
Lesson 2: Windows Network Load Balancing	13-9
Lesson 3: Configuring Windows Network Load Balancing	13-14
Lab: Implementing Network Load Balancing	13-21

Module Overview

- Server Availability and Scalability Overview
- Windows Network Load Balancing
- Configuring Windows Network Load Balancing

Network load balancing is a system that enhances the availability and scalability of applications. Window Network Load Balancing is a load balancing solution that is included as part of Windows Server 2008.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 1

Server Availability and Scalability Overview

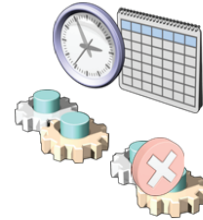
- What Is Availability?
- What Is Scalability?
- What Is Load Balancing?
- Comparing Hardware and Software Load Balancing
- What Is Clustering?

Server availability is a concern for all organizations. And, as organizations grow, scalability can also be a concern. Load balancing is a solution that provides both availability and scalability. You can implement load balancing as a hardware- or software- based solution depending on your needs. You can also use clustering to enhance availability for some applications that are not suitable for load balancing.

What Is Availability?

Availability is a level of service that applications, services, or systems provide, expressed as a percentage of time

Highly available services or systems are available more than 99% of the time



High availability:

- Requirements differ based on how availability is measured
- Does not typically include planned outages when calculating availability

Key Points

Availability refers to a level of service that applications, services, or systems provide, and is expressed as the percentage of time that a service or system is available. Highly available systems have minimal downtime, whether planned or unplanned, and are available more than 99 percent of the time, depending on the needs and the budget of the organization. For example, a system that is unavailable for 8.75 hours per year would have a 99.9 percent availability rating.

Question: What are some different ways that availability can be defined?

What Is Scalability?

Scalability measures the ability to increase capacity

Scaling up:

- Increases the capacity of a single server
- Involves adding more or better hardware to a server

Scaling out:

- Increases the capacity of an application
- Involves adding additional servers to perform processing

Key Points

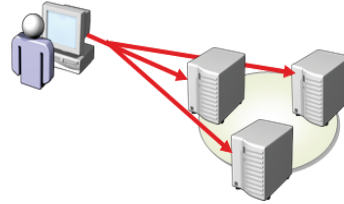
Scalability refers to the ability to increase the volume of activity that applications, services, or systems provide. Scalable systems have the ability to increase or decrease capacity as required.

Question: Which type of scaling is the simplest to implement?

USE PROHIBITED

What Is Load Balancing?

Load Balancing (NLB) is a system that increases the scalability and availability of the servers that provide access to data



Other load balancing methods:

- A virtual IP address is used to distribute requests between multiple servers
- Not suitable for all applications

Key Points

Load balancing is a system that increases the scalability and availability of the servers that provide data access. Multiple servers are configured with a single, virtual Internet Protocol (IP) address that they share to service requests. When a client makes a request to the virtual IP address, one server in the load-balancing cluster handles the request.

Question: Why is a separate back-end server used to store data for a load balancing cluster?

Comparing Hardware and Software Load Balancing

Hardware load balancing:

- Uses a device to provide the virtual IP
- Requires multiple devices to ensure fault tolerance

Software load balancing:

- All cluster nodes provide the virtual IP
- There is no single point of failure

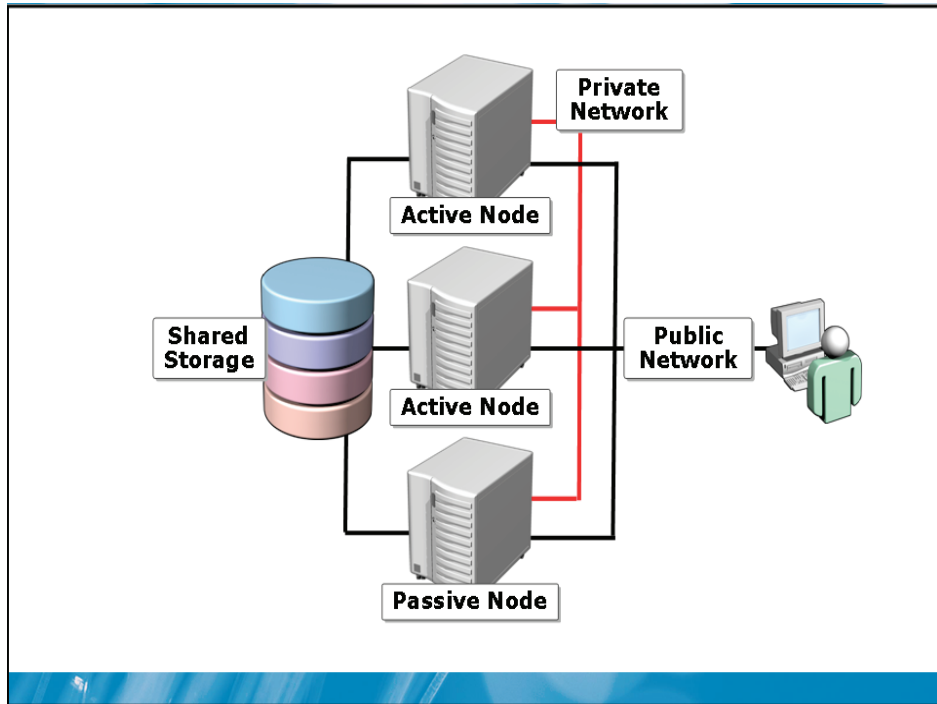
Key Points

Load balancing can be implemented as either a hardware or software solution. Both solutions are acceptable and which one you select will depend on the needs of your organization. Your choice may also be influenced by corporate standards specifying a particular vendor for all networking products.

Question: What is the lowest cost solution to implement load balancing for a low capacity Web-based application?

USE PROHIBITED

What Is Failover Clustering?



Key Points

Failover clustering is a solution to increase the availability of an application or service. Failover clustering creates virtual servers with an IP address that can failover from one cluster node to another. The application or service runs on a virtual server in the failover cluster. If the node running the application or service fails, then the application is started on another node in the cluster along with the virtual IP address and virtual server name. When the failover process occurs, clients connect to the virtual server on a new node.

Question: How does a cluster differ from load balancing?

Lesson 2

Windows Network Load Balancing

- What Is Windows Network Load Balancing?
- Requirements for Windows Network Load Balancing
- How Windows Network Load Balancing Works
- Data Synchronization between NLB Nodes

Windows Network Load Balancing is software-based load balancing included as part of Windows Server 2008. It has minimal requirements, but data must be synchronized between the nodes.

Microsoft
COURSEWARE
PROHIBITED

What Is Windows Network Load Balancing?

Windows Network Load Balancing:

- Is a fully distributed software solution for load balancing
- Is included with all versions of Windows Server 2008

Session Broker:

- For Terminal Services
- Distributes session requests to the least loaded server
- Provides scalability and availability
- Included in all version of Windows Server 2008

Key Points

Windows Network Load Balancing (NLB) is a fully distributed software solution for load balancing. It is included with all versions of Windows Server 2008, even the lower cost Web Edition. Because Windows NLB is fully distributed to all nodes, there is no single point of failure.

Question: Why is intelligent load distribution for terminal servers a benefit?

Requirements for Windows Network Load Balancing

Requirements:

- At least one network adapter for load balancing
- Only TCP/IP on the NLB adapter
- All NLB nodes on the same subnet

Key Points

It is preferred for NLB nodes to have two network adapters. This simplifies network communication by isolating NLB cluster traffic from host traffic. If only a single network adapter is used in NLB nodes, then the NLB cluster must be configured to use multicasts for network communication. The network adapter used for NLB can only be configured with TCP/IP.

Question: Are there any client considerations when the subnet for the NLB cluster is selected?

USE PROHIBITED

How Windows Network Load Balancing Works

Unicast mode:

- A unique NLB MAC address is assigned to NLB adapter in all nodes
- The original MAC address of the NLB adapter cannot be used
- Packets are received by all NLB nodes
- Only the appropriate NLB node responds
- Outgoing MAC is unique for each node to avoid switch problems

Multicast mode:

- A multicast MAC address is assigned to the NLB adapter in all nodes
- The original MAC address of the NLB adapter can still be used
- Removes the need for two network cards
- Only the appropriate NLB node responds

Key Points

The process varies slightly depending on whether unicast or multicast mode is selected.

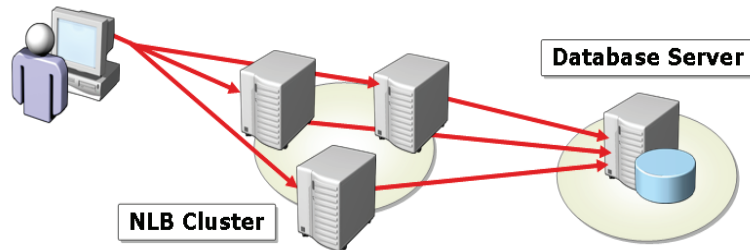
Question: Which mode will result in more overall network traffic?

Data Synchronization between NLB Nodes

All NLB nodes must have the same data to ensure that all nodes respond identically to requests

Data access can be provided by:

- Synchronizing content between servers
- Storing data in a common location



Key Points

All NLB nodes must have the same data to ensure that all nodes respond identically to requests. To ensure that this is the case, you can synchronize data between nodes or store the data in a common location. The option you select will depend on the type of application the NLB cluster is hosting.

Question: What are some methods you could use to synchronize data between Web servers?

USE PROHIBITED

Lesson 3

Configuring Windows Network Load Balancing

MCT USE ONLY. STUDENT USE PROHIBITED

- What Are the Cluster Parameters?
- What Are Port Rules?
- What Is the Filtering Mode?
- What Is Affinity?
- What Are the Host Parameters?
- Demonstration: Creating an NLB Cluster

Windows NLB has several parameters that can be configured to control how the NLB cluster functions. The settings that you select for these parameters will be based on the particular applications that are running on the NLB cluster. Some of the parameters include the filtering mode and affinity.

What Are the Cluster Parameters?

Cluster parameters include:

Cluster parameter	Description
IP address	Virtual IP address of the NLB cluster
Network address	MAC address of the NLB cluster
Cluster operation mode	Specified whether unicast or multicast operation is used

Key Points

For each NLB cluster, you can configure the following parameters: IP address, network address, and cluster operation mode.

Question: How do you determine the IP address that is used for the NLB cluster?

What Are Port Rules?

Port rules specify how requests to a certain IP address and port range are handled

Port rules define:

- Filtering mode
- Affinity
- Load weight
- Handling priority

Key Points

Port rules specify how requests to a certain IP address and port ranges are handled.

This allows you to define different rules for different applications running on the NLB cluster. For example, requests for a Web application on TCP port 80 may be distributed evenly among servers, but all requests for the Web application on TCP port 8080 may be directed to a single server.

Question: Why do you need port rules?

What Is the Filtering Mode?

Filtering mode	Description
Multiple hosts	All NLB nodes respond based on the weight assigned to each node
Single host	Only the NLB node with the highest priority responds
Disable this port range	All traffic for this port range is blocked

Key Points

Windows NLB uses the filtering mode in a port rule to determine how requests are distributed among nodes in the NLB cluster.

Question: Why would you use single-host filtering mode rather than multiple-hosts filtering mode?

What Is Affinity?

Affinity controls how requests from a client are distributed among multiple nodes in an NLB cluster

Affinity	Description
None	Each client request could be distributed to any node
Single	All requests from a single client are distributed to a single node
Network	All requests from a single class C sized network are distributed to a single node

Key Points

Affinity controls how requests from a specific client are distributed among the nodes in an NLB cluster. This setting is only relevant when the multiple-hosts filtering mode is selected.

Question: Can you think of other stateful applications where single affinity would be required?

What Are the Host Parameters?

Host parameters include:

Host parameter	Description
Initial host state	Specifies whether the host automatically joins the NLB cluster when started
Dedicated IP address	IP address that is used on the host for cluster management
Priority	Determines in which order the host is when a port rule does not apply

Key Points

For an NLB node, you can configure host parameters that are specific to that node. The host parameters control how each NLB node participates in the NLB cluster.

Demonstration: Creating an NLB Cluster

In this demonstration, you will see how to configure an NLB cluster

Question: How is NLB installed on Windows Server 2008?

Lab: Implementing Network Load Balancing

- Exercise 1: Preparing Web Servers for NLB
- Exercise 2: Creating an NLB Cluster for Failover
- Exercise 3: Configuring an NLB Cluster for Load Balancing

Logon information

Virtual machine	NYC-DC1, NYC-WEB, NYC-SVR1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

You are the server administrator for Woodgrove Bank. A new web-based application is being implemented. To increase the availability of the new Web-based application, you are using NLB in Windows Server 2008.

Exercise 1: Prepare Web Servers for NLB

Your new Web-based application will be installed on servers NYC-WEB and NYC-SRV1. You must install the Web server role on each server before configuring and testing the Web application on each server. The Network Load Balancing role must also be installed.

UNAUTHORIZED USE PROHIBITED

- ▶ Task 1: Prepare network connections on NYC-WEB for NLB
 1. On NYC-WEB, log on as Administrator with a password of Pa\$\$w0rd.
 2. Edit the properties of TCP/IPv4 on the Local Area Connection 2 interface:
 - IP address: **10.10.0.221**
 - Subnet mask: **255.255.0.0**
- ▶ Task 2: Prepare network connections on NYC-SRV1 for clustering
 1. On NYC-SVR1, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Edit the properties of TCP/IPv4 on the Local Area Connection 2 interface
 - IP address: **10.10.0.31**
 - Subnet mask: **255.255.0.0**
- ▶ Task 3: Join NYC-SRV1 to the domain
 1. On NYC-SRV1, open System Properties from within Server Manager.
 2. On the Computer Name tab, use the Change button to join the woodgrovebank.com domain.
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Reboot the system.
- ▶ Task 4: Create a Web site on NYC-WEB
 1. On NYC-WEB, create the folder C:\Webapp.
 2. Copy the file \\NYC-DC1\D\$\Mod13\Labfiles\srv1.txt to C:\Webapp\default.htm.
 3. Use the Internet Information Services (IIS) Manager administrative tool to create a new Web site.
 - Web site name: **Webapp**
 - Physical path: **C:\Webapp**
 - Port: **10080**

- ▶ Task 5: Create a Web site on NYC-SRV1
 1. On NYC- SRV1, use Server Manager to add the Web Server (IIS) server role, including the ASP.NET and ASP server features.
 2. Create the folder C:\Webapp.
 3. Copy the file \\NYC-DC1\DS\Mod13\Labfiles\SVR1.txt to C:\Webapp\default.htm.
 4. Use the Internet Information Services (IIS) Manager administrative tool to create a new Web site.
 - Web site name: **Webapp**
 - Physical path: **C:\Webapp**
 - Port: **10080**

- ▶ Task 6: Configure Firewall rules for the Web site
 1. On NYC-WEB, use the Windows Firewall with Advanced Security administrative tool to create a new inbound rule.
 - Rule type: **Port**
 - Port type: **TCP**
 - Specific local port: **10080**
 - Allow the connection
 - Profiles: all
 - Name: **Web Application**
 2. On NYC-SRV1, use the Windows Firewall with Advanced Security administrative tool to create a new inbound rule.
 - Rule type: **Port**
 - Port type: **TCP**
 - Specific local port: **10080**
 - Allow the connection
 - Profiles: all
 - Name: **Web Application**

- ▶ Task 7: Verify Web site functionality
 1. On NYC-DC1, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Use Internet Explorer to view the following Web sites:
 - <http://NYC-WEB:10080>
 - <http://NYC-SRV1:10080>
- ▶ Task 8: Install the Network Load Balancing feature
 1. On NYC-WEB, use Server Manager to install the Network Load Balancing Feature.
 2. On NYC-SRV1, use Server Manager to install the Network Load Balancing Feature.

Exercise 2: Create an NLB Cluster for Failover

To increase the availability of the new Web-based application, you have decided create an NLB cluster with failover. You will also create a port rule for the Web-based application.

- ▶ Task 1: Create a DNS record for the NLB cluster
 - On NYC-DC1, use the DNS administrative tool to create a new host record in the WoodgroveBank.com domain:
 - Name: **webapp**
 - IP address: **10.10.0.200**
- ▶ Task 2: Create an NLB cluster
 - On NYC-WEB, use the Network Load Balancing Manager administrative tool to create a new cluster.
 - Connect to NYC-WEB
 - Use the External interface
 - Accept the default host parameters
 - Cluster IP address: **10.10.0.200**
 - Subnet mask: **255.255.0.0**
 - Full Internet name: **webapp.woodgrovebank.com**
 - Operation mode: Unicast

- ▶ Task 3: Add NYC-SRV1 to the NLB cluster
 1. On NYC-SRV1, use the Network Load Balancing Manager administrative tool to connect to the existing cluster named webapp.woodgrovebank.com on NYC-WEB.
 2. Add NYC-SRV1 as a node to the cluster.

- ▶ Task 4: Configure a port rule for failover
 1. On NYC-SRV1, use the Network Load Balancing Manager administrative tool to open the properties of the cluster.
 2. On the Port Rules tab, edit the existing rule with the following settings:
 - Port range: from 10080 to 10080
 - Protocols: TCP
 - Filtering mode: Single host

- ▶ Task 5: Verify cluster failover
 1. On NYC-DC1, use Internet Explorer to view Web site on the NLB cluster.
 - `http:// webapp.woodgrovebank.com:10080`
 2. Reload the page several times to confirm that it is always loaded from NYC-WEB.
 3. On NYC-WEB in the Load Balancing Manager Administrative tool, stop the NYC-WEB node by using the Control Host submenu.
 4. On NYC-DC1, use Internet Explorer to view Web site on the NLB cluster.
 - `http:// webapp.woodgrovebank.com:10080`
 5. Verify that the Web page loaded from NYC-SRV1.
 6. On NYC-WEB in the Load Balancing Manager Administrative tool, start the NYC-WEB node by using the Control Host submenu.

Exercise 3: Configure an NLB Cluster for Load Balancing

The utilization of the Web application on NYC-WEB has grown to the point where the server is becoming overloaded. You have decided that you will configure the NLB cluster to load balance between to two nodes rather than failing over.

- ▶ Task 1: Configure a port rule for load balancing
 1. On NYC-WEB, use the Network Load Balancing Manager administrative tool to open the properties of the cluster.
 2. On the Port Rules tab, edit the existing rule with the following settings:
 - Filtering mode: Multiple host
 - Affinity: None
 3. If the status of NYC-SVR1 changes to misconfigured with the IP address 10.10.0.200 not bound, then disable and enable Local Area Connection 2.
- ▶ Task 2: Verify cluster load balancing
 1. On NYC-DC1, use Internet Explorer to view Web site on the NLB cluster.
 - [http:// webapp.woodgrovebank.com:10080](http://webapp.woodgrovebank.com:10080)
 2. Verify that the Web page loads after the configuration changes.

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Best Practices
- Tools

Review Questions

1. What is the difference between availability and scalability?
2. Which component intelligently distributes incoming requests for terminal servers?
3. Which option in a port filtering rule defines which NLB node will respond to the second request that a client makes?

Real-world Issues and Scenarios

1. Your organization is implementing a new Web-based application. The design calls for two front-end Web servers that communicate with a single, back-end database server. You were able to connect to the application on each server and successfully run tests. However, now that the servers have been added to an NLB cluster, the application does not seem to be functioning properly after initial login. What is the likely cause of this problem?

2. Your organization has a Web-based application that originally ran on a single Web server with a back-end database server. As your organization has grown, the load on the Web server has increased to the point where client performance is suffering. During peak periods, users wait up to 10 seconds for a response. To resolve this problem, you have implemented an NLB cluster. However, in the NLB cluster, one node is unused and the other is still running at capacity. What is the likely cause of this problem?

Best Practices for Implementing NLB

Supplement or modify the following best practices for your own work situations:

- Configure a static ARP entry for multicast MAC addresses if required by your router. Some routers do not support resolving a unicast address used by the cluster to a multicast MAC address.
- Enable Network Load Balancing logging. This can help during trouble shooting.
- Ensure that port rules include all of the ports used by an application. For example, a port rule for FTP should include TCP ports 20 and 21.
- Verify that applications on NLB nodes start automatically. This is required because NLB is not aware of applications and cannot verify that an application is functional before automatically joining the cluster.
- Use single host filtering mode when applications do not support multiple instances running at the same time.
- Use single affinity to support stateful applications.
- Use load weight to ensure specific NLB nodes respond only to the volume of requests that they can adequately service.
- Use the TS Session Broker to intelligently distribute the load among multiple Terminal Servers.

Tools

Tool	Use for	Where to find it
Network Load Balancing Manager	<ul style="list-style-type: none">• Create an NLB cluster• Manage NLB nodes	Administrative Tools
NLB.exe	<ul style="list-style-type: none">• Manage NLB from a command line• Manage NLB in scripts	Command prompt

NOT FOR STUDENT USE PROHIBITED

Module 14

Configuring Print Resources and Printing Pools

Contents:

Lesson 1: Printing Overview	14-3
Lesson 2: Configuring Network Printers	14-11
Lesson 3: Using Print Management	14-18
Lesson 4: Managing Printers	14-25
Lesson 5: Troubleshooting Network Printing	14-31
Lab: Implementing Printing	14-34

Module Overview

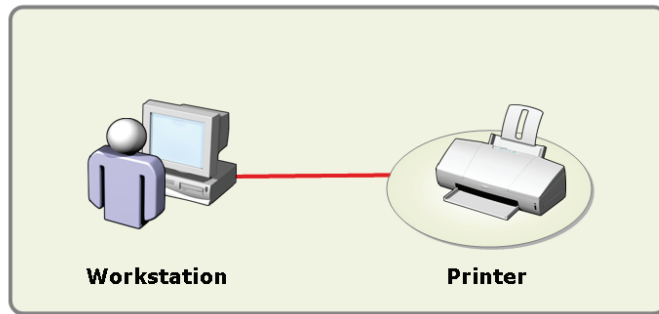
- Printing Overview
- Configuring Network Printers
- Using Print Management
- Managing Printers
- Troubleshooting Network Printing

Printing is an essential component of any corporate network. In many cases, Window Server 2008 is used as a print server to centralize management of printing to network printers. The Print Management Microsoft Management Console (MMC) snap-in is included to simplify printer management across multiple servers.

What Is Local Printing?

Local printing:

- Uses lower quality printers
- High consumables cost
- Low managability

**Key Points**

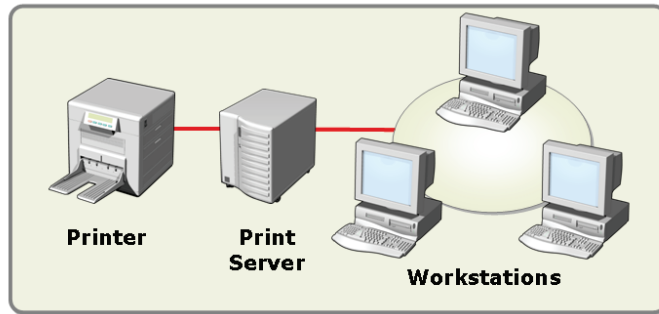
Local printing is when a printer is connected directly to a computer. The connection is typically done with a parallel cable or Universal Serial Bus (USB).

Question: If an organization uses local printing and has 10 computers, how many printers will there be?

What Is Network Printing?

Network printing:

- Allows for centralized management of printing
- Allows for queuing of jobs
- Uses lower cost consumables
- Uses higher quality printers



Key Points

Network printing is when a printer is available to computers over the network instead of being connected locally. A network printer can be connected locally to a print server, but most network printers are connected directly to the network with their own Internet Protocol (IP) address.

Question: What is the flow of a print job when Windows Server 2008 is used as a print server for a printer attached directly to the network?

What Are Printer Drivers?

Printer drivers:

- Convert documents to page description language understood by a specific printer
 - Postscript
 - Printer Control Language (PCL)
 - XML Paper Specification (XPS)
- Presents configuration options for a printer

Key Points

Printer drivers are software that is responsible for controlling how Windows operating systems communicate with a printer.

Question: What happens when you install an incorrect printer driver for a specific printer?

What Is XPS?

XML Paper Specification (XPS):

- Is a new document description language
- Can also be used as a page description language for printers

Key Points

XPS is a new document description language that is introduced in Windows Server 2008 and Windows Vista. XPS is a single format for document presentation that can be used to display documents and can also be used as a PDL for printing.

Question: When would you convert documents to XPS format?

PRINT USE PROHIBITED

What Is GDI-based Printing?

GDI-based printing:

- Is used in previous versions of Windows
- Uses enhanced metafile format (EMF) as the spool file format
- Is used by legacy applications

Key Points

GDI printing was used in versions of Windows previous to Windows Vista. The set of application programmer interfaces (APIs) used by applications to access operating system resources is called Win32. Win32 application use GDI-based printing.

Question: Would a document printed from Word 2003 use GDI-based printing?

What Is XPS-based Printing?

XPS-based printing:

- Is a new printing process in Windows Server 2008 and Windows Vista
- Requires an XPS printer driver
- Is used only by WPF applications
- Generates a spool file in XPS format

XPS-based printing improvements:

- Higher print quality
- Better color information
- Smaller spool files
- Print job and device configuration information that is easier for applications to access

Key Points

Windows Server 2008 and Windows Vista include a new printing process called XPS-based printing. This printing process uses only XPS as a single format for print jobs. Only newer applications that use Windows Presentation Foundation (WPF) APIs use XPS-based printing.

Question: Will all new applications use the XPS-based printing process?

Interoperability of XPS and GDI-based Printing

XPS-based printing:

- Can print to an older GDI-based printer driver
- Print job is converted from XPS to EMF

GDI-based printing :

- Can print to a new XPS-based printer driver
- Print job is converted from EMF to XPS

Key Points

There is interoperability between XPS and GDI-based printing. This allows you to use older GDI-based printer drivers with an application that used XPS-based printing. If necessary, the printing subsystem converts an XPS file to EMF to support older printer drivers.

Question: Do you need to replace existing printers with XPS-based printers when introducing Windows Server 2008 as a print server?

Lesson 2

Configuring Network Printers

- What Is the Printer Driver Store?
- How Printer Drivers are Distributed
- Printer Configuration Options
- How to Share a Printer
- What Is a Printer Pool?
- Demonstration: Configuring a Shared Printer

One of the most challenging tasks when configuring network printers is ensure that the appropriate printer drivers are available for the printer. Windows Vista and Windows Server 2008 use a new method for storing and distributing printer drivers. After the necessary driver is available, you can share the printer to make it available to client computers. You can also configure a printer pool to increase printer scalability and availability.

Microsoft
M
S
E
R
V
E
R
2
0
0
8
U
S
E
P
R
O
H
I
B
I
T
E
D

What Is the Printer Driver Store?

The printer driver store:

- Is a central location where printer drivers are stored
- Can store printer driver packages
- Can stage drivers before printer installation
- Supports multiple driver versions

Key Points

Windows Vista and Windows Server 2008 include a new printer driver store as method for storing printer drivers.

Question: Why is staging drivers on a print server a benefit?

How Printer Drivers are Distributed

Windows Server 2008 print servers use point and print to distribute printer drivers and printer driver packages to workstations

Printer drivers are added to the store when:

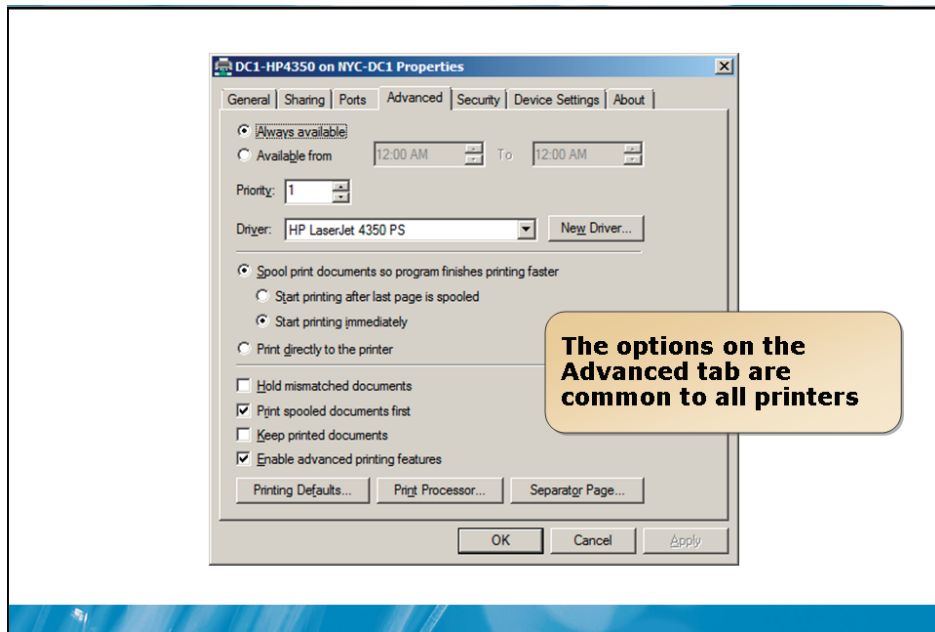
- The printer is installed on the print server
- Pnputil can stage drivers

Key Points

When clients install a printer that is shared on a Windows Server 2008 print server, Point and Print distributes printer drivers and printer driver packages to the clients. Windows Vista clients install the printer driver package. Windows 2000 and Windows XP clients cannot retrieve full printer driver packages and install only the basic printer driver. Point and print prevents the need to have drivers available on a disk or compact disc when a new printer is installed.

Question: Why do Windows 2000 and Windows XP clients only install printer drivers and not printer driver packages?

Printer Configuration Options



Key Points

The printer configuration options available for a printer vary depending on the printer and printer driver that are installed. However, the options on the Advanced tab are consistent for all printers.

Question: In what situation would a separator page be used?

How to Share a Printer

Printers on a print server must be shared before workstation can access them

Configuration options for shared printers:

- Shared printer name
- Job rendering location
- Add printer drivers for additional operating systems

Printer Security Permission	Description
Print	Allow or deny the ability to print to a shared printer
Manage printer	Allow or deny the ability to modify printer settings
Manage documents	Allow or deny the ability to pause, delete, and modify print jobs

Key Points

After a printer is installed on a print server, the printer must be shared before clients can begin using those printers.

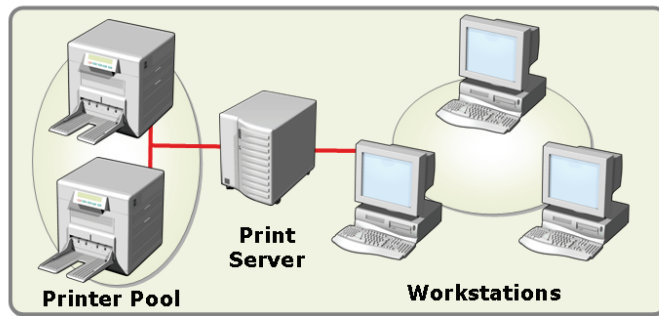
Question: What is an example of a situation in which you would want to pause a job in the queue?

PRINT USE PROHIBITED

What Is a Printer Pool?

A printer pool:

- Combines multiple physical printers into a single logical unit
- Uses as single logical printer connected to multiple ports
- Must use printers of the same model
- Increases printing scalability and availability
- Should use printers in the same location



Key Points

A printer pool is a way to combine multiple physical printers into a single logical unit. To client computers, the printer pool appears to be a single printer. When jobs are submitted to the printer pool, they can be processed by any available printer in the printer pool.

Question: What would happen if multiple printer models were combined in a printer pool?

Demonstration: Configuring a Shared Printer

In this demonstration, you will see how to configure a shared printer

Question: What are the default permissions on a shared printer?

BETA COURSEWARE. EXPIRES 5/16/2008
STUDENT USE PROHIBITED

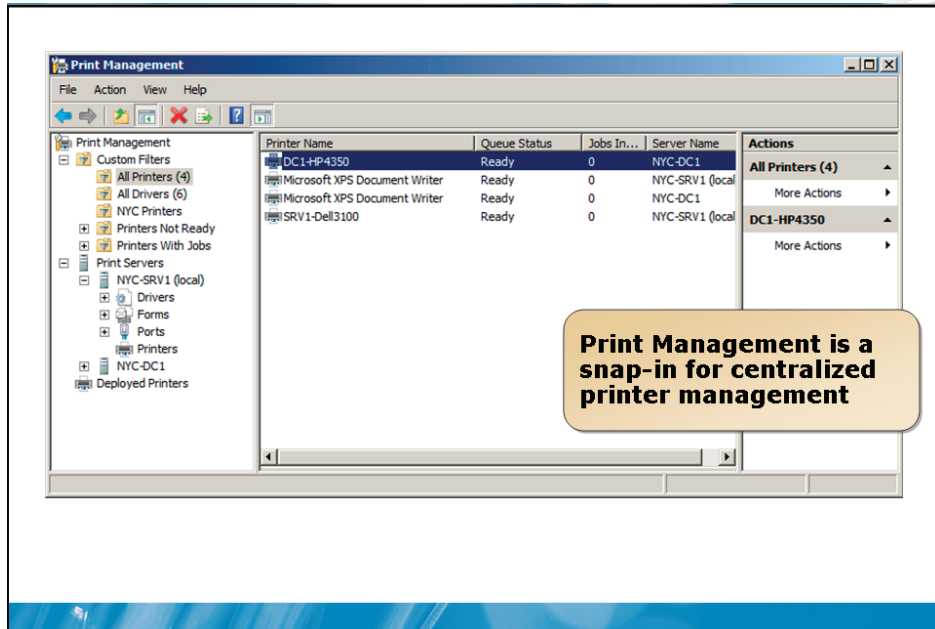
Lesson 3 Using Print Management

MCT USE ONLY. STUDENT USE PROHIBITED

- What Is Print Management?
- Print Server Configuration Options
- Printer Management Options
- What Are Printer Filters?
- How Automatic Printer Installation Works
- Demonstration: Using Print Management

Windows Server 2003 R2 introduced the Print Management snap-in for managing printers and print servers. This tool includes the ability to filter printers based on status. Also Printer Management can be used to create group policy objects for automatic printer installation.

What Is Print Management?



Key Points

Print Management is a snap-in for centralized printer management that was first introduced in Windows Server 2003 R2. Through Control Panel, you can manage only the local print server and printers. With Print Management, you can manage remote print servers and printers in addition to the local print server and printers.

Question: Why is it easier to manage multiple print servers by using Print Management?

Print Server Configuration Options

Print Server configuration options include:

Option	Description
Forms	The sizes and formats of paper that the printer can be configured to use
Ports	The methods available to communicate with printers such parallel ports and TCP/IP ports
Drivers	The drivers used to convert print jobs into a language the printers can use
Spooler configuration	Configuration options related creating and managing print jobs such as to start printing a job only after the last page is spooled
Automatically adding network printers to a print server	This option scans the local subnet for network printers and adds them to a print server
Setting notifications	Notifications can be configured to notify administrators by using e-mail or scripts when there are errors on the print server
Export/Import Printers	Migrates printers from one print server to another

Key Points

Print Management allows you to manage printers that are running on print servers running Windows 2000 Server, Windows Server 2003, and Windows Server 2003 R2. In addition, Print Management can manage shared printers on Windows XP and Windows 2000 clients. There is also limited support for Windows NT 4.0 print servers.

Question: Why is the \spoolss name pipe important for using Print Management?

Printer Management Options

You can use the Print Management snap-in to perform all of the tasks that can be performed by using Control Panel

Tasks that can only be performed by using Print Management are:

- Deploy printers by using Group Policy
- Add and remove printers from Active Directory by using a context menu
- Perform bulk operations to multiple printers at a time

Key Points

For each print server you have added to Print Management you can manage the printers on that server. You can use Print Management to perform all of the printer management tasks possible in Control Panel.

Question: Is there any reason to manage printers through Control Panel rather than by using Printer Management?

NT USE PROHIBITED

What Are Printer Filters?

A printer filter displays the printers that meet a certain set of criteria

Default filters include:

- All Printers
- Printers Not Ready
- Printers With Jobs

Key Points

A printer filter displays the printers that meet a certain set of criteria. You can use printer filters to display only printers with errors to aid with troubleshooting. You can also use printer filters to display only printers in a certain physical location such as a branch office.

Question: Why is Jobs in queue a commonly used field for a custom printer filter?

How Automatic Printer Installation Works

Automatic printer installation detects and installs all printers on the local subnet of the print server

Steps performed for automatic printer installation:

- 1** Trigger automatic printer installation on the print server
- 2** Find valid IP addresses on the local subnet by using ARP requests
- 3** Query the type of printer by using SNMP requests
- 4** Install the appropriate printer driver
- 5** Grant default print permissions

Key Points

Print Management can automatically detect all network attached printers located on the same subnet as the print server, install the appropriate printer drivers, set up the queues, and share the printers. Unless a printer driver cannot be found, no intervention is needed. For this process, you must run Printer Management on the print server that the printers are being installed on.

Question: Will the size of a subnet affect the time required to perform automatic printer installation?

NTUSEREPROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Demonstration: Using Print Management

In this demonstration, you will see how to use the Print Management snap-in

Question: What are the default printer filters?

Lesson 4

Managing Printers

- Bulk Print Management Tasks
- How To Manage Printer Drivers
- How to Deploy Printers with Group Policy
- How to Manage Print Jobs
- Demonstration: Managing Printers

Printing is an important function of computer networking. Consequently, managing printers is an important and highly visible task within an organization. By using Printer Management, you can perform bulk printer management tasks and deploy printers with Group Policy. Also, you can manage printer drivers and manage print jobs.

Bulk Print Management Tasks

Tasks you can perform on multiple printers at the same time are the bulk print management tasks

The bulk print management tasks include:

- Pausing printing
- Resuming printing
- Cancelling all print jobs
- Listing printers in Active Directory
- Removing printers from Active Directory
- Deleting printers from print servers

Key Points

Using Print Management you can perform some tasks on multiple printers at the same time. Tasks you can perform on multiple printers at the same time are the bulk print management tasks. Not all printer management tasks can be performed on multiple printers at once.

Question: Why is bulk print management a benefit?

How To Manage Printer Drivers

Each print server maintains a separate set of printer drivers

By using Print Management you can:

- Add printer drivers
- View driver details on each print server
- Export driver details to a text file

Key Points

Each print server maintains a separate set of printer drivers. You must manage printer drivers on each server separately.

Question: Does Printer Management allow you to add a printer driver to multiple servers with a single action?

CONTENT USE PROHIBITED

How to Deploy Printers with Group Policy

Steps for deploying printers with Group Policy:

- 1 Select Deploy with Group Policy in Print Management
- 2 Select a group policy object
- 3 Select per user and/or per machine connections
- 4 Run PushPrinterConnections.exe in a logon script

Key Points

Print Management can be used with Group Policy to automatically add printer network printers to a computer. This is useful in any environment with various workgroups that use different printers.

Question: What will happen if you run PushPrinterConnections as part of a user logon script on Windows XP clients and there are per-computer printer connections defined in a GPO?

Demonstration: Managing Printers

In this demonstration, you will see how to manage printers

Question: Does a user get any notification when their print job is paused or deleted?

Lesson 5

Troubleshooting Network Printing

- Discussion: Common Printing Problems
- How to Identify Printing Problems

Troubleshooting network printing is an essential skill for network administrators. You should be aware of common printing problems and how to resolve them. Also, you should be aware of the methods available in Windows Server 2008 to detect printing problems.

Discussion: Common Printing Problems

- What are some common printing problems and how can you resolve them?

Key Points

Answer the questions in a classroom discussion.

Lab: Implementing Printing

MCT USE ONLY. STUDENT USE PROHIBITED

- Exercise 1: Creating an XPS document
- Exercise 2: Adding a Printer by using Control Panel
- Exercise 3: Using Print Management
- Exercise 4: Deploying Printers by using Group Policy

Logon information

Virtual machine	NYC-DC1, NYC-WEB, NYC-CL1
User name	Administrator
Password	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

You are the printing administrator for Woodgrove Bank. As the printing administrator, you are responsible for maintenance of all print servers. In addition, you are responsible for adding and removing all printers from the network.

The main tasks for this exercise are as follows:

- Create and view an XPS document
- Add and share a printer by using Control Panel
- Use Print Management to add and share a printer
- Deploy a printer by using Group Policy
- Migrate a printers between servers

Exercise 1: Creating an XPS document

As part of the testing for implementation of Windows Server 2008 as a print server, you have been reading about the use of XPS as a format for distributing documents. You would like your organization to consider using XPS for internal distribution of documents. The first step in your proposal is demonstrating the process to other members of the server administration team.

- ▶ Task 1: Create a file share
 1. On NYC-DC1, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Share the folder D:\Mod14\Labfiles.
 3. Assign Dana Birkby the Co-owner permission level.
- ▶ Task 2: Convert a document to XPS
 1. On NYC-CL1, log on as **Dana** with a password of **Pa\$\$w0rd**.
 2. View the Microsoft XPS Document Writer in the list of printers in Control Panel.
 3. Open \\NYC-DC1\Labfiles\xps-read in WordPad
 4. Use the **Microsoft XPS Document Writer** printer to convert xps-read to the file new-xps-read in the same folder.
 5. Open **new-xps-read** and verify that you cannot modify the text.
- ▶ Task 3: View an XPS document on a server.
 1. On NYC-DC1, use Server Manager to add the XPS Viewer .NET Framework 3.0 Feature.
 2. Open **D:\Mod14\Labfiles\new-xps-read.xps**.

Exercise 2: Adding a Printer by using Control Panel

A new printer has been purchased for the New York office of Woodgrove bank. The physical printer has been attached to the network with an IP address of 10.10.0.100. Eventually a dedicated print server running Windows Server 2008 will host this printer, but as a temporary measure, you are sharing this printer on NYC-DC1.

- ▶ Task 1: Install a printer on a server
 1. On NYC-DC1, use the Printers icon in Control Panel to install a new local printer.
 2. Create a new port:
 - Type of port: Standard TCP/IP port
 - Device type: TCP/IP Device
 - IP Address: 10.10.0.100
 - Device type: Standard, Generic Network Card
 3. Configure the printer:
 - Printer driver: HP LaserJet 4350 PS
 - Printer name: DC1-HP4350
 - Share this printer
 - Share name: DC1-HP4350
- ▶ Task 2: Install the printer on a client
 1. On NYC-CL1, log on as **Dana** with a password of **Pa\$\$w0rd**.
 2. Use Printers in Control Panel to add a new network printer:
 - Share name: \\NYC-DC1\DC1-HP4350
 3. Set the new printer as the default printer.
- ▶ Task 3: Test the shared printer
 1. On NYC-CL1, in the properties of **DC1-HP4350 on NYC-DC1**, print a test page.
 2. On NYC-DC1, verify that there is a print job from Dana in the queue for DC1-HP4350.
 3. Cancel the Test Page print job.

Exercise 3: Using Print Management

A new computer running Windows Server 2008 has been installed on the network. This new computer is going to be a print server. You need to install the Print Server role and configure a new shared network printer on this computer.

- ▶ Task 1: Install the Print Services role
 1. On NYC-WEB, log on as **Administrator** with a password of **Pa\$\$w0rd**.
 2. Use Server Manager to install the Print Services role.
 2. Install only the **Print Server** role service.

- ▶ Task 2: Install a printer by using Print Management
 1. On NYC-WEB, use the Print Management administrative tool to create a port on NYC-WEB:
 - Standard TCP/IP port
 - IP Address: 10.10.0.101
 - Device Type: Standard, Generic Network Card
 2. Use the Print Management administrative tool to install a new printer on NYC-WEB.
 - Printer driver: Dell 3100cn PS
 - Printer Name: WEB-Dell3100
 - Share this printer
 - Share Name: WEB -Dell3100

- ▶ Task 3: Create a printer filter for New York printers
 1. On NYC-WEB in Print Management, add the NYC-DC1 print server.
 2. View the contents of the All Printers custom filter.
 3. View the contents of the All Drivers custom filter.
 4. Create a new printer filter:
 - Name: NYC Printers
 - Field: Location
 - Condition: contains
 - Value: NYC
 5. Verify that no printers are listed in the NYC Printers filter.

- ▶ Task 4: Configure printer locations
 1. On NYC-WEB in Print Management, configure the location of DC1-HP4350 as **NA/US/NYC/Reception**.
 2. Configure the location of **WEB-Dell3100** as **NA/US/NYC/5th Floor**.
 3. Verify that the NYC Printers filter now shows two printers.

Exercise 4: Deploying Printers by using Group Policy

In the past, you have configured printers on user workstations by running scripts during logon. This has worked well for you, but other members of the server administration team are not familiar with writing scripts. You have decided to configure all new printers on user workstations by using Group Policy.

- ▶ Task 1: Add a printer connection to a group policy object
 1. On NYC-WEB in Print Management, use the context menu of **WEB-Dell3100** to **Deploy with Group Policy**.
 2. Create a new group policy object named **NYC Printer**.
 3. Apply the printer connection per user.
- ▶ Task 2: Test deployment of a printer by using Group Policy
 1. On NYC-CL1, log on as **Dana** with a password of **Pa\$\$w0rd**.
 2. Verify that WEB-Dell3100 on NYC-WEB appears in the list of printers.

Exercise 5: Migrate a printer to a new server

Now that the new print server is in place, you need to migrate an existing printer. As part of the migration process, you need to install the printer on user workstations as well.

- ▶ Task 1: Export printers from NYC-DC1
 1. On NYC-WEB in Print Management, export the printers on NYC-DC1 to a file:
 - File name: C:\DC1printers

- ▶ Task 2: Import printers to NYC-WEB
 1. On NYC-WEB in Print Management, import the printers from a file to NYC-WEB:
 - File name: C:\DC1printers
 - Import mode: Keep existing printers; import copies.
 - List all printers in the directory
- ▶ Task 3: Verify migration of the printer
 1. On NYC-WEB in Print Management, use the All Printers filter to verify that the printer DC1-HP4350 now exists on NYC-WEB.
 2. Remove DC1-HP4350 from NYC-DC1.
- ▶ Task 4: Add a printer connection to a group policy object
 1. On NYC-WEB in Print Management, use the context menu of **DC1-HP4350** to **Deploy with Group Policy**.
 2. Use the **NYC Printer** group policy object.
 3. Apply the printer connection per user.
- ▶ Task 5: Confirm deployment of a printer by using Group Policy
 1. On NYC-CL1, log on as **Dana** with a password of **Pa\$\$w0rd**.
 2. Verify that DC1-HP4350 on NYC-WEB appears in the list of printers.

Module Review and Takeaways

MCT USE ONLY. STUDENT USE PROHIBITED

- Review Questions
- Real-world Issues and Scenarios
- Best Practices
- Tools

Review Questions

1. Is XPS a document description language or a page description language?
2. Are all printer drivers included with Windows Server 2008 automatically installed in the printer driver store?
3. Which feature of the Print Management snap-in allows you to view only printers with specific properties?
4. How can you allow one print job to print ahead of another?
5. How can Print Management help identify incorrect drivers?

Real-world Issues and Scenarios

1. You are the IT support person for an organization with 50 users. One of the managers has indicated to you that a local office supply store is selling inkjet printers for \$50 each. This manager would like to purchase one for each of ten users under his supervision. Explain why you think this is not a good idea.

2. You are the printing administrator for a large organization with over 30 print servers. You understand the advantages of XPS-based printing and would like to implement Windows Server 2008 on all print servers. A server administrator is less enthusiastic. Explain to the server administrator why introducing Windows Server 2008 will not cause printing problems for GDI-based printing devices.
3. You are the printing administrator for a large organization with over 30 print servers. You have upgraded all print servers to Windows Server 2008 and are managing them by using the Print Management snap-in. To date, there have been no problems connecting to the print servers. However, when you install a new print server, you are unable to connect to it remotely by using Print Management. What is the likely source of the problem?
4. You are the printing administrator for a large organization that prints thousands of checks per day. After the checks are printed, the forms are folded and placed into envelopes. The current check printer can just barely keep up with the needs of users. There are concerns that a failure of the check printer could interrupt service to customers. How can you enhance the scalability and availability of the check printing without reconfiguring workstations?

Best Practices for Printer Management

Supplement or modify the following best practices for your own work situations:

- **Use Print Management to centralize printer management.** By using Print Management, you can manage all of the print servers in an organization from a single interface. This makes printer management faster and more efficient.
- **Use printer filters to group printers.** A printer filter lets you quickly find printers with specific errors or printers in a specific location.
- **Use a custom MMC console to share custom printer filters.** Sharing a single MMC console ensures that you have access to your custom filters no matter which computer you are logged into.

- **Use printer notifications.** By using printer notifications, you can be quickly notified if a printer error occurs. In addition, depending on the error, it may be possible to run a script and fix the problem.
- **Use server notifications.** By using server notifications, you can be quickly notified if a server error occurs. In addition, depending on the error, it may be possible to run a script and fix the problem.
- **Use Group Policy Objects to deploy printers.** By using Group Policy Objects to deploy printers, you can centralize the installation and removal of printers on the network. This significantly reduces the effort required to support printing on workstations.

Tools

Tool	Use for	Where to find it
Print Management	<ul style="list-style-type: none"> • Managing printers • Managing print servers 	Administrative Tools
PushPrinterConnections.exe	<ul style="list-style-type: none"> • Enabling printer connections on Windows XP and Windows 2000 by using Group Policy 	C:\Windows\System32

Module 15

Virtualization Overview

Contents:

Lesson 1: Overview of Server Virtualization	15-3
Lesson 2: Overview of Windows Server Virtualization	15-9
Lesson 3: Creating a Virtual Environment	15-15

MCT USE ONLY STUDENT USE PROHIBITED

Module Overview

- Overview of Server Virtualization
- Overview of Windows Server Virtualization
- Creating a Virtual Environment

Server virtualization is used by many organizations reduce hardware costs and simplify server management. Windows Server 2008 includes Windows Server Virtualization as a server role to implement server virtualization. To create a virtual environment, you must consider how you will manage the virtual infrastructure.

Lesson 1

Overview of Server Virtualization

- What Is Server Virtualization?
- Hypervisor Architecture
- Hypervisor Types
- Benefits of Server Virtualization
- Server Virtualization Scenarios

Server virtualization lets you run multiple operating systems on a single physical server. There are several different architectures for implementing a hypervisor that allows virtualization. Depending on the needs of your organization, there are several scenarios where server virtualization is commonly used.

MOOREHEAD GROUP
USE PROHIBITED

What Is Server Virtualization?

Server virtualization allows multiple instances of an operating system to run on a single computer

A hypervisor:

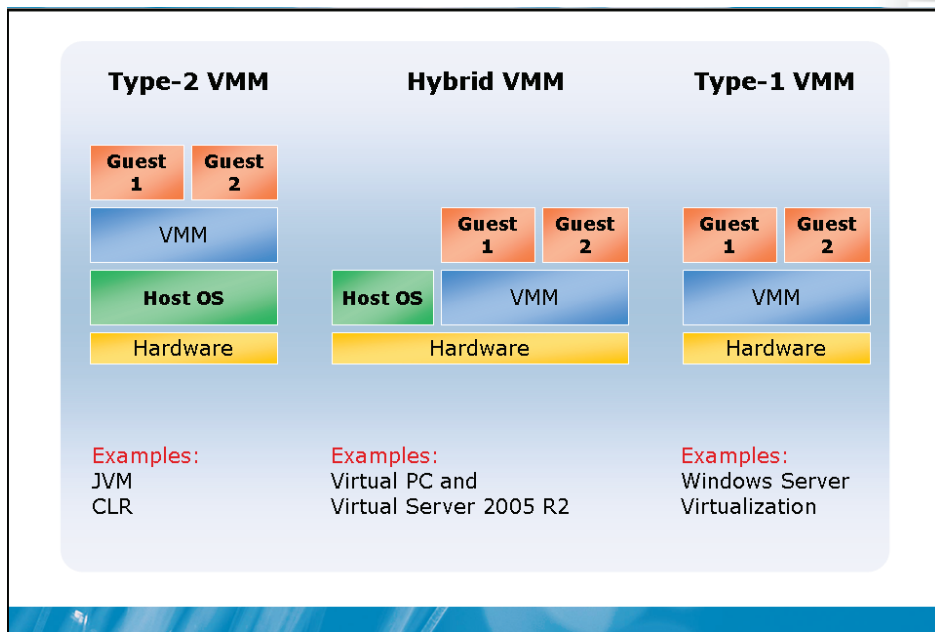
- May run on bare metal or within a host operating system
- Can present emulated hardware to guest operating systems
- Isolates operating system instances

Key Points

Server virtualization is a system that allows multiple operating systems to run on a single physical computer. This is implemented by installing virtualization software. The virtualization software includes the ability to create and manage virtual machines (VMs).

Question: How does server virtualization relate to a multi-boot configuration?

Hypervisor Architecture



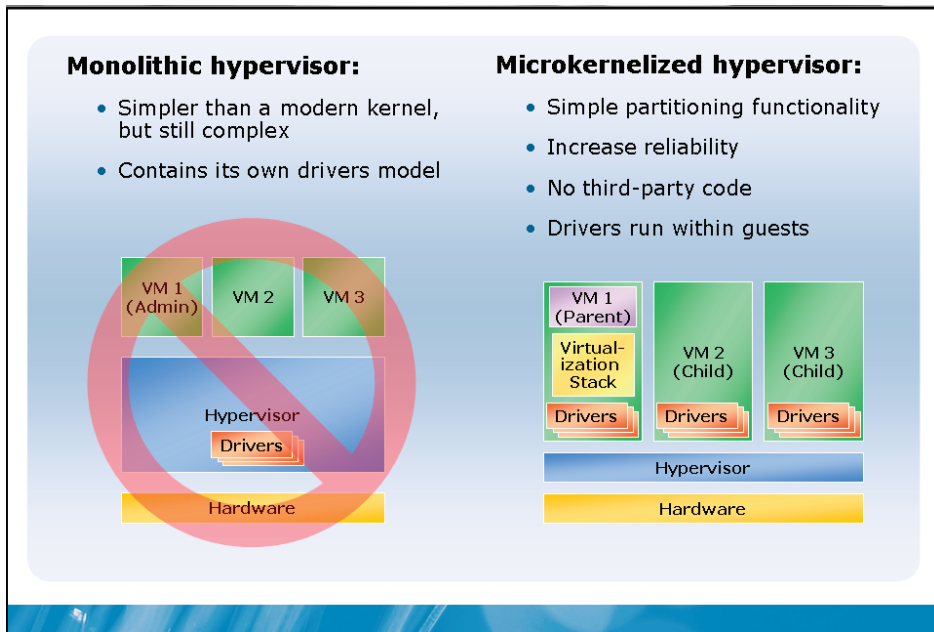
Key Points

VMs can be implemented in a number of ways depending on design architecture of the vendor of the virtualization software. It also depends on the task you are trying to accomplish.

Question: Why will a type 1 architecture have better performance than a type 2 architecture?

BETA COURSEWARE. EXPIRES 5/16/2008

Hypervisor Types



Key Points

Even when a type 1 architecture is used by virtualization software, there can be different hypervisor types.

Question: With a microkernelized hypervisor, will additional software need to be installed for a Guest operating system to run in a VM?

Server Virtualization Scenarios

The server virtualization scenarios are:

- Server consolidation
- Testing and development
- Re-host legacy applications
- Disaster recovery

Key Points

There are several server virtualization scenarios.

Question: What are some types of testing that can be performed with a virtual environment?

Lesson 2

Overview of Windows Server Virtualization

- What Is Virtual Server?
- What Is Windows Server Virtualization?
- Windows Server Virtualization Requirements
- Windows Server Virtualization Features
- Windows Server Virtualization Architecture

Windows Server Virtualization is the virtualization software that is included with Windows Server 2008. This virtualization software uses a similar disk file to Microsoft Virtual Server 2005 R2, but has some unique hardware and software requirements and a very different architecture.

MICROSOFT USE PROHIBITED

What Is Virtual Server?

Virtual Server:

- Is a hypervisor that runs parallel to the Windows operating system (hybrid VMM)
- Works with previous versions of Windows Server
- Stores disks in .vhd files
- Stores configuration settings in .vmc files
- Hardware devices are emulated

Key Points

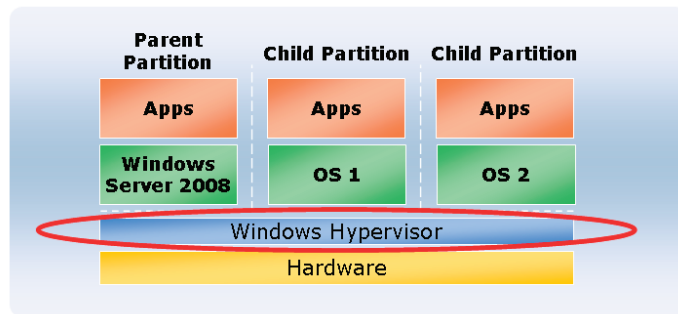
Microsoft Virtual Server 2005 R2 is virtualization software that includes a hypervisor that runs parallel to the Windows operating system. It is a hybrid virtual machine manager (VMM) architecture that has a monolithic hypervisor. As such, it emulates devices for guest operating systems. This is virtualization software that can be used on Windows Server 2003 and Windows XP (non-production).

Question: What benefit is there to a fixed-size virtual disk rather than growing dynamically?

What Is Windows Server Virtualization?

Windows Server Virtualization:

- Is a bare metal hypervisor for 64-bit versions Windows Server 2008
- Supports dynamic resource allocation
- Supports 32-bit and 64-bit guests
- Supports live migration of virtual machines



Key Points

Windows Server Virtualization is software that is added to Windows Server 2008 as a server role. When the Windows Server virtualization role is installed, the Windows hypervisor is installed and begins running after reboot. The Windows hypervisor runs before the operating system.

Question: What is the benefit of dynamic resource allocation between child partitions?

Windows Server Virtualization Requirements

Software Requirements:

- Windows Server 2008 Standard, Enterprise, or Datacenter Editions
- Windows Server 2008 64-bit versions only
- Enterprise Edition includes licenses for up to 4 virtualized servers
- Datacenter Edition includes licenses for an unlimited number of virtualized servers

Hardware Requirements:

- 64-bit x86 processor
- Hardware assisted virtualization
 - AMD-V or Intel VT
- Hardware enabled Data Execution Prevention
 - AMD NX (no execute bit)
 - Intel XD (execute disable)

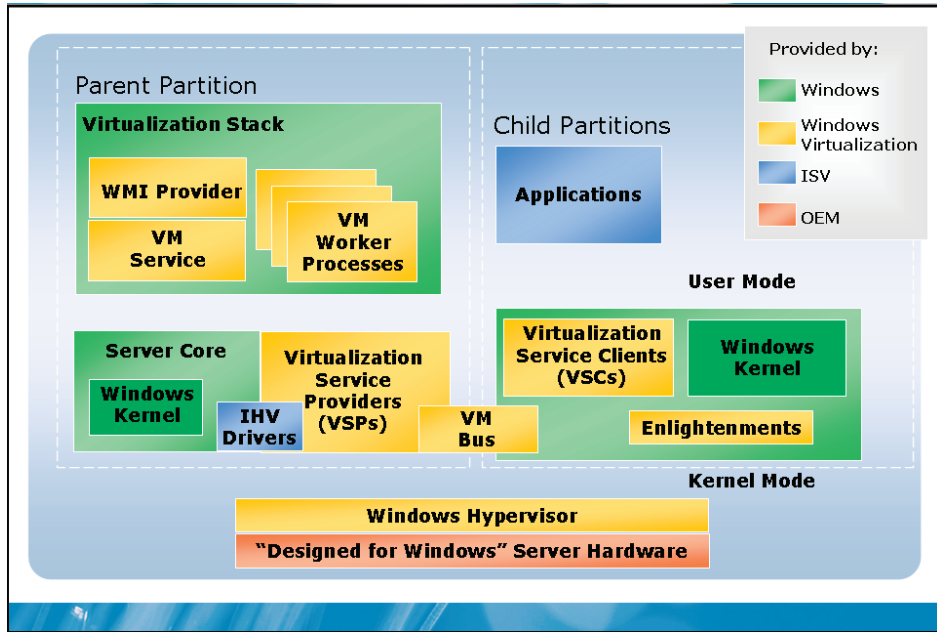
Key Points

Windows Server Virtualization can run on the 64-bit versions of Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition, or Windows Server 2008 Datacenter Edition. However, Windows Server Virtualization cannot run on Windows Server 2008 Web Edition or any 32-bit version of Windows Server 2008.

Question: Why are hardware-assisted virtualization and hardware-enabled DEP required by Windows Server Virtualization?

MCT USE ONLY. STUDENT USE PROHIBITED

Windows Server Virtualization Architecture



Key Points

When Windows Server Virtualization is installed as a role, the Windows hypervisor is inserted between the hardware and the parent partition. The parent partition is the instance of Windows Server 2008 that you just installed the role into. This partition is required for the proper functioning of child partitions, which are the VMs.

Question: From the perspective of the user, how do synthetic hardware devices vary from emulated hardware devices?

Lesson 3

Creating a Virtual Environment

- Hardware Consideration for Virtualization
- Software Considerations for Server Virtualization
- Management Considerations for Server Virtualization
- What Is System Center Virtual Machine Manager?
- What Is Quick Migration?

There are number of unique considerations when creating a virtual environment. These are caused by multiple VMs sharing the same hardware. To help manage virtual environments, you can use System Center Virtual Machine Manager.

Hardware Consideration for Virtualization

Hardware considerations:

- ✓ Physical memory needs to be enough to support all virtual machines concurrently
- ✓ Processor capacity need to be enough to support all virtual machines concurrently
- ✓ Disk I/O is intensive for .vhd files and memory contents stored on disk
- ✓ Multiple VMs share the network capacity of the hardware

Key Points

When planning a virtualized environment, you must consider the resource requirements of all VMs that will be running on each server.

Question: How can you expand disk throughput?

Software Considerations for Server Virtualization

Software considerations:

- The guest operating system must be supported
- Windows Server virtualization can run operating systems without modification
- Hypervisor aware operating system can make more efficient use of hardware resources

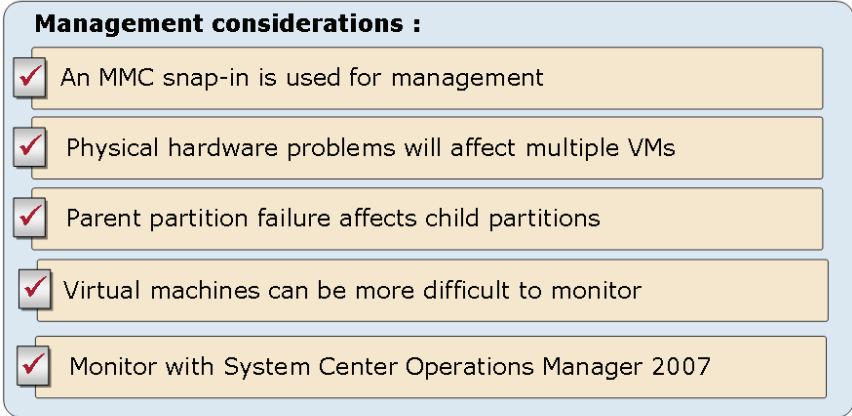
Key Points

When planning a virtualized environment, you must consider the characteristics of both the virtualization software and the guest operating systems.

Question: Which Windows operating system will have the best performance when virtualized?

NT USE PROHIBITED

Management Considerations for Server Virtualization



Management considerations :

- An MMC snap-in is used for management
- Physical hardware problems will affect multiple VMs
- Parent partition failure affects child partitions
- Virtual machines can be more difficult to monitor
- Monitor with System Center Operations Manager 2007

Key Points

The key thing to consider about managing VMs is that some issues can affect multiple VMs.

Question: How does using Server Core make the parent partition more stable?

What Is Quick Migration?

Quick Migration allows VMs on a SAN to be migrated to a standby server

Planned migration:

- State is saved to disk then restored on standby server
- Downtime depends on memory and speed of SAN
- Downtime can be only a few seconds

Unplanned migration

- State is not saved
- Virtual machine is restarted on standby server
- Downtime will be minutes

Key Points

Quick Migration is a system that combines failover clustering and Windows Server Virtualization. This requires VMs to be hosted on a virtual server in the cluster and the storage to be on a SAN. All configuration files and virtual disks are stored on the SAN. Migration of VMs to a standby server can be planned or unplanned.

Question: When a planned migration is performed using Quick Migration, do the applications on the VM need to be restarted?

Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Best Practices

Review Questions

1. What is the difference between a monolithic and microkernelized hypervisor?
2. What are the hardware requirements for running Windows Server Virtualization?
3. What considerations beyond the basic hardware requirements need to be considered when purchasing hardware to host VMs?

Real-world Issues and Scenarios

1. You are an IT architect at a large insurance provider with seven physical locations, 12,000 users and 220 servers. Your organization would like to use server virtualization to reduce management and hardware costs by consolidating existing servers on new hardware. What criteria will you use when selecting servers for consolidation?

2. You are an IT architect at a large insurance provider. You have migrated many critical applications to VMs and would like to increase the availability of those VMs. How can availability of VMs be increased when using Windows Server Virtualization?
3. You are the manager responsible for controlling the process used for testing new application patches and releases at a large insurance provider. In the past, you have maintained development, test, and production servers for all of your applications. This resulted in hundreds of servers being stored in the datacenter. How can you use Windows Server Virtualization to reduce hardware costs for development and testing?

Best Practices for Increasing VM Performance

Supplement or modify the following best practices for your own work situations:

- **Ensure that there is enough RAM in the host server.** In addition to the requirements of the individual VMs, the parent partition needs to be allocated sufficient RAM.
- **Ensure that there is sufficient processing power in the host server.** You may need to add multiple processors depending on the workload. Workload is shared among CPUs and CPU cores.
- **Ensure that the disk subsystem is high performing.** This is relevant only for the physical disks that virtual hard disks are stored on. Due to the synthetic drivers used in Windows Server Virtualization, the performance of SCSI and IDE disks within a VM is equivalent. Virtual hard disks should be stored on a separate disk from the parent partition operating system.
- **Add additional network cards to increase network performance.**
- **Use fixed-size virtual disks.** This avoids waiting for the virtual hard disk file to expand dynamically when required. Also, it minimizes fragmentation of virtual hard disks.
- **Do not run other applications in the parent partition.** A parent partition that is dedicated only to virtualization will deliver better performance. Minimizing applications running in the parent partition also increases overall system stability and security.