

Microsoft® Windows® 2000 Network and Operating System Essentials Delivery Guide

Course Number: 2151A

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Contents

Introduction

Introduction.....	1
Course Materials	2
Prerequisites.....	3
Course Outline	4
Microsoft Official Curriculum.....	7
Microsoft Certified Professional Program	8
Facilities.....	10

Module 1: Introduction to Windows 2000 and Networking

Overview.....	1
Windows 2000 Operating Systems	2
Introduction to Networks	8
Lab A: Identifying Computer Networks	15
Windows 2000 Implementation of Networking.....	16
Lab B: Identifying Features of a Windows 2000 Network	25
Lab C: Logging On to Windows 2000.....	26
Review	29

Module 2: Administration of a Windows 2000 Network

Overview.....	1
Windows 2000 Help	2
Lab A: Using Windows 2000 Help.....	7
Administrative Tasks	14
Administrative Tools	18
Lab B: Identifying Administrative Tools.....	39
Review	45

Module 3: Securing a Windows 2000 Network

Overview.....	1
User Accounts.....	2
Groups.....	7
Lab A: Examining Users and Groups	8
User Rights	10
Lab B: Examining User Rights	14
Permissions	17
Lab C: Examining File and Folder Permissions	27
Review	31

Module 4: Examining the Network

Overview.....	1
Scope of Networks.....	2
Basic Connectivity Components.....	3
Network Topologies.....	9
Network Technologies	15
Expanding the Network	21
Lab A: Examining the Network Architecture	34
Review	36

Module 5: Examining Network Protocols

Overview	1
Introduction to Protocols.....	2
Protocols and Data Transmissions	6
Common Protocols.....	10
Other Communication Protocols.....	15
Remote Access Protocols.....	18
Lab A: Identifying Protocol Capabilities	23
Review	24

Module 6: Examining TCP/IP

Overview	1
Introduction to TCP/IP	2
TCP/IP Protocol Suite.....	7
Lab A: Using TCP/IP Utilities	17
Name Resolution.....	20
Examining the Data Transfer Process	26
Routing Data	32
Lab B: Identifying Processes and Protocols in TCP/IP.....	37
Review	38

Module 7: Examining IP Addressing

Overview	1
Classful IP Addressing.....	2
Subnetting a Network.....	6
Lab A: Determining Class Addresses and Subnet Masks	11
Planning IP Addressing.....	15
Lab B: Identifying Valid IP Addresses	19
Assigning TCP/IP Addresses.....	20
Lab C: Examining the Configuration of TCP/IP.....	25
Review	32
Course Evaluation.....	34

Module 8: Optimizing IP Address Allocation

Overview	1
Classless Inter-Domain Routing (CIDR)	2
Binary IP Addresses.....	5
Lab A: Using Windows Calculator to Convert Decimal and Binary Numbers	10
Binary Subnet Masks	18
Lab B: Determining Local and Remote Destinations	27
IP Address Allocation Using CIDR.....	28
Lab C: Allocating IP Addresses.....	33
Review	37

Module 9: Examining Web Services

Overview.....	1
Identifying Internet Concepts.....	2
Using Client Technologies.....	9
Lab A: Accessing an FTP Site by Using Internet Explorer	17
Connecting to the Internet.....	19
Identifying Web Server Concepts.....	25
Lab B: Identifying Web Concepts	29
Review	30
Course Evaluation.....	32

About This Course

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

Description

Course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*, introduces students to the Microsoft Windows 2000 operating system and the networking technologies it supports. Students will be able to describe the principal features of Windows 2000 and the basics of networking with Windows 2000; describe the types of user accounts and the principal security features of a Windows 2000 network; identify the tools used to perform various administrative tasks; describe the features of the common protocols used in a Windows 2000 network; describe the fundamentals of TCP/IP, including name resolution, routing, and IP addressing—classful versus Classless Inter-Domain Routing (CIDR); describe the network communication models used in a Windows 2000 network; differentiate between the various types of network architectures; describe the common physical components used for network communication; describe the concepts and protocols for remote access communication; and describe the client and server technologies used in accessing Web services.

Audience

This three-day course is intended for a broad range of computer professionals who are new to network computing environments and whose goal is to administer or support Windows 2000 networks. This is an introductory course designed to provide an overview of networking concepts, and how they are implemented in Windows 2000. The course provides students with the prerequisite knowledge and skills required for Course 2152A, *Supporting Microsoft Windows 2000 Professional and Server*.

Student Prerequisites

This course requires that students meet the following prerequisites:

- Proficiency using the Windows interface to locate, create, and manipulate folders and files and to configure the desktop environment
- General knowledge of computer hardware components, including memory, hard disks, and CPUs
- General knowledge of networking concepts, including network operating system, server-client relationship, and local area network (LAN)

Course Objectives

Upon successful completion of *Microsoft Windows 2000 Network and Operating System Essentials*, the student will be familiar with networking and operating system concepts and the common tasks required to administer and support the Windows 2000 operating system in a network environment. The student will be able to:

- Describe the principal features of the Windows 2000 operating system and the basics of networking using Windows 2000.
- Identify the tools used to perform common administrative tasks.
- Describe the types of user accounts and the principal security features of Windows 2000.
- Describe the features of the common network protocols used in Windows 2000.
- Describe the fundamentals of TCP/IP.
- Describe the communication process in a Windows 2000 network.
- Differentiate between the various types of network architectures.
- Describe the common hardware components used in network communication.
- Describe the requirements for Internet access and Web security.

Course Timing

The following schedule is an estimate of the course timing. Your timing may vary.

Day 1

Start	End	Module
9:00	9:30	Introduction
9:30	10:15	Module 1: Introduction to Windows 2000 and Networking
10:15	10:30	Lab A: Identifying Computer Networks
		Break
10:45	11:15	Module 1: Introduction to Windows 2000 and Networking (<i>continued</i>)
11:15	11:30	Lab B: Identifying Features of a Windows 2000 Network
11:30	11:45	Lab C: Logging On to Windows 2000
		Lunch
12:45	1:15	Module 2: Administration of a Windows 2000 Network
1:15	1:30	Lab A: Using Windows 2000 Help
1:30	2:30	Module 2: Administration of a Windows 2000 Network (<i>continued</i>)
2:30	2:45	Lab B: Identifying Administrative Tools
		Break
3:00	3:15	Module 3: Securing a Windows 2000 Network
3:15	3:30	Lab A: Examining Users and Groups
3:30	3:45	Module 3: Securing a Windows 2000 Network (<i>continued</i>)
3:45	4:00	Lab B: Examining User Rights
4:00	4:30	Module 3: Securing a Windows 2000 Network (<i>continued</i>)
4:30	4:45	Lab C: Examining File and Folder Permissions

Day 2

Start	End	Module
9:00	9:30	Day 1 review
9:30	10:30	Module 4: Examining the Network
		Break
10:45	11:45	Module 4: Examining the Network (<i>continued</i>)
11:45	12:15	Lab A: Examining the Network Architecture
		Lunch
1:15	2:00	Module 5: Examining Network Protocols
2:00	2:15	Lab A: Identifying Protocol Capabilities
2:15	3:15	Module 6: Examining TCP/IP
		Break
3:30	3:45	Lab A: Using TCP/IP Utilities
3:45	4:30	Module 6: Examining TCP/IP (<i>continued</i>)
4:30	4:45	Lab B: Identifying Processes and Protocols in TCP/IP

Day 3

Start	End	Module
9:00	9:15	Day 2 review
9:15	9:45	Module 7: Examining IP Addressing
9:45	10:00	Lab A: Determining Class Addresses and Subnet Masks
10:00	10:15	Module 7: Examining IP Addressing (<i>continued</i>)
		Break
10:30	11:00	Lab B: Identifying Valid IP Addresses
11:00	11:15	Module 7: Examining IP Addressing (<i>continued</i>)
11:15	11:30	Lab C: Examining the Configuration of TCP/IP
		Lunch
12:30	1:30	Module 8: Optimizing IP Address Allocation
1:30	1:45	Lab A: Using Windows Calculator to Convert Decimal and Binary Numbers
1:45	2:15	Module 8: Optimizing IP Address Allocation (<i>continued</i>)
2:15	2:45	Lab B: Determining Local and Remote Destinations
		Break
3:00	3:30	Module 8: Optimizing IP Address Allocation (<i>continued</i>)
3:30	3:45	Lab C: Allocating IP Addresses
3:45	4:15	Module 9: Examining Web Services
4:15	4:30	Lab A: Accessing an FTP Site by Using Internet Explorer
4:30	4:45	Module 9: Examining Web Services
4:45	5:00	Lab B: Identifying Web Concepts

Trainer Materials Compact Disc Contents

The Trainer Materials compact disc contains the following files and folders:

- *Default.htm*. This file opens the Trainer Materials Web page.
- *Readme.txt*. This file contains a description of the compact disc contents and setup instructions in ASCII format (non-Microsoft Word document).
- *2151a_sg.doc*. This file is the Classroom Setup Guide. It contains a description of classroom requirements, classroom configuration, and classroom setup instructions.
- *Errorlog*. This folder contains a template that is used to record any errors that you find in the course and additions or corrections you want to make.
- *Fonts*. This folder contains fonts that are required to view the Microsoft PowerPoint® presentation and Web-based materials.
- *Mplayer*. This folder contains files that are required to install Microsoft Windows Media Player.
- *Powerpnt*. This folder contains the PowerPoint slides that are used in this course.
- *Pptview*. This folder contains the PowerPoint Viewer, which is used to display the PowerPoint slides.
- *Studntcd*. This folder contains the Web page that provides students with links to resources pertaining to this course, including additional reading, review and lab answers, lab files, multimedia presentations, and course-related Web sites.
- *Tprep*. This folder contains the Trainer Preparation Presentation, a narrated slide show that explains the instructional strategy for the course and presentation tips and caveats. To open the presentation, on the Trainer Materials Web page, click **Trainer Preparation Presentation**.

Student Materials Compact Disc Contents

The Student Materials compact disc contains the following files and folders:

- *Default.htm*. This file opens the Student Materials Web page. It provides students with resources pertaining to this course, including additional reading, review and lab answers, lab files, multimedia presentations, and course-related Web sites.
- *Readme.txt*. This file contains a description of the compact disc contents and setup instructions in ASCII format (non-Microsoft Word document).
- *AddRead*. This folder contains additional reading pertaining to this course. If there are no additional reading files, this folder does not appear.
- *Answers*. This folder contains answers to the module review questions and hands-on labs.
- *Appendix*. This folder contains appendix files for this course. If there are no appendix files, this folder does not appear.
- *Fonts*. This folder contains fonts that are required to view the PowerPoint presentation and Web-based materials.
- *Labfiles*. This folder contains files that are used in the hands-on labs. These files may be used to prepare the student computers for the hands-on labs.
- *Media*. This folder contains files that are used in multimedia presentations for this course. If this course does not include any multimedia presentations, this folder does not appear.
- *Mplayer*. This folder contains files that are required to install Microsoft Windows Media Player.
- *Pptview*. This folder contains the PowerPoint Viewer, which is used to display the PowerPoint presentations that accompany the additional reading. If there are no PowerPoint presentations, this folder does not appear.
- *Webfiles*. This folder contains the files that are required to view the course Web page. To open the Web page, open Windows Explorer, and in the root directory of the compact disc, double-click **Default.htm**.
- *Wordview*. This folder contains the Word Viewer that is used to view any Word document (.doc) files that are included on the compact disc. If no Word documents are included, this folder does not appear.

Document Conventions

The following conventions are used in course materials to distinguish elements of the text.

Convention	Use
◆	Indicates an introductory page. This symbol appears next to a slide title when additional information on the topic is covered on the page or pages that follow it.
bold	Represents commands, command options, and portions of syntax that must be typed exactly as shown. It also indicates commands on menus and buttons, icons, dialog box titles and options, and icon and menu names.
<i>italic</i>	In syntax statements, indicates placeholders for variable information. Italic is also used for introducing new terms, for book titles, and for emphasis in the text.
Title Capitals	Indicate domain names, user names, computer names, directory names, folders, and file names, except when specifically referring to case-sensitive names. Unless otherwise indicated, you can use lowercase letters when you type a directory name or file name in a dialog box or at a command prompt.
ALL CAPITALS	Indicate the names of keys, key sequences, and key combinations—for example, ALT+SPACEBAR.
monospace	Represents code samples, examples of screen text, or entries that you type at a command prompt or in initialization files.
[]	In syntax statements, enclose optional items. For example, <i>[filename]</i> in command syntax indicates that you can choose to type a file name with the command. Type only the information within the brackets, not the brackets themselves.
{ }	In syntax statements, enclose required items. Type only the information within the braces, not the braces themselves.
	In syntax statements, separates an either/or choice.
►	Indicates a procedure with sequential steps.
...	In syntax statements, specifies that the preceding item may be repeated.
.	Represents an omitted portion of a code sample.
.	
.	

Introduction

Contents

Introduction	1
Course Materials	2
Prerequisites	3
Course Outline	4
Microsoft Official Curriculum	7
Microsoft Certified Professional Program	8
Facilities	10



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
30 Minutes

The Introduction module provides students with an overview of the course content, materials, and logistics for Course 2151A: *Microsoft Windows 2000 Network and Operating System Essentials*.

Course Materials and Preparation

Required Materials

To teach this course, you need the following materials:

- Delivery Guide
- Trainer Materials compact disc

Preparation Tasks

To prepare for this course, you must:

- Complete the Course Preparation Checklist that is included with the trainer course materials.

Module Strategy

Use the following strategy to present this module:

- Course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*

Show the slide that displays the course number and course title.

- Introduction

Welcome students to the course and introduce yourself. Provide a brief overview of your background to establish credibility.

Have students introduce themselves and provide their background, product experience, and expectations of the course.

Record student expectations on a whiteboard or flip chart to which you can refer later in the class.

- Course Materials

Explain the purpose of all materials used in this course.

Tell students that they will have an opportunity at the end of the class to provide feedback on the course and facilities by using the Microsoft Online Evaluation System.

- Prerequisites

Provide the students with the list of prerequisites that they should have met before taking this course. This is an opportunity for you to identify students who may not have the appropriate background or experience to attend this course.

- Course Outline

Provide an overview of each module and what students will learn.

Explain how this course will meet students' expectations by describing the information covered in individual modules.

- Microsoft Certified Professional Program

Inform students about the Microsoft Certified Professional (MCP) program and the various certification options.

- Microsoft Official Curriculum

Inform students about the Microsoft Official Curriculum program and refer them to the Microsoft Official Curriculum Web page at <http://www.microsoft.com/traincert/moc/>

- Facilities

Explain the facility information for the training site.

Introduction

Topic Objective

To introduce yourself, establish credibility, meet students, and set student expectations for the course.

Lead-in

Good morning. Welcome to *Microsoft Windows 2000 Network and Operating System Essentials*.

My name is...

- Name
- Company Affiliation
- Title/Function
- Job Responsibility
- Networking Experience
- Operating System Experience
- Expectations for the Course

*****ILLEGAL FOR NON-TRAINER USE*****

Introduce yourself.

Provide a brief overview of your background to establish credibility as a *Microsoft Windows 2000 Network and Operating System Essentials* instructor.

Ask students to introduce themselves, addressing the bulleted items on the slide.

Delivery Tip

As students introduce themselves, use a white board or flip chart to record their expectations of the course.

Course Materials

Topic Objective

To identify and describe the course materials.

Lead-in

We have provided everything you need for this course. You will find the following materials at your desk...

- **Name Card**
- **Student Workbook**
- **Student Materials Compact Disc**
- **Course Evaluation**

*****ILLEGAL FOR NON-TRAINER USE*****

Describe the contents of the student workbook and the Student Materials compact disc.

Have students write their names on both sides of the name card.

Tell students that a course evaluation must be completed at the end of the course.

Tell students where they can send comments.

Delivery Tip

Demonstrate how to open the Web page provided on the Student Materials compact disc. On the Trainer Materials compact disc, double-click **Default.htm** in the StudntCD folder.

The following materials are included with your kit:

- *Name card.* Write your name on both sides of the name card.
- *Student workbook.* The student workbook contains the material covered in class, in addition to the hands-on lab exercises.
- *Student Materials compact disc.* The Student Materials compact disc contains the Web page that provides students with links to resources pertaining to this course, including additional readings, review and lab answers, lab files, multimedia presentations, and course-related Web sites.

Note To open the Web page, insert the Student Materials compact disc into the CD-ROM drive, and then in the root directory of the compact disc, double-click **Default.htm**.

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

To provide additional comments or inquire about the Microsoft Certified Professional program, send e-mail to mcphep@microsoft.com.

Prerequisites

Topic Objective

To present and describe the prerequisites for this course.

Lead-in

The following prerequisite knowledge is needed for this course.

- Proficiency Using the Windows Interface
- General Knowledge of Computer Hardware
- General Knowledge of Networking Concepts

*****ILLEGAL FOR NON-TRAINER USE*****

This course requires that you meet the following prerequisites:

- Proficiency using the Microsoft® Windows® interface to configure the desktop environment and to locate, create, and manipulate folders and files
- General knowledge of computer hardware components, including memory, hard disks, and CPUs
- General knowledge of networking concepts, including network operating system, client/server relationship, and local area network (LAN)

Course Outline

Topic Objective

To provide an overview of each module and what students will learn.

Lead-in

In this course, we will examine Windows 2000 and how it functions in a network.

- **Module 1: Introduction to Windows 2000 and Networking**
- **Module 2: Administration of a Windows 2000 Network**
- **Module 3: Securing a Windows 2000 Network**
- **Module 4: Examining the Network**
- **Module 5: Examining Network Protocols**

*****ILLEGAL FOR NON-TRAINER USE*****

Briefly describe each module.

As you describe each module, acknowledge any information that will meet the student expectations that you recorded earlier.

Module 1, “Introduction to Windows 2000 and Networking,” explains networking concepts and describes how Windows 2000 and networking are combined. The module introduces the concept of a domain and describes the implementation of Microsoft Windows 2000 Directory Services with Active Directory™ directory service. At the end of this module, you will be able to identify the features of the Windows 2000 operating systems and describe the different types of networks and network operating systems.

Module 2, “Administration of a Windows 2000 Network,” describes routine tasks that you must perform to maintain a network. The module introduces Windows 2000 Help, which provides instructions for performing many tasks. The first part of the module explains how to search Windows 2000 Help for information and how to bookmark information that you regularly access. Control Panel is introduced as the main point of access for the various administrative tools. At the end of this module, you will be able to use Windows 2000 Help as an administrative resource and describe the tools used to perform routine administrative tasks.

Module 3, “Securing a Windows 2000 Network,” describes how administrators can secure access to a network. The module describes user accounts as a means for implementing network security. The module also explains the local and domain user categories and how user accounts in these categories are further divided into user-defined accounts and built-in user accounts. The module describes the role of user rights and permissions in controlling access to network resources and how to set permissions on shared resources to ensure that only authorized users have access. At the end of this module, you will be able to identify types of user accounts, describe the different types of groups, describe user rights, and verify permissions to printers and folders.

Module 4, “Examining the Network,” describes network components, including the cables and the communication tools that are used to build the network. The module describes the network *topologies*, or designs, that support the administrative and organizational structures of an organization. It also identifies the network components that allow for expansion of a network, including the components required for remote access to a network. At the end of this module, you will be able to describe the components and scope of a network and identify current network topologies and related technologies.

Module 5, “Examining Network Protocols,” describes the *protocols*, or sets of standards, designed to enable computers to connect with one another and to exchange information. The module describes the characteristics of the protocols available today and their compatibility with Windows 2000. At the end of this module, you will be able to identify the common protocols and describe their characteristics.

Course Outline (*continued*)

- **Module 6: Examining TCP/IP**
- **Module 7: Examining IP Addressing**
- **Module 8: Optimizing IP Address Allocation**
- **Module 9: Examining Web Services**

*****ILLEGAL FOR NON-TRAINER USE*****

Module 6, “Examining TCP/IP,” describes the TCP/IP protocol suite that enables enterprise networking and connectivity on Windows 2000-based computers. The module describes how TCP/IP provides a technology for connecting dissimilar systems in a client/server framework and provides a foundation for access to global Internet services and e-mail. At the end of this module, you will be able to describe the TCP/IP communication process, including the protocols in the TCP/IP protocol stack, and you will be able to describe the process for resolving computer names to IP addresses.

Module 7, “Examining IP Addressing,” describes the primary function of the Internet Protocol (IP): to add address information to a data packet before it is sent across a network. To understand the procedure used by IP, you should be familiar with the process of determining the addresses of the intermediate and final destinations of the data. At the end of this module, you will be able to describe the rules that identify hosts in a network and describe the IP address classes. You will be able to describe issues in planning an IP address and describe the procedure used to assign an IP address.

Module 8, “Optimizing IP Address Allocation,” describes the binary notation system used for designating IP addresses, by which computers in a network are identified. The module also describes Classless Inter-Domain Routing (CIDR), which is an efficient method of IP address allocation. At the end of this module, you will be able to convert IP addresses from decimal format to binary format, calculate the network ID of an IP address represented in CIDR notation, and describe IP address allocation using CIDR.

Module 9, “Examining Web Services,” describes the services provided by Windows 2000 to support large internetworks, including the Internet. The module introduces basic concepts and terminologies of Web services and describes the methods of connecting and securing access to the Internet, including the server technologies for providing information on the Internet. At the end of this module, you will be able to describe internetworking technologies and explain how to securely connect to the Internet.

Microsoft Official Curriculum

Topic Objective

To explain the Microsoft Official Curriculum program and provide information about curriculum paths.

Lead-in

Let's briefly talk about the Microsoft Official Curriculum program.

Microsoft Official Curriculum

- Microsoft Windows Operating Systems
- Microsoft Office
- Microsoft BackOffice Small Business Server
- Microsoft SQL Server
- Microsoft Exchange
- Microsoft BackOffice Server Infrastructure and Solutions
- Microsoft FrontPage
- Microsoft Systems Management Server
- Knowledge Management Solutions

*****ILLEGAL FOR NON-TRAINER USE*****

Microsoft® Official Curriculum (MOC) is hands-on facilitated classroom and Web-based training. Microsoft develops skills-based training courses to educate computer professionals who develop, support, and implement solutions by using Microsoft products, solutions, and technologies. MOC courses are available for the following products and solutions:

- Microsoft Windows® operating systems
- Microsoft Office
- Microsoft BackOffice® Small Business Server
- Microsoft SQL Server™
- Microsoft Exchange
- Microsoft BackOffice Server Infrastructure and Solutions
- Microsoft FrontPage®
- Microsoft Systems Management Server
- Knowledge Management Solutions

MOC provides a curriculum path for each product and solution. For more information on the curriculum paths, see the Microsoft Official Curriculum Web page at <http://www.microsoft.com/traincert/moc/>

The Microsoft Official Curriculum Web page provides information about MOC courses. In addition, you can find recommended curriculum paths for individuals who are entering the Information Technology (IT) industry, who are continuing their training on Microsoft products and solutions, or who currently support non-Microsoft products.

Microsoft Certified Professional Program

Topic Objective

To provide students with information about the Microsoft Certified Professional Program.

Lead-in

The Microsoft Certified Professional Program includes these certifications.



*****ILLEGAL FOR NON-TRAINER USE*****

The Microsoft Certified Professional program is a leading certification program that validates your experience and skills to keep you competitive in today's changing business environment. The following table describes each certification in more detail.

Certification	Description
MCSA on Microsoft Windows 2000	The Microsoft Certified Systems Administrator (MCSA) certification is designed for professionals who implement, manage, and troubleshoot existing network and system environments based on Microsoft Windows 2000 platforms, including the Windows .NET Server family. Implementation responsibilities include installing and configuring parts of the systems. Management responsibilities include administering and supporting the systems.
MCSE on Microsoft Windows 2000	The Microsoft Certified Systems Engineer (MCSE) credential is the premier certification for professionals who analyze the business requirements and design and implement the infrastructure for business solutions based on the Microsoft Windows 2000 platform and Microsoft server software, including the Windows .NET Server family. Implementation responsibilities include installing, configuring, and troubleshooting network systems.
MCSD	The Microsoft Certified Solution Developer (MCSD) credential is the premier certification for professionals who design and develop leading-edge business solutions with Microsoft development tools, technologies, platforms, and the Microsoft Windows DNA architecture. The types of applications MCSDs can develop include desktop applications and multi-user, Web-based, N-tier, and transaction-based applications. The credential covers job tasks ranging from analyzing business requirements to maintaining solutions.
MCDBA on Microsoft SQL Server 2000	The Microsoft Certified Database Administrator (MCDBA) credential is the premier certification for professionals who implement and administer Microsoft SQL Server databases. The certification is appropriate for individuals who derive physical database designs, develop logical data models, create physical databases, create data services by using Transact-SQL, manage and maintain databases, configure and manage security, monitor and optimize databases, and install and configure SQL Server.

(continued)

Certification	Description
MCP	The Microsoft Certified Professional (MCP) credential is for individuals who have the skills to successfully implement a Microsoft product or technology as part of a business solution in an organization. Hands-on experience with the product is necessary to successfully achieve certification.
MCT	Microsoft Certified Trainers (MCTs) demonstrate the instructional and technical skills that qualify them to deliver Microsoft Official Curriculum through Microsoft Certified Technical Education Centers (Microsoft CTECs).

Certification Requirements

The certification requirements differ for each certification category and are specific to the products and job functions addressed by the certification. To become a Microsoft Certified Professional, you must pass rigorous certification exams that provide a valid and reliable measure of technical proficiency and expertise.

For More Information See the Microsoft Training and Certification Web site at <http://www.microsoft.com/traincert/>.

You can also send e-mail to mcphelp@microsoft.com if you have specific certification questions.

Acquiring the Skills Tested by an MCP Exam

Microsoft Official Curriculum (MOC) and MSDN® Training Curriculum can help you develop the skills that you need to do your job. They also complement the experience that you gain while working with Microsoft products and technologies. However, no one-to-one correlation exists between MOC and MSDN Training courses and MCP exams. Microsoft does not expect or intend for the courses to be the sole preparation method for passing MCP exams. Practical product knowledge and experience is also necessary to pass the MCP exams.

To help prepare for the MCP exams, use the preparation guides that are available for each exam. Each Exam Preparation Guide contains exam-specific information, such as a list of the topics on which you will be tested. These guides are available on the Microsoft Training and Certification Web site at <http://www.microsoft.com/traincert/>.

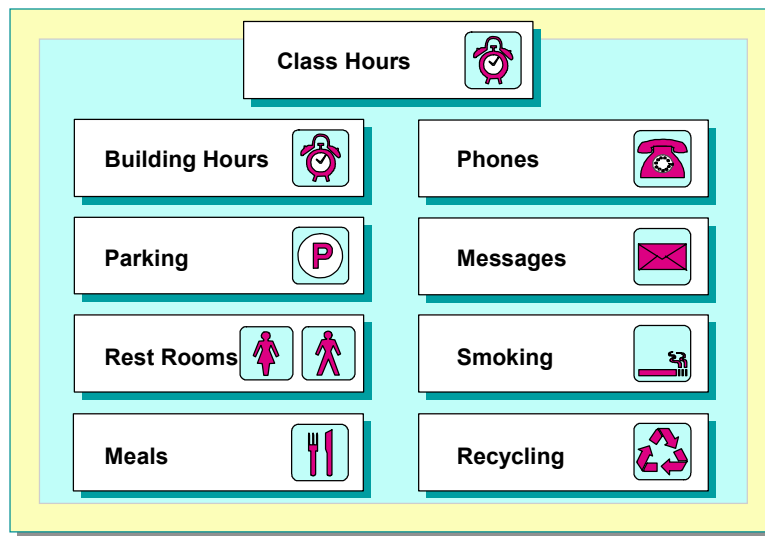
Facilities

Topic Objective

To inform students of class logistics and rules for the training site.

Lead-in

Before we start, let's go over the class logistics.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the class hours, extended building hours for labs, parking, rest room location, meals, phones, message posting, and where smoking is or isn't allowed.

Also make sure that the students are aware of the recycling program if one is available.

Module 1: Introduction to Windows 2000 and Networking

Contents

Overview	1
Windows 2000 Operating Systems	2
Introduction to Networks	8
Lab A: Identifying Computer Networks	15
Windows 2000 Implementation of Networking	16
Lab B: Identifying Features of a Windows 2000 Network	25
Lab C: Logging On to Windows 2000	26
Review	29



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

Labs:
45 Minutes

This module provides students with an overview of the Microsoft® Windows® 2000 operating system and how it implements networking. The students learn about operating system and networking concepts as well as the features of Windows 2000. Then the module introduces networking concepts, the types of networks, and the functions of a network operating system. This section is followed by a lab in which the students distinguish between the different types of networks and identify the capabilities and limitations of some types of networks.

The contents of the first two sections are then applied in explaining how Windows 2000 implements networking. The concepts of authentication, domains, and Microsoft Active Directory™ directory services are introduced and explained. Two labs follow this section. In the first lab, students identify the benefits of a domain and the components of Active Directory. In the second lab, the students log on to Windows 2000 and determine whether their computer belongs to a workgroup or domain.

At the end of this module, students will be able to:

- Describe the features of the Windows 2000 operating system and its different versions.
- Define different networks and describe their advantages.
- Describe how Windows 2000 implements networking.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_01.ppt
- Module 1, “Introduction to Windows 2000 and Networking”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the three labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Windows 2000 Operating Systems**
Introduce the need for an operating system and the functions it performs. Then explain the features of the Windows 2000 operating system and end the section by explaining the characteristics of the four versions of Windows 2000.
- **Introduction to Networks**
Provide an overview of the need for networking and its benefits. Then explain the roles of clients and different types of servers in a network. Discuss the different types of networks next, followed by the features of a network operating system.
- **Windows 2000 Implementation of Networking**
Explain how Windows 2000 provides enhanced networking capabilities. Introduce the concept of domains and explain the features and benefits of a domain. Then introduce Active Directory and describe its features and benefits. Conclude by discussing the mandatory logon feature and the procedure for logging on to Windows 2000.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about basic operating system and networking concepts.

- Windows 2000 Operating Systems
- Introduction to Networks
- Windows 2000 Implementation of Networking

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use this page to introduce the need for the course and describe the major sections in it.

Key Points

The operating system provides an environment for running applications. A network connects multiple computers and peripherals to enable sharing of data and resources.

The fundamental core of a computer is its operating system: the software that controls its hardware. As its name suggests, the operating system operates the computer. It loads applications into the computer's memory, runs these applications, and manages peripheral devices, such as disks and printers.

A computer environment that consists of multiple computers and printers can be connected together to exchange data and information. Such a group of connected computers and devices is called a network.

Coordinating the numerous applications that run simultaneously on a network and managing the various peripheral devices attached to a network requires additional support. The network operating system provides this support in the form of networking features. Microsoft® Windows® 2000 is a new generation network operating system that provides improved infrastructure, management, and application support to network users and organizations.

At the end of this module, you will be able to:

- Describe the features of the Windows 2000 operating system and its different versions.
- Define a network and describe its advantages.
- Describe how Windows 2000 implements networking.

◆ Windows 2000 Operating Systems

Topic Objective

To introduce topics related to the Windows 2000 operating system.

Lead-in

Windows 2000 is a robust operating system with a number of useful features.

- Operating System Functions
- Features of Windows 2000
- Versions of Windows 2000

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 provides an array of tools to assist the network administrator in simplifying day-to-day administrative tasks and in configuring client computers. Windows 2000 provides advanced capabilities for automating many of these tasks, thus decreasing overhead costs. The Windows 2000 operating system family consists of the following versions:

- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

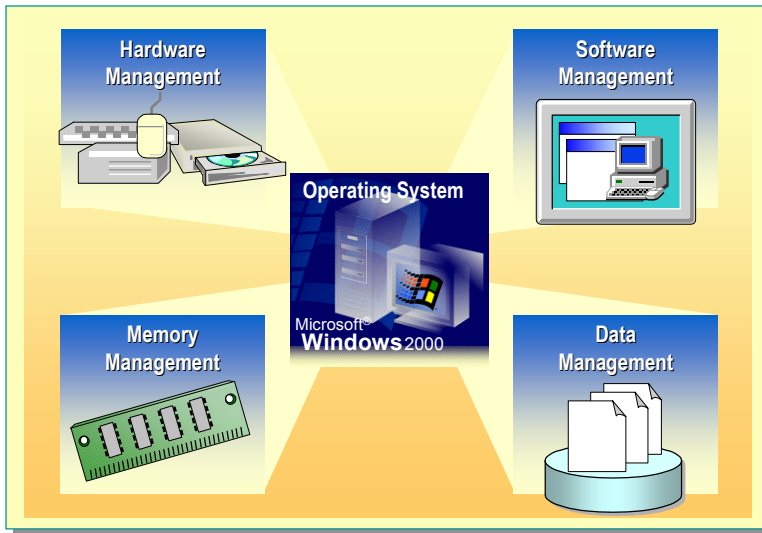
Operating System Functions

Topic Objective

To illustrate the functions of an operating system.

Lead-in

An operating system serves as the bridge between the software you use and the hardware with which you interact.



*****ILLEGAL FOR NON-TRAINER USE*****

An operating system is software that provides the means for applications to interact with the computer's hardware. An operating system manages four key aspects of a computer's operation: hardware management, software management, memory management, and data management.

- **Hardware management**

The operating system enables the computer to communicate with peripheral devices, such as a printer or a mouse.

- **Software management**

The operating system provides a mechanism for initiating processes that include programs, such as Microsoft Word and Microsoft PowerPoint®.

- **Memory management**

The operating system allocates memory to each application, without affecting the memory used by other applications.

- **Data management**

The operating system manages files stored on hard disks and other mass-storage devices. The operating system enables applications to create and open files, transfer data between devices, and perform such file-management tasks as renaming and deleting.

The operating system coordinates the interaction between the computer and applications that run on it. It controls the flow of data within the computer and provides the graphical user interface (GUI), a means of interacting with the computer. The GUI provides an intuitive graphical way of issuing commands to the system, as compared to a text-based environment.

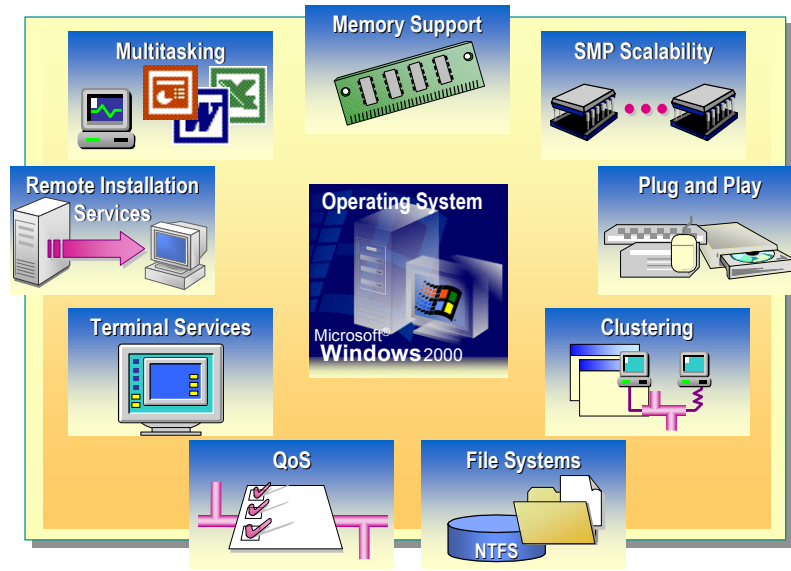
Features of Windows 2000

Topic Objective

To illustrate the features of the Windows 2000 operating system.

Lead-in

Windows 2000 has many features that enhance its functionality.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

If the level of the class permits, define the features provided by the NTFS file system at a high level. You do not need to explain the features in detail and you can refer the students to **Additional Reading** for more information.

The Windows 2000 operating system provides many enhanced features for its users. These features include multitasking, memory support, symmetric multiprocessing, Plug and Play, clustering, NTFS, Quality of Service, Terminal Services and Remote Installation Services.

Multitasking

Multitasking enables users to run multiple applications simultaneously on the same system. The number of applications that a user can run simultaneously and the system performance when running them depends on the amount of memory in the system.

Memory Support

To function, each application that runs on Windows 2000 requires a certain amount of memory. In order to support multiple applications running simultaneously (multitasking) and applications with large requirements for memory, Windows 2000 provides support for up to 64 gigabytes (GB) of memory.

Symmetric Multiprocessing (SMP) Scalability

Symmetric multiprocessing (SMP) is a technology that allows an operating system to use multiple processors simultaneously to improve performance by reducing transaction time. Depending on the version, Windows 2000 provides SMP support for up to 32 processors.

Plug and Play

With Windows 2000, it is easy to install a Plug and Play device. This is a device that you plug in and use immediately without having to perform a complicated setup process. After you plug in such a device, Windows 2000 automatically identifies the added component and completes the configuration.

Clustering

Windows 2000 provides the ability to group independent computers together to run a common set of applications. This grouping appears as a single system to the client and application. Such a grouping is called clustering, and the groups of computers are called clusters. This arrangement of computers avoids a single point of failure. If one computer fails, another computer in the cluster provides the same services in its place.

File System Features

The NTFS file system is the recommended file system for use with Windows 2000. Windows 2000 provides the following features through NTFS support:

- File system recovery
- Large partition size
- Security
- Disk quotas
- Compression

Note You can also use the FAT (file allocation table) and FAT32 file systems with Windows 2000. For more information about the NTFS, FAT, and FAT32 file systems, please see *File and Print Services Technical Overview* under **Additional Reading** on the Web page on the Student Materials compact disc.

Quality of Service (QoS)

In Windows 2000, Quality of Service (QoS) is a set of service requirements that the network must meet to ensure an adequate service level for data transmission. Using QoS, you can control how network bandwidth is allocated to applications. QoS provides a guaranteed, end-to-end, express delivery system for information across the network.

Terminal Services

Terminal Services provides remote access to a server desktop through a *terminal emulator*. A terminal emulator is an application that lets you access a remote computer as though you were physically located at it. Using Terminal Services, you can run client applications on the server so that client computers function as terminals rather than as independent systems.

By using Terminal Services, you can reduce the total cost of operation of your network. You can distribute Windows-based applications to client computers that might not normally be able to run Windows. You can also use Terminal Services to administer your server from anywhere on the network.

Remote Installation Services

Remote Installation Services (RIS) enables an administrator to deploy an operating system throughout the organization, without needing to physically visit each client computer. RIS is an optional component that is available as part of the Microsoft Windows 2000 Server operating system.

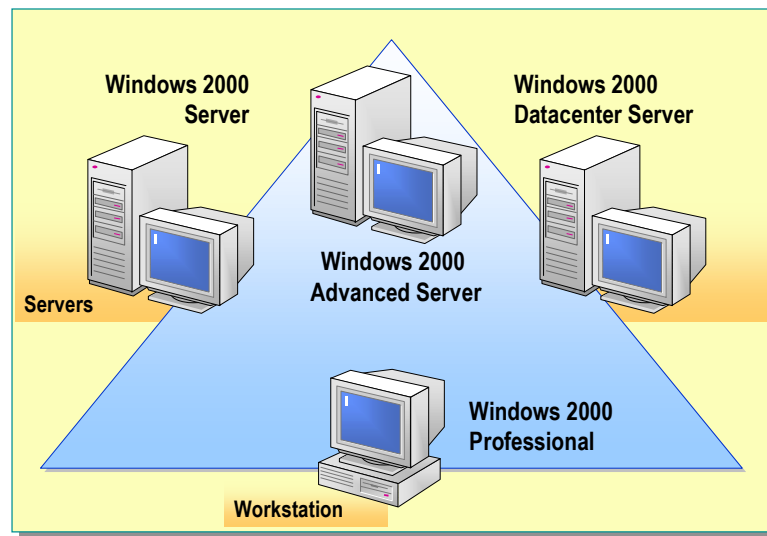
Versions of Windows 2000

Topic Objective

To illustrate the four versions of Windows 2000.

Lead-in

The Windows 2000 operating systems include four members: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server.



*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 consists of four operating systems: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, and Windows 2000 Datacenter Server.

Windows 2000 Professional

Windows 2000 Professional is a desktop operating system that incorporates the best business features of Microsoft Windows 98 and builds on the traditional strengths of Microsoft Windows NT® version 4.0. Windows 2000 Professional includes a simplified user interface, improved Plug and Play functionality, power management, and support for a broad range of hardware devices. It supports SMP systems with two processors and 4 GB of physical memory.

Windows 2000 Server

Windows 2000 Server is the standard edition of the Windows 2000 server family. It contains all the features of Windows 2000 Professional and is ideal for small to medium-sized organizations. This version of Windows 2000 works well for file and print servers, Web servers, and workgroups. Windows 2000 Server supports SMP systems with four processors and 4 GB of physical memory.

Windows 2000 Advanced Server

Windows 2000 Advanced Server contains all of the functionality of Windows 2000 Server, plus increased scalability and system availability. Scalability is the ability to increase processing power incrementally to meet increased network demands. This functionality is provided through clusters of multiple servers. These servers provide additional processing power, thereby increasing system availability. This way, if one server becomes unavailable, the other servers in the cluster provide the requested service.

Windows 2000 Advanced Server is designed for servers that are used in large-scale networks and for database-intensive work. Windows 2000 Advanced Server supports SMP systems with eight processors and 8 GB of physical memory.

Windows 2000 Datacenter Server

Windows 2000 Datacenter Server contains all of the functionality of Windows 2000 Advanced Server, plus support for additional memory and CPUs per computer. It is designed for large data warehouses, online transaction processing, and large-scale simulations. It can also support more than 10,000 simultaneous users in certain workloads. Windows 2000 Datacenter Server supports SMP systems with 32 processors and 64 GB of physical memory.

◆ Introduction to Networks

Topic Objective

To introduce the basic concepts of networking.

Lead-in

Members of a group need to be able to share information if they are to work together effectively. They can share information by connecting their computers to form a network.

- **Networking Benefits**
- **Roles of Computers in a Network**
- **Types of Networks**
- **Network Operating Systems**

*****ILLEGAL FOR NON-TRAINER USE*****

Consider a situation in which many employees in an organization need to work with the same data. A copy of the data can be loaded on each computer so that the employees can access the data individually. However, a more efficient method is to load the data on one computer and provide the other computers access to the data from this computer remotely. This option saves disk space on the computers and provides a central location for storing and managing the data that multiple users need to access.

This need to share data and resources led to the development of networking. A network is a group of connected computers that allows people to share information. In a network, multiple users can access the same information and connect to the same resource. For example, instead of linking each computer to its own printer, all computers can be linked to a common printer for shared access by multiple users. In this section, you will learn about the basic concepts of networking.

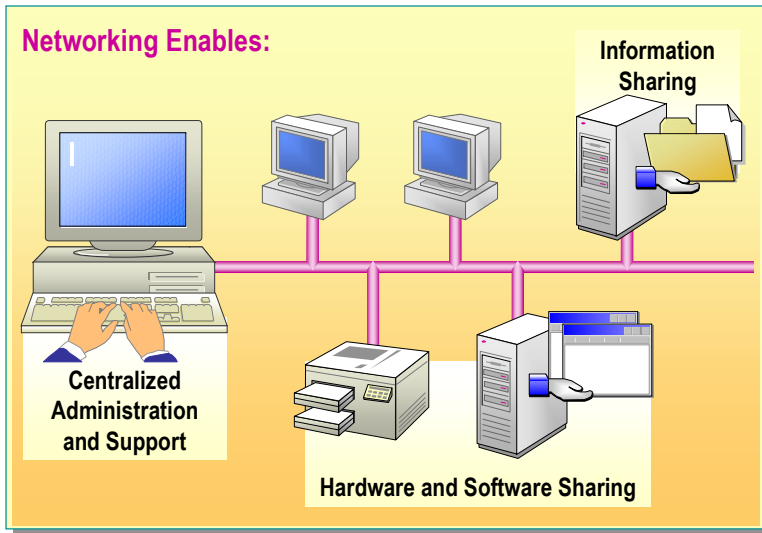
Networking Benefits

Topic Objective

To illustrate the benefits of a network.

Lead-in

A network is a group of computers that are interconnected.



*****ILLEGAL FOR NON-TRAINER USE*****

Linking computers into networks provides benefits in the following areas: information sharing, hardware and software sharing, and administrative support. These benefits help increase productivity.

- Information sharing

The ability to share information and data quickly and inexpensively is one of the popular benefits of networking technology. Network-based e-mail messages and scheduling are some of the activities for which many organizations use networks today.

- Hardware and software sharing

Before the advent of networks, computer users required their own printers and other peripherals, which is an expensive factor in a large organization. The network revolution reduced these costs drastically by making it possible for several users to share hardware and software simultaneously.

- Centralized administration and support

Networking computers also simplifies administration and support tasks. From just a single location, the network administrator can perform administrative tasks on any computer on the network. Also, it is more efficient for technical personnel to support one version of an operating system or application than to oversee a number of individual and unique systems and setups.

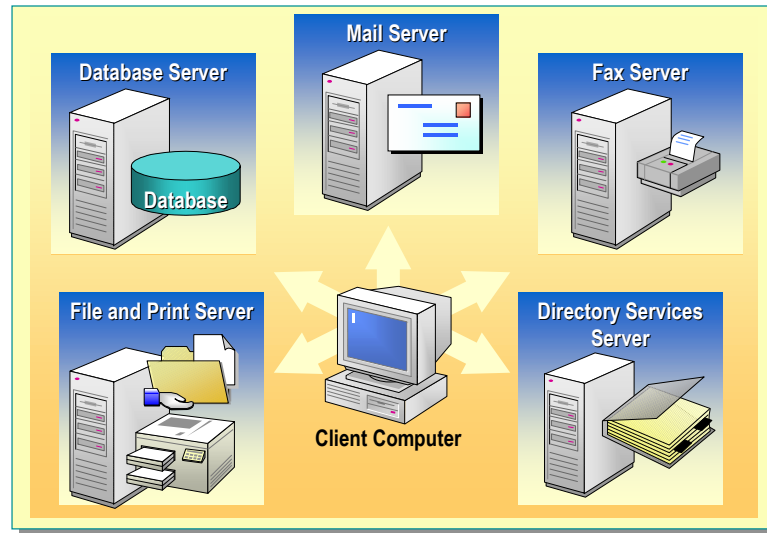
Roles of Computers in a Network

Topic Objective

To illustrate the functions of the two types of computers on a network.

Lead-in

A network consists of two types of computers: clients and servers.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Do not introduce Active Directory while explaining about the directory services servers. Active Directory is introduced later in the module.

Computers in a network function as either clients or servers.

Clients

Client computers (such as the users' computers) make requests for services or data on the network from computers referred to as servers.

Servers

Servers are computers that provide services and data to client computers. The servers in a network perform a variety of complex tasks. Servers for large networks have become specialized to accommodate the expanding needs of users.

The following are some examples of the different types of servers included on many large networks:

File and Print Servers

File and print servers provide file and printer resources from a centralized location. When a client sends a request for data to the file and print server, the entire database or file is downloaded to the computer making the request.

For example, when you open a word-processing application, the application runs on your computer and the document stored on the file and print server is loaded into your computer's memory so that you can edit or use the document locally. Once the document is saved back on the server, anyone on the network who has the proper access, or permission, may look at the file. In other words, file and print servers are used to store and retrieve centralized file and data records.

Database Servers

Database servers can store large amounts of data in a centralized location and make this data available to users so that they do not need to download the entire database. With a database server, the entire database stays on the server and only the results of a request are downloaded to the computer making the request.

For example, you might use a client application that runs locally, such as Microsoft Access, to search an employee database for the names of all employees born in November. The employee database is stored on a database server, such as Microsoft SQL Server™. When the server processes your request, only the result of your query (the list of November birth dates) is downloaded from the server onto your local computer.

Mail Servers

Mail servers operate like database servers in that there are separate server and client applications, with data selectively downloaded from the server to the client. Mail servers manage the e-mail services for the network.

Fax Servers

Fax servers manage fax traffic into and out of the network by sharing one or more fax modems. This makes a fax service available to anyone on the network without having to install a fax machine on everyone's computer.

Directory Services Servers

Directory services servers provide a central location to store information about the network, including the identity of the users accessing the network and the names of the resources available in the network. This enables network security to be administered centrally.

An administrator can define a resource, such as a printer, and the type of access that users have to that resource. After the administrator defines the resource, users can locate the resource and use it, depending on the type of access assigned to them.

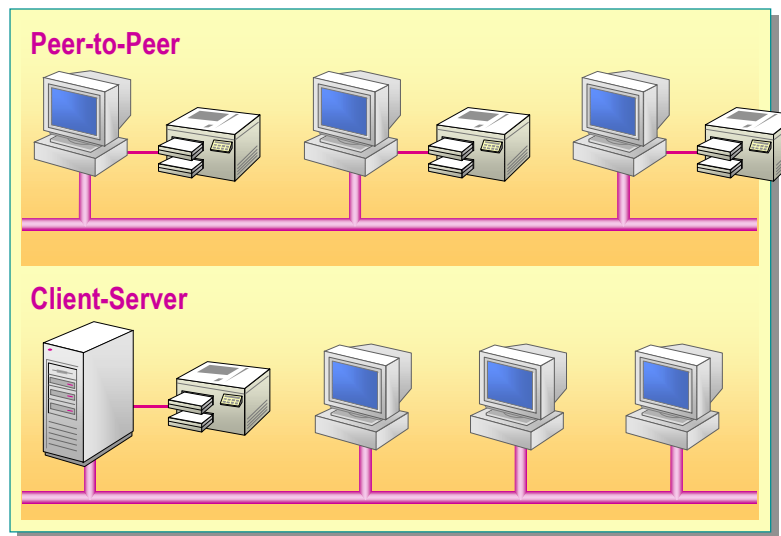
Types of Networks

Topic Objective

To illustrate the two types of networks.

Lead-in

Networks can be broadly classified into two types: peer-to-peer and client-server.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Ensure that students clearly understand the definition of a workgroup.

Based on how the computers in a network are configured and how they access information, networks are classified into two types: peer-to-peer and client-server. Distinctions between the two types of networks are important because each type possesses different capabilities.

Peer-to-Peer Networks

In a peer-to-peer network, there are no dedicated servers, and there is no hierarchy among the computers. All computers are equal and therefore are known as peers. Each computer functions as both a client and a server, and usually no administrator is responsible for maintaining the network. Security is provided by the local directory database on each computer. The user at each computer determines what data on that computer is shared on the network.

Peer-to-peer networks are also called *workgroups*. The term workgroup describes a small group of individuals, typically 10 or fewer, who work together. Peer-to-peer networks are good choices for environments where:

- There are 10 or fewer users.
- Users share resources and printers, but no specialized servers exist.
- Security is not an issue.
- The organization and the network will experience only limited growth within the foreseeable future.

Client-Server Networks

As a network grows, a peer-to-peer network will probably no longer be able to meet the increased demand on shared resources. To accommodate the increased demand and provide additional functionality, most networks have dedicated servers. A dedicated server functions as a server only, not as a client. The configuration of these servers is optimized to process requests from network clients.

Client-server networks have become standard models for networking. As networks increase in size due to the number of connected computers and the physical distance and traffic between them, more than one server is usually needed. Distributing the network tasks among several servers ensures that each task is performed as efficiently as possible. Also, with the servers performing the network tasks, the workload on the individual computers is reduced.

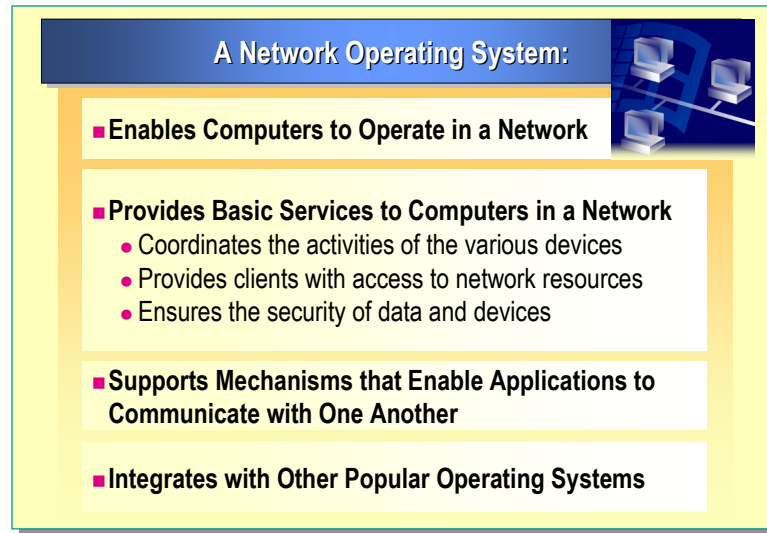
Network Operating Systems

Topic Objective

To describe the features of a network operating system.

Lead-in

The network operating system manages the task of providing network functionality and ensuring the efficient functioning of a network.



*****ILLEGAL FOR NON-TRAINER USE*****

The core of a network is the network operating system. Just as a computer cannot operate without an operating system, a network of computers cannot operate without a network operating system. Every network operating system provides basic services to the computers on its network. These services include:

- Coordinating the activities of the various devices on the network to ensure that communication takes place as and when required.
- Providing clients with access to network resources, including files and such peripheral devices as printers and fax machines.
- Ensuring the security of data and devices on the network.

Features of Network Operating Systems

A network operating system must support mechanisms that enable applications to communicate with one another: for example, applications that enable multiple computers to work jointly on a single task, such as a mathematical calculation. A network operating system must also support multiple processors, clusters of disk drives, and data security features. Finally, a network operating system must be reliable and be able to recover quickly from errors.

Depending upon the network operating system's manufacturer, a desktop computer's networking software can be added either to the computer's own operating system or be integrated with it. Network operating system software is integrated into a number of popular operating systems, including Microsoft Windows 2000, Windows NT, Windows 98, Windows 95, and Apple Macintosh.

Lab A: Identifying Computer Networks

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the types of computer networks.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Distinguish between different types of networks.
- Identify components that are added to the network to provide additional functionality.
- Identify limitations and capabilities of certain types of networks.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors. (16-bit recommended).
- Microsoft Internet Explorer 5 or higher.

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Computer Networks**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 15 minutes

◆ Windows 2000 Implementation of Networking

Topic Objective

To introduce topics related to the implementation of networking by Windows 2000.

Lead-in

Windows 2000 is the new generation of Microsoft network operating systems.

- Features of a Domain
- Benefits of a Domain
- Domain Organization
- Features of Active Directory
- Benefits of Active Directory
- Accessing a Windows 2000 Network

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 serves organizational needs by making it easy to connect people and networks in innovative ways through domain organization and Microsoft Active Directory™ directory service for enhanced communication.

A Windows 2000 network allows organizations to improve information sharing, streamline operations, and create an efficient communications infrastructure. Windows 2000 includes centralized security and information management services. It also provides network communications services through directory-enhanced management and adherence to established networking standards.

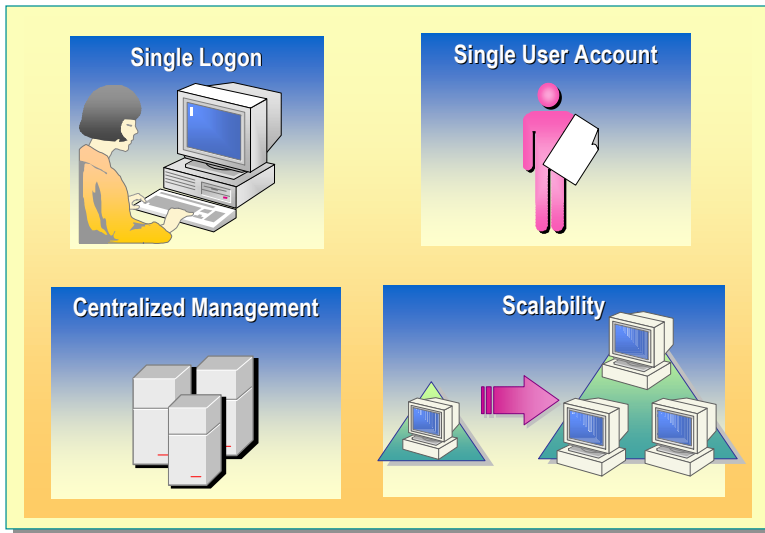
Features of a Domain

Topic Objective

To illustrate the features of a domain.

Lead-in

Windows 2000 manages networks by organizing them into structures called domains.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Ensure that the students obtain a clear understanding of the differences between domains and workgroups.

In Windows 2000, a domain is a logical grouping of networked computers that share a common area for storing security information. A domain provides a centralized approach to administering network resources. Users on one computer can access shared resources on other computers in the domain, provided they have been assigned the appropriate permissions.

Domains are similar in concept to workgroups, but provide a number of useful features, as described below.

Single logon

Domains provide a single logon process for users to access various network resources, including file, print, and application resources. All user accounts are stored in a central location.

Single user account

Users in a domain need only a single account to access resources on various computers. (In contrast, users in a workgroup require a separate account on each computer that they access.)

Centralized management

Domains provide centralized administration. All user account and resource information can be administered from a single location within the domain.

Scalability

Domains are scalable to very large networks. The ways in which users access resources and how resources are managed in very large networks are the same as on a small network.

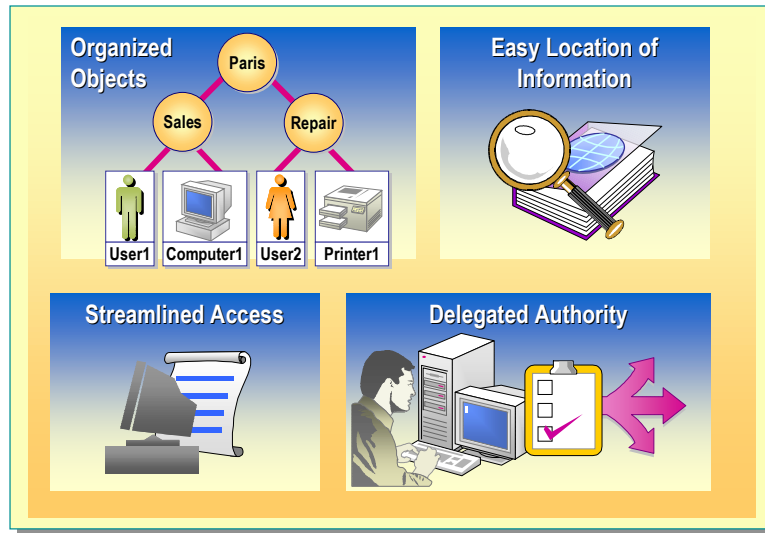
Benefits of a Domain

Topic Objective

To illustrate the benefits of a domain.

Lead-in

Windows 2000 manages networks by organizing them into structures called domains, which provide many benefits.



*****ILLEGAL FOR NON-TRAINER USE*****

A domain provides several benefits:

- **Organized objects**

You can organize the objects in the domain into organizational units. An organizational unit is a collection of *objects* in a domain. Objects are representations of the actual physical components that exist in an organization's network. They are associated with one or more domains, such as users, specific groups of users, computers, applications, services, files, and distribution lists.

For example, consider a domain in the network of a company. To simplify the management of all the resources in the company network, the resources of each department in the company can be organized into an organizational unit. Each organizational unit can be managed by someone in that department. In this manner, each department in the company constitutes an organizational unit, and the network administrator can manage groups of organizational units instead of individual resources.

- **Easy location of information**

Publishing a resource refers to making it available in a listing of domain objects, which makes it easy for users to locate and use the resources. For example, if a printer installed in a domain is published, users can locate it from the list of domain objects and access it. If the printer is not published, users can still access it, but they have to know its location to be able to do so.

- Streamlined access

Applying a policy to the domain establishes how users can access, configure, and use domain resources, which consolidates resource and security management. These policies are applied only within the domain, not across domains.

- Delegated authority

Domains enable you to assign permissions to an administrator to manage objects in an entire domain or in one or more organizational units within the domain. This eliminates the need for a number of administrators with wide-ranging administrative authority and overlapping responsibilities.

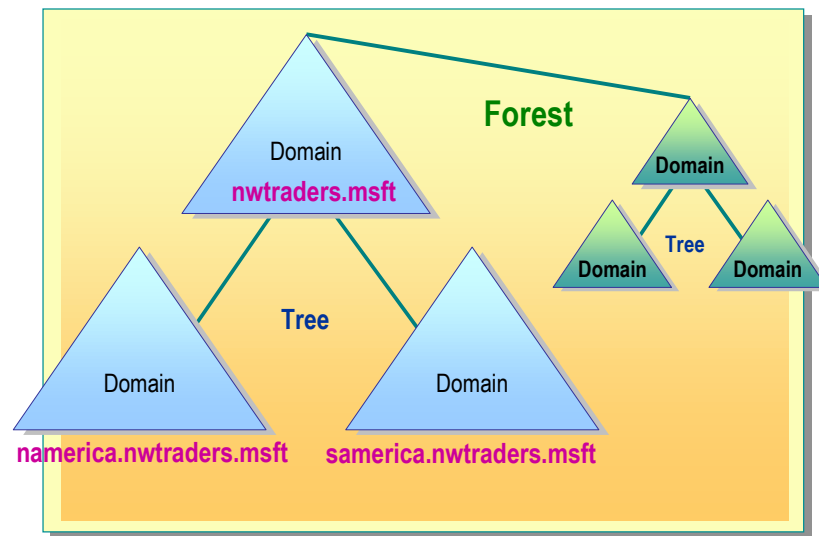
Domain Organization

Topic Objective

To illustrate how domains are organized.

Lead-in

Windows 2000 manages networks by organizing them into structures called domains.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

After lecturing on this topic, conduct a class discussion using the classroom configuration as an example of domain and sub-domain structures. Draw the classroom configuration on the board and ask the students to identify the structures in it in terms of a domain.

Every domain is managed by a domain controller. To simplify the management of multiple domains, domains are grouped into structures called trees and forests.

Domain Controller

A computer running Windows 2000 Server manages each domain. Such a computer is known as a domain controller. A domain controller manages all security-related interactions between users and the domain.

Trees

A *tree* is a hierarchical arrangement of Windows 2000 domains that share a common name. When you add a domain to an existing tree, you make it a sub-domain of a domain in the tree. This sub-domain is called a child domain, and the domain to which it is added is known as its parent domain.

After the child domain joins the tree, its domain name is added to the domain name of the parent. For example, when the domain London joins an existing tree and becomes a child of the parent domain nwtraders.msft, its domain name becomes london.nwtraders.msft.

Forests

A *forest* is a group of trees that do not share a common name, but do share a common configuration. By default, the name of the root tree, or the first tree that is created in the forest, is used to refer to a given forest. For example, if nwtraders.msft is the first domain in the first tree and another tree joins it to make a forest, the name of the forest is nwtraders.msft.

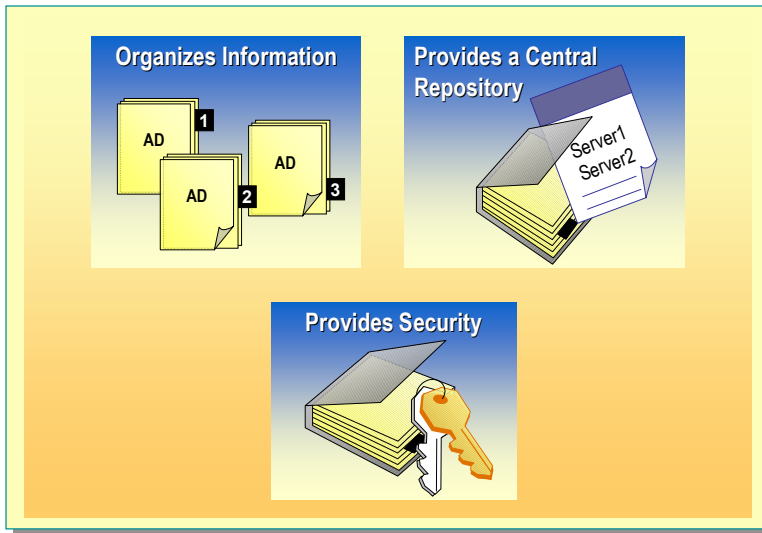
Features of Active Directory

Topic Objective

To illustrate the features of Active Directory.

Lead-in

Windows 2000 organizes information in a centralized location known as Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Active Directory™ directory service is the Windows 2000 directory service. Active Directory stores information about network objects and provides a hierarchical structure that makes it easier to organize domains and resources. This in turn makes it easier for users to locate network resources, such as files and printers.

Active Directory has many useful features:

- Active Directory organizes the directory into sections that permit storage of a very large number of objects. As a result, Active Directory can expand as an organization grows. This allows the network to grow from a network with a single server and a few hundred objects to a network with thousands of servers and millions of objects.
- Active Directory provides a central repository for gathering and distributing information about objects on a network, including users, groups, and printers, and makes this information easy to find and use.
- Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage the directory data throughout their network, and authorized network users can access resources anywhere on the network.

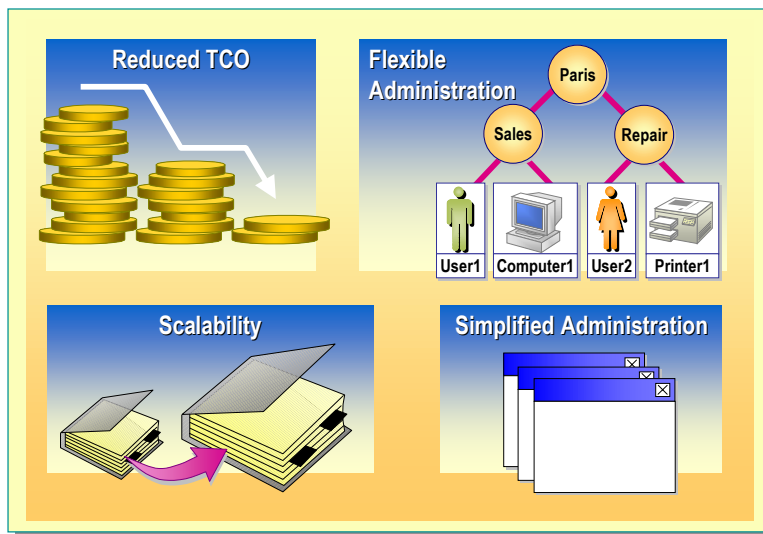
Benefits of Active Directory

Topic Objective

To illustrate the benefits of Active Directory.

Lead-in

Windows 2000 organizes information in a centralized location known as Active Directory, which provides many benefits.



*****ILLEGAL FOR NON-TRAINER USE*****

Active Directory addresses the following organizational needs: reduced total cost of ownership, flexible administration, scalability, and simplified administration.

- Reduced total cost of ownership

Total cost of ownership (TCO) refers to the actual cost of owning a computer. This includes the costs of maintenance, training, technical support, and upgrades to the hardware and software.

Active Directory helps reduce TCO by implementing policies. Applying a policy within Active Directory allows you to configure desktop environments and install applications from a central location. This reduces the time it takes to configure settings and install applications on each computer.

- Flexible administration

The organizational units into which a domain can be divided reside in Active Directory. The organizational units allow you to specify the users who will have administrative authority over portions of your network.

- Scalability

Active Directory extends the features of previous Windows-based directory services and is designed to work well in organizations of any size.

- Simplified administration

Active Directory provides customizable administrative tools that simplify administration and make it easier to administer resources throughout a network.

Accessing a Windows 2000 Network

Topic Objective

To illustrate the mandatory logon feature of Windows 2000.

Lead-in

Windows 2000 has a number of built-in network management features.



*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 features a mandatory logon process to validate the identity of every user accessing the system. During the logon process, Windows 2000 authenticates a user to verify the identity of the user. This process ensures that only valid users gain access to resources on a computer or the network. Logging on provides the user with access to everything on the network for which the user has been assigned the appropriate permissions.

To gain access to resources in a Windows 2000 network, a user needs a user account. A user account contains information about a user, including the user's name and password. If the computer is a member of a domain, the user account enables a user to log on to either the local computer or to the domain, but not to both, and, with the appropriate permissions, to access network resources. If the computer is a member of a workgroup, a user account enables a user to log on to the local computer only, since the user account exists only in the security database on the local computer.

To log on to a Windows 2000 domain, a user provides a user principal name. A user principal name consists of the user's logon name followed by the @character and a user principal name suffix. This suffix is usually the domain where the account exists, such as nwtraders.msft. An example of a user principal name is user@nwtraders.msft. The default user principal name suffix for a user account is the full domain name of the domain that contains the user account.

Logging On to Windows 2000

To log on to Windows 2000, press CTRL+ALT+DELETE. This displays the **Log On to Windows** dialog box. Type the user name and password in the appropriate areas to initiate the logon process. If the computer is a member of a domain, you can click **Options** to display the **Log on to** list box. You can then log on by clicking either the local computer or the relevant domain in the list.

Viewing Network Membership

After you log on, you can access the **System Properties** dialog box of your computer to determine the type of network membership you have—a domain or a workgroup.

To access the System Properties dialog box

- From the desktop, right-click the **My Computer** icon, and then click **Properties**.

The **System Properties** dialog box has five tabs. Click the **Network Identification** tab to determine whether your computer belongs to a workgroup or a domain.

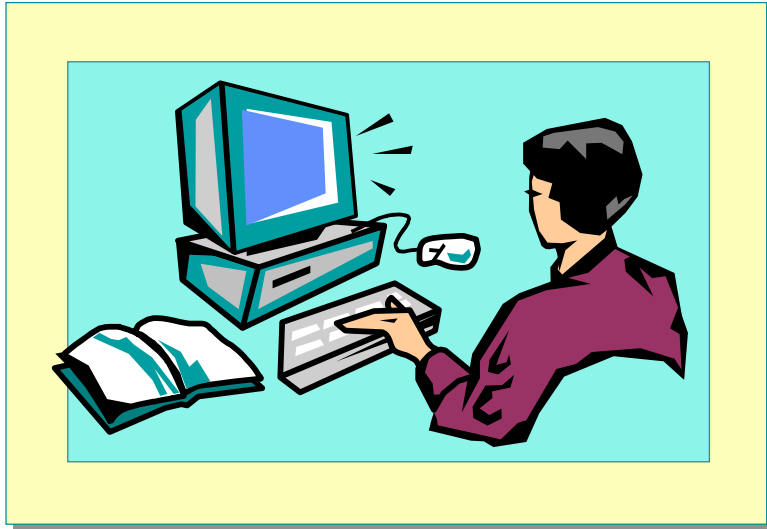
Lab B: Identifying Features of a Windows 2000 Network

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the features of a Windows 2000 network.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify components that are added to the network to provide additional functionality.
- Identify benefits of a domain.
- Identify components of Active Directory.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors. (16-bit recommended).
- Microsoft Internet Explorer 5 or higher.

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Features of a Windows 2000 Network**.
5. Read the introduction information, and then click the link to begin the lab.

Estimated time to complete this lab: 15 minutes

Lab C: Logging On to Windows 2000

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will log on to Windows 2000 and identify the operating system running on your computer.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Log on to Windows 2000.
- Identify which operating system is running on your computer.
- Determine whether your computer is located in a workgroup or domain.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Server configured as a primary domain controller.

Estimated time to complete this lab: 15 minutes

Exercise 1

Logging On to Windows 2000

Goal

In this exercise, you will use My Computer on the desktop to determine your computer name and whether your computer is in a domain or workgroup. You will log off and then log on using the **Log On To Windows** dialog box, specifying the domain information that you identified in the first step.

Tasks	Detailed Steps
1. Using the Network Identification tab in the System Properties dialog box, determine whether your computer is in a domain or workgroup.	- On the desktop, right-click the My Computer icon on the desktop. - Click Properties, and then click the Network Identification tab.
 What is the name of your computer? Answers will vary. _____ _____ _____ _____	
 Is your computer a member of a workgroup or domain? Domain. _____ _____ _____ _____	
 What is the name of your computer's workgroup or domain? Answers will vary. _____ _____ _____ _____	

Tasks	Detailed Steps
2. Log off from Windows 2000, and then display the Security dialog box.	a. Press CTRL+ALT+DELETE, and click Log Off. b. In the Log Off Windows dialog box, click Yes to the question: Are you sure you want to log off?  <i>You will be logged off. The Welcome to Windows screen appears.</i> c. Press CTRL+ALT+DELETE  <i>The Log On to Windows dialog box appears.</i>
 What operating system is currently installed on the computer? Microsoft Windows 2000 Advanced Server.	
3. Log on to your domain as Administrator with a password of password.	a. Type administrator for the user name and password for the password. b. Click Options.  <i>The Log on to box appears, letting you click your domain in a list.</i> c. In the Log on to list, click your own domain, and then click OK.
4. Close the System Properties dialog box and log off from Windows 2000.	a. Click OK to close the System Properties dialog box. b. Press CTRL+ALT+DELETE, and then click Log Off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Windows 2000 Operating Systems**
- **Introduction to Networks**
- **Windows 2000 Implementation of Networking**

*****ILLEGAL FOR NON-TRAINER USE*****

1. Which four key aspects of a computer's operation does an operating system manage?

Hardware Management.

Software Management.

Memory Management.

Data Management.

2. All the employees in your organization have access to individual hardware and software resources. Lately, the number of employees has increased. What can you do to ensure that several employees can share the existing hardware and software simultaneously?

Install a network.

3. Your organization is upgrading to the Windows 2000 operating system. Since the company's network has about 5,000 computers, which Windows 2000 operating system would best ensure scalability and system availability?

Windows 2000 Advanced Server.

4. When installing a network, you want to ensure that an administrator can maintain the network with minimal effort. What type of network enables this and also ensures that each computer functions as both a client and a server?

A peer-to-peer network.

5. Your company's network has increased in size due to an increase in the number of connected computers and in the physical distance and traffic between them. Which network type is most suitable for use in this situation?

A client-server network.

6. In a workgroup, where are the user accounts located?

In the security database on the local computer.

7. What are the benefits of using domains in Windows 2000?

Organizing domain objects.

Easy location of information about domain objects.

Streamlined access to domain objects.

Delegating authority.

8. Which organizational needs are addressed by Active Directory?

Reduced total cost of ownership (TCO).

Simplified administration.

Flexible administration.

Scalability.

Module 2: Administration of a Windows 2000 Network

Contents

Overview	1
Windows 2000 Help	2
Lab A: Using Windows 2000 Help	7
Administrative Tasks	13
Administrative Tools	17
Lab B: Identifying Administrative Tools	38
Review	44



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

Labs:
30 Minutes

This module informs students about the tasks associated with the administration of a Microsoft® Windows® 2000 network. Students learn the skills required to open Windows 2000 Help and locate information in it. The students will perform a lab exercise in which they open Windows 2000 Help, use the **Contents** and **Search** tabs to locate information, and add items to a list on the **Favorites** tab.

The module next introduces the routine administrative tasks performed by a network administrator. Then the module explains the set of common administrative tools provided by Windows 2000 to perform administrative tasks. This section is followed by a lab in which students identify the common administrative tools and their locations. The purpose of the module is to describe the functions performed by the tools and the procedure to access them from Control Panel. The module does not attempt to explain how to use the tools.

At the end of this module, students will be able to:

- Use Windows 2000 Help to locate specific information.
- Describe routine administrative tasks required for network maintenance.
- Associate the Windows 2000 administrative tools with the tasks they perform.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_02.ppt
- Module 2, “Administration of a Windows 2000 Network”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the two labs.
- Practice demonstrating the administrative tools listed in the module.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- Windows 2000 Help

Provide an overview of Windows 2000 Help as a source of information for performing administrative tasks. Then demonstrate the procedure to open Windows 2000 Help and explain the four tabs in the window. Explain and demonstrate the procedure for using the Search feature and Search options. Practice the procedure before demonstrating it to the class. In the last topic in the section, explain and demonstrate the procedure for creating a list of favorites.

- Administrative Tasks

Introduce the various administrative tasks and the activities they involve. Then explain how to schedule a task to run automatically. Have the students perform the inline exercise provided in the module.

- Administrative Tools

In this section, introduce the students to Control Panel and its functions. Then demonstrate how to open Control Panel and explain how changes made to the system by the administrative tools are reflected in the registry. It is important to caution the students to make no changes to the registry until they gain further experience. Then explain the function of each of the common tools listed in the module and demonstrate how to access them. Be sure to demonstrate only the procedure that is taught in the course material. Even though there is more than one procedure to access a tool, the course material teaches how to access the tools from Control Panel.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about the routine administrative tasks that must be performed to maintain a network and the administrative tools provided by Windows 2000 to perform them.

- Windows 2000 Help
- Administrative Tasks
- Administrative Tools

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The goal of this module is to provide information about the tools used to maintain a network, not how to use them. The students need to be familiar with each tool's function and how to use Windows 2000 Help to obtain any required information.

As an administrator, you perform a number of tasks to maintain an efficiently functioning network. These tasks include maintaining user accounts and printers, backing up and restoring data, and monitoring network activities.

For information about performing these administrative tasks, you can use Microsoft® Windows® 2000 Help, a database of information on every aspect of Windows 2000.

To assist you in performing routine administrative tasks, Windows 2000 provides a set of administrative tools that simplifies the tasks by providing a user-friendly interface.

At the end of this module, you will be able to:

- Use Windows 2000 Help to locate specific information.
- Describe routine administrative tasks required for network maintenance.
- Associate the Windows 2000 administrative tools with the tasks they perform.

◆ Windows 2000 Help

Topic Objective

To introduce the features and functions of Windows 2000 Help.

Lead-in

Windows 2000 Help provides a quick reference for information about performing most routine administrative tasks.

- Accessing Windows 2000 Help
- Using the Search Feature
- Creating a List of Favorites

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 Help is a database containing information about a variety of topics. This database is especially useful for locating information about performing specific administrative tasks in a Windows 2000 network. Windows 2000 Help is always available and can be used in such activities as searching for information and bookmarking topics for later retrieval.

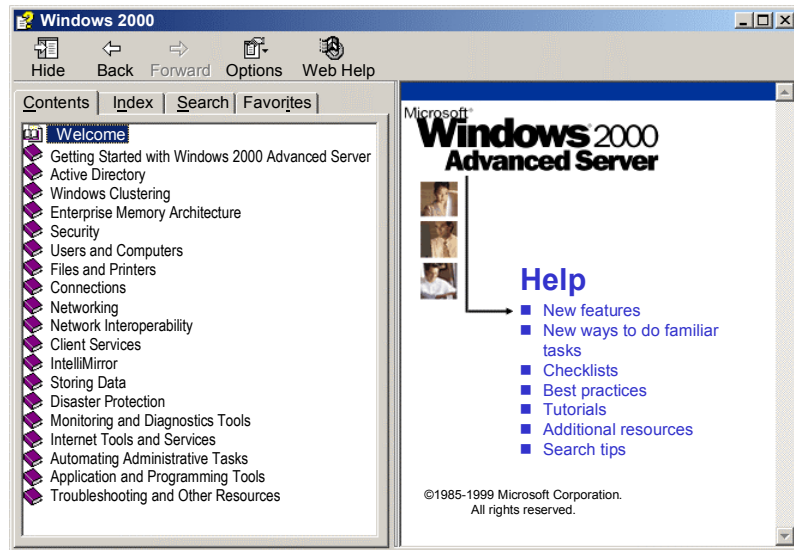
Accessing Windows 2000 Help

Topic Objective

To provide an overview of Windows 2000 Help.

Lead-in

You can use the Windows 2000 Help feature to locate information about administrative tasks.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to access Help and guide the students through the four tabs.

Windows 2000 Help provides information about a variety of administrative tasks. In addition to providing detailed instructions for performing the tasks, the topics also provide links for navigating through the Help topics.

To access Windows 2000 Help

- On the **Start** menu, click **Help**.

The Windows 2000 Help window displays two panes. The left pane contains four tabs, each of which provides a different method for locating information. The following table describes how to use these tabs.

Use this tab	To
Contents	Display a listing of all topics in Windows 2000 Help in an organized manner. Use this tab if you are unfamiliar with the terminology.
Index	Locate information by using an index of all the keywords in the Help file. Use the index if you know a specific keyword.
Search	Search for a keyword or a set of keywords and locate all topics that contain the keywords. Use this tab if you are looking for specific information about a general phrase or word.
Favorites	Add topics to a list of favorites. Use this tab to revisit specific topics without having to search for them again.

Windows 2000 Help is context-sensitive and provides information about the particular feature that you are using. For example, if you access Help when using Microsoft Internet Explorer, it displays Internet Explorer topics.

Note Window 2000 Help also includes a Web feature that you can use to view Help information available on the Internet. This feature provides access to the latest information on Windows 2000, including additional support information.

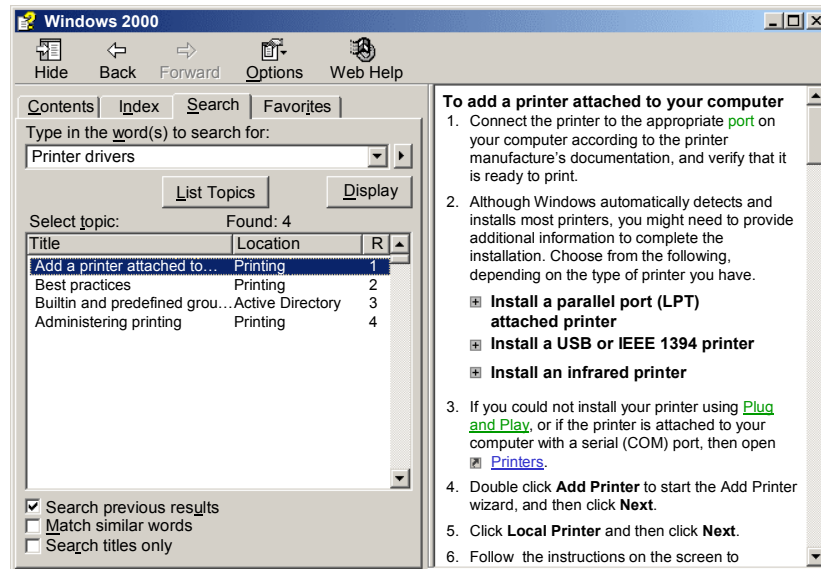
Using the Search Feature

Topic Objective

To explain the use of the Search feature in Windows 2000 Help.

Lead-in

Windows 2000 Help enables you to search for information by specifying a keyword.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the animation slides to demonstrate how to use the Search feature and refine the search using the options available with the Search feature. Make sure to practice using the Search feature before demonstrating it to the class.

Sometimes you may not know which Help category contains information about a specific topic. To assist in such a situation, Help provides the Search feature. Using this feature, you can search for information by providing one or several keywords that define it. For example, to find information about administering a printer, you can specify **how to administer a printer** as the search keywords.

Also, you can use Windows 2000 Help to review previous searches. Help stores information about the last 20 words and phrases searched for in a drop-down list box on the **Search** tab.

To search using a keyword

1. In the Help window, click the **Search** tab.
2. In the **Type in the word(s) to search for** box, type the keyword or phrase, and then click **List Topics**.
A list of topics appears.
3. In the displayed list, click the topic of your choice, and then click **Display**.

Refining a Search

Usually a search produces a long list of topics. To generate a manageable list of search results, you can refine your search by using one or more of the three check boxes located at the bottom of the **Search** tab:

■ Search previous results

After the first search, select this check box and specify another keyword to search against the results of the earlier search. This narrows the scope of the search. You can continue to refine your search in this manner until the results suit your requirements.

- **Match similar words**

The **Match similar words** check box is selected by default. Use this option to search for all words that match the keywords as well as words similar to them. For example, if you search for the keyword Administer, you will find topics with the keywords Administering and Administrator, too.

- **Search titles only**

The **Search titles only** option allows you to search for a keyword in topic titles only, not in topic content.

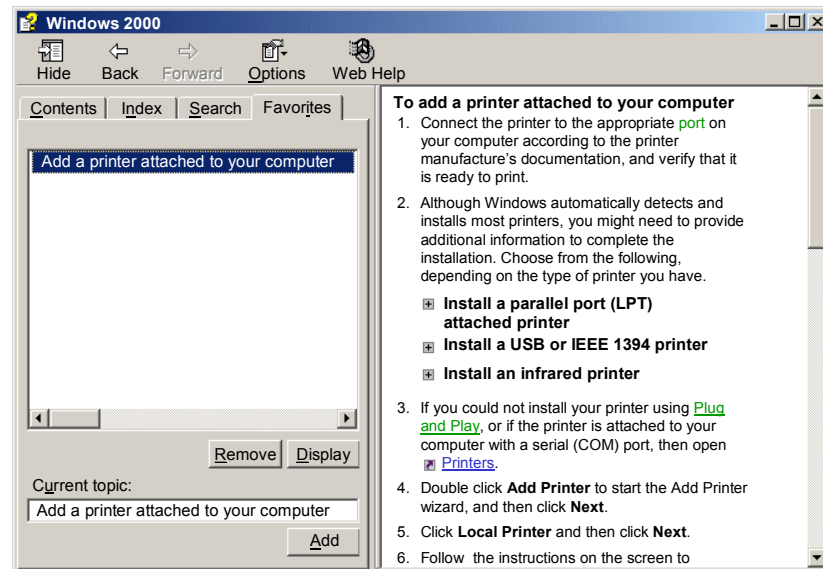
Creating a List of Favorites

Topic Objective

To explain how to create a list of favorites.

Lead-in

In Windows 2000 Help, you can bookmark the entries you often search for.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to create a list of favorites. Make sure to practice the procedure before demonstrating it to the class.

You can use the Windows 2000 Help database to bookmark information that you regularly access. You can create a list of favorites and add or remove entries from it. Bookmarking favorite topics reduces the time required to find information that you have located previously.

To create a list of favorites

1. Use the **Search** tab and a keyword to search Windows 2000 Help to display a list of topics.
2. To save a specific topic, select the topic, click the **Favorites** tab, and then click **Add**.

You can place new bookmarked topics on your list of favorites according to their original names, or you can rename the entries to be more meaningful for you. You should specify a different name before adding the entry to the list of favorites. After you click the **Favorites** tab, the original name appears selected. Type a new name for the topic in the **Current topic** box, and then click **Add**.

Note You can rename a topic after adding it to the list of favorites by right-clicking the topic and clicking **Rename**.

Lab A: Using Windows 2000 Help

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will use Windows 2000 Help to locate information.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Use the **Contents** tab in Help to find a topic.
- Use the **Search** tab to find a topic in Help.
- Refine a search using the **Search** options.
- Activate a Windows 2000 utility by using links in Help.
- Add a bookmark to the **Favorites** tab.

Prerequisites

Before working on this lab, you must have:

- Basic knowledge of the Windows 2000 interface.
- Ability to log on Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Using the Contents Tab of Windows 2000 Help

Scenario

You are an administrator of a Windows 2000 network and need to perform an unfamiliar administrative task. Before beginning this task, you decide to gain more knowledge about it by using Windows 2000 Help. Because of the large amount of information contained in Windows 2000 Help, you use various methods to search for relevant information. You search for information on administrative tools. When you find the relevant topics, you configure Help so that you can return to these topics more quickly in the future.

Goal

In this exercise, you will use the **Contents** tab to locate information on some of the administrative tools that you use in your job. You will locate information on how to use the Windows 2000 Server Help from a computer that is not running Windows 2000 Server. You will use the search capabilities built in to the Help system and then save the results so that you can quickly find a particular topic the next time you need the information.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password .	a. Log on to Windows 2000 as Administrator with a password of password .
2. Start Windows 2000 Help and display the Contents tab.	a. Click Start, and then click Help. b. Maximize the Help window. If it is not selected, click the Contents tab. c. In the left pane of the Help window, click Getting Started with Windows 2000 Advanced Server.  <i>The right pane shows the additional topics for Getting Started with Windows 2000 Advanced Server.</i> d. In the left pane of the Help window, click Active Directory. e. <i>The right pane shows the additional topics for Active Directory.</i> f. In the left pane of the Help window, click Security.  <i>The right pane shows the additional topics for Security.</i> g. In the left pane of the Help window, click Users and Computers.
 If you are currently running Windows 2000 Professional and need access to the Windows 2000 Server Help files, which topic from the right pane would provide you with additional information on accessing the server Help files? Accessing Windows 2000 Server Help remotely. _____ _____ _____ _____	

Tasks	Detailed Steps
3. Activate the Help topic: Accessing Windows 2000 Server Help remotely.	a. In the right pane of the window, click the Accessing Windows 2000 Server Help remotely topic.
 How many different ways are there to access the Help files remotely? List them. There are 6 different ways to access the Help files remotely. They are: Allow read-only access to the Help folder on a server. Copy all Help files to a shared folder on your network. Copy all Help files to your local computer. Install Windows 2000 Administration Tools on your local computer. Print Help topics from a server. View the Help files on the Microsoft Web site. _____ _____ _____ _____ _____	
 Looking for a specific topic this way could be time-consuming. Is there a faster way to find information in Windows 2000 Help? If so, what is it? Yes. Use the Search function of Windows 2000 Help. _____ _____ _____ _____	
4. Use the Search tab to search for administrative tools and take into account variations in the words.	a. Click the Search tab. b. Type administrative tools in the Type in the word(s) to search for box. c. At the bottom of the Help window, see if the Match similar words check box is selected. If it isn't checked, select it. d. Click List Topics.
 How many results were found? 500 _____ _____ _____ _____	

Tasks	Detailed Steps
5. Display the Help topic Managing servers remotely (the first topic in the list).	a. In the left pane of the window, double-click Managing servers remotely (the first topic in the list).
 Note: You will notice that the selected item in the text is administration tools and not administrative tools.	
 Why did Help find the words administration tools instead of administrative tools in this Help topic? Because match similar words is selected so Windows 2000 Help finds variations of the words. _____ _____ _____ _____	
6. Open the Help topic: Common problems and their solutions (the eleventh topic in the list).	a. Double-click the topic Common problems and their solutions (the eleventh topic in the list).
 Why did Help find this topic if tools is not mentioned? Because Help searched for either word—administration or tools—you will get results that are not exact matches. _____ _____ _____ _____	
 How could you modify the search criteria to return results that contained only the phrase administrative tools? By putting quotation marks around the words, Windows 2000 Help will treat it as a single phrase and only return results with administrative tools in the topic. _____ _____ _____ _____	
7. Refine the search to look for administrative tools as a phrase.	a. In the Type in the word(s) to search for box, type “administrative tools” (including the quotation marks). b. Click List Topics.

Tasks	Detailed Steps
 How many results were found? 500 _____ _____ _____ _____	
8. Configure Help so that it will not return results that contain variations of the words.	a. Clear the Match similar words check box. b. Click List Topics.
 How many results were found? 500 _____ _____ _____ _____	
9. Configure Help so that it will only search in titles.	a. Select the Search titles only check box. b. Click List Topics.
 How many results were found? 4 _____ _____ _____ _____	
10. Open the Help topic Administrative Tools.	a. In the left pane, double-click Administrative Tools.
 Note: This lists the common administrative tools in Windows 2000.	

Tasks	Detailed Steps
 If you want to find this topic more easily in the future, what could you do? Add it to your list on the Favorites tab. _____ _____ _____ _____	
11. Add the topic Administrative Tools to your list on the Favorites tab.	a. Click the Favorites tab, and then click Add .
12. Activate Event Viewer using Windows 2000 Help.	a. In the right pane, click Event Viewer. b. In the list of additional information that appears below Event Viewer, click the Using Event Viewer link.  <i>Using Event Viewer Help topic opens.</i> c. Click the Event Viewer link.  <i>The Event Viewer administrative tool opens and shows you the event logs.</i>
13. Close Event Viewer and add the Using Event Viewer Help topic to your list on the Favorites tab.	a. Close the Event Viewer window. b. Click Add to add Using Event Viewer to your favorites. c. Click the Related Topics link.
 What kinds of information are found in the Related Topics link? Additional Help topics that are related to the current Help topic. _____ _____ _____ _____	
14. Return to the Administrative Tools topic using the Related Topics link.	a. Click Administrative Tools from the menu.  <i>You are returned to the previous topic Administrative Tools.</i>
15. Close Windows 2000 Help and log off from Windows 2000.	a. Close Windows 2000 Help, and then log off from Windows 2000.

◆ Administrative Tasks

Topic Objective

To introduce the administrative tasks required for network maintenance.

Lead-in

There are a number of administrative tasks that must be performed on a regular basis.

- Routine Administrative Tasks
- Scheduling Administrative Tasks

*****ILLEGAL FOR NON-TRAINER USE*****

As a network administrator, you provide users with access to the network, control the kind of access that each user has to network resources, and perform maintenance tasks. You create user accounts and assign permissions for users to access such resources as printers, applications, and data files.

You also manage the hardware and software installed on the computers as well as perform such tasks as creating printer shares and administering database and mail servers. Some of these routine tasks, such as backing up data on the servers, can be scheduled to run on a recurring basis automatically.

In this section, you will learn about the various routine tasks and the procedure for scheduling a task to run at a preset time.

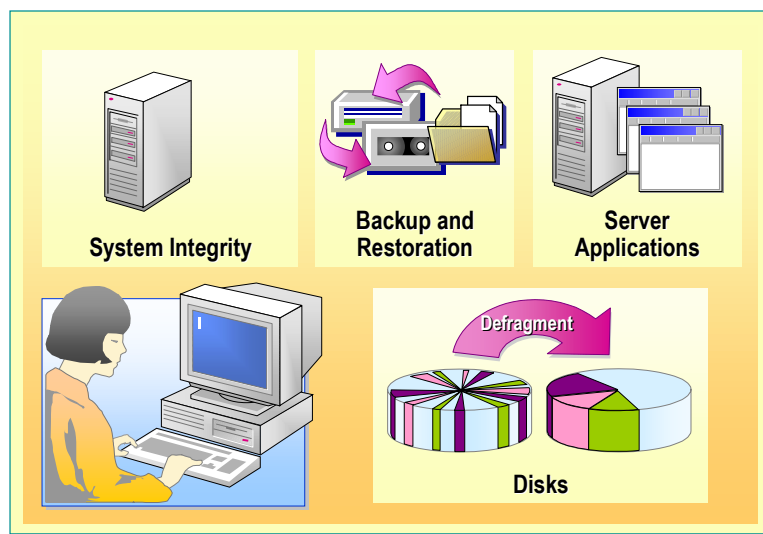
Routine Administrative Tasks

Topic Objective

To introduce the major areas in which routine tasks need to be performed.

Lead-in

Let us go over the routine tasks that a network administrator performs.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This topic has two slides; each slide illustrates four administrative tasks.

A network administrator performs administrative tasks in the following areas: users and groups, printers, security, network events and resources, system integrity, backup and restoration, server applications, and disks.

Users and Groups

As an administrator, you assign and maintain user names and passwords for each user account. A user account enables the user to log on to a server to access network resources or to log on to an individual computer to access resources on that computer. You also create and maintain groups and define their membership. Organizing users into groups simplifies assigning permissions.

Printers

Administering printers includes setting up local and network printers and troubleshooting common printing problems, thereby ensuring that users can connect to and use printer resources easily.

Security

Maintaining network security involves planning, implementing, and enforcing a security policy for protecting data and shared network resources, including folders, files, and printers. By assigning user permissions, you can control access to resources. You determine *who* has access to specific resources and specify the *kind* of access that each user has.

Network Events and Resources

Monitoring network functioning is a very important task. Regular monitoring of the network can help detect a problem and resolve it before it causes the network to fail. Network monitoring includes evaluating resource usage and planning and implementing a policy for tracking security breaches.

System Integrity

Maintaining system integrity is critical to the network. The network administrator must regularly check the computers for the presence of computer *viruses*. A virus is a program that runs without your knowledge and may damage data. The administrator must safeguard the network by installing and updating anti-virus software regularly. In the event of the network being infected by a virus, the network administrator must take necessary steps to delete the virus from the network.

Backup and Restoration

One of the most important recurring tasks is backing up the data in the system. This task includes planning, scheduling, and performing regular backups to protect important data. Having a good backup system ensures that you can quickly locate and restore critical data that has been lost or damaged.

Server Applications

A system may run numerous server applications that require administration. For this purpose, there are specific tools that you use to administer application-based services, such as mail servers and database servers.

Disks

A computer's hard drive, or hard disk, is responsible for data storage. It is important to maintain these disks to ensure optimum performance and minimize the chances of data loss, while at the same time maintaining the data access speed. You verify the integrity of hard drives in terms of their reliability and configure them as part of your routine administrative tasks.

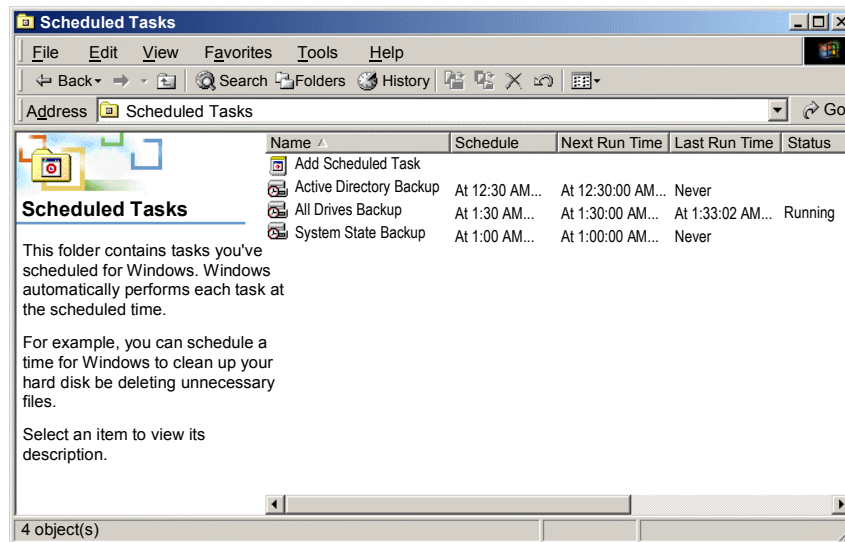
Scheduling Administrative Tasks

Topic Objective

To describe tasks that can be scheduled.

Lead-in

To ensure that recurring administrative tasks are performed, you can schedule them to run independently of your involvement.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the animation slides to demonstrate the procedure for accessing this tool and have the students perform the steps provided. After they complete the exercise successfully, ask questions about the parameters governing the task, such as the date and time when the task is scheduled to run.

Some administrative tasks are performed on a recurring basis and can be scheduled to run automatically. For example, you can schedule backups to run at a specific time daily and weekly. This ensures that a regular backup schedule is maintained and that the data in the system is safe. Other tasks, such as creating a user account, cannot be made automatic because they take place as needed.

Scheduled Tasks

To schedule recurring tasks, you can use Scheduled Tasks, a tool that helps you to schedule any application to run at a preset time. Using the options available in Scheduled Tasks, you can:

- Schedule a task to run daily, weekly, monthly, or at other specified times.
- Change the schedule for a task.
- Stop a scheduled task after it has started or before it starts.
- Run a scheduled task immediately.
- Customize how a task runs at a scheduled time. For example, you can specify that a task be postponed if the computer is running on batteries or delay the task until the computer has been idle for a certain time.

To run a scheduled task

1. From the **Start** menu, point to **Programs**, **Accessories**, and **System Tools**, and then click **Scheduled Tasks**.
2. Right-click the task and click **Run**.

As an exercise, right-click the **Weekly Backup** task and click **Run** from the menu.

◆ Administrative Tools

Topic Objective

To introduce the administrative tools provided by Windows 2000.

Lead-in

Windows 2000 provides tools to perform a wide range of tasks.

■ Control Panel	■ Shared Folders
■ System Properties	■ Disk Management
■ System Information	■ Backup
■ Event Viewer	■ Security Management
■ Windows Task Manager	■ Network Tools
■ Performance	■ Additional Tools
■ Printers	■ Microsoft Management Console

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

All tools except the Backup tool can be accessed from Control Panel. Demonstrate the procedure as listed in the course material. The focus of this section is to provide only a high-level introduction to the administrative tools available, not an explanation of how to use them.

From managing user accounts and printers to monitoring resources for security purposes, the administrative tools provided by Windows 2000 help you perform a wide range of routine administrative tasks. You can access most of these tools from Control Panel.

This section discusses the most common tools used in administering a network. It does not discuss all of the available tools.

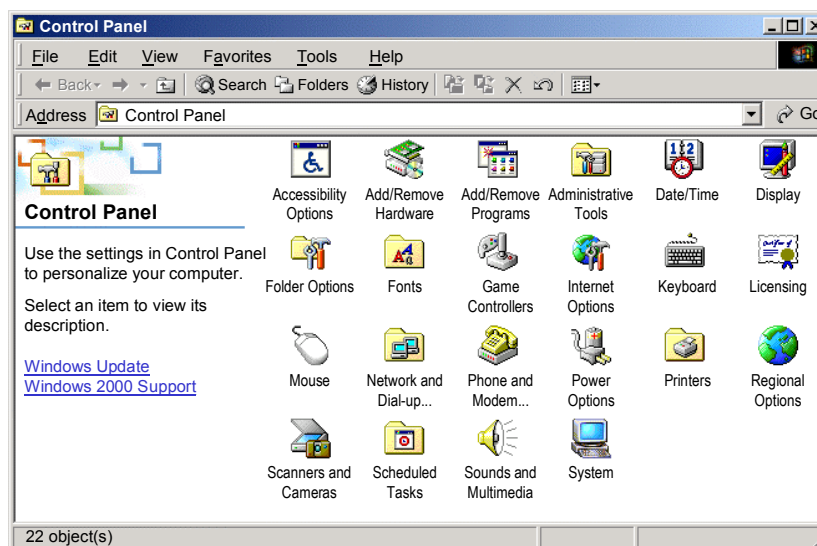
Control Panel

Topic Objective

To describe the role of Control Panel.

Lead-in

Most of the common administrative tools are available at one location, Control Panel.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to access Control Panel.

Instruct the students to make no changes to the registry until they gain further experience and are sure of what they are doing.

Mention here that not all of the tools available in Control Panel are always required. Tell the students that they can assemble a customized collection of frequently used tools by using the Microsoft Management Console (MMC), which is discussed later in the module.

Most of the administrative tools provided by Windows 2000 are available in Control Panel. Control Panel serves as a repository of tools that you can use to configure and monitor system settings. For example, using the tools in Control Panel, you can change the display on your monitor and modify security settings for a specific user.

To access Control Panel

- From the **Start** menu, point to **Settings**, and click **Control Panel**.

Registry

The registry reflects the changes that you make to the system when you use the tools in Control Panel. The registry is a database in which Windows 2000 stores configuration information pertaining to the system hardware and applications installed on the computer. Windows 2000 continually refers to this information during its operation.

Caution Do not make changes to the registry until you gain further knowledge and experience working with the registry.

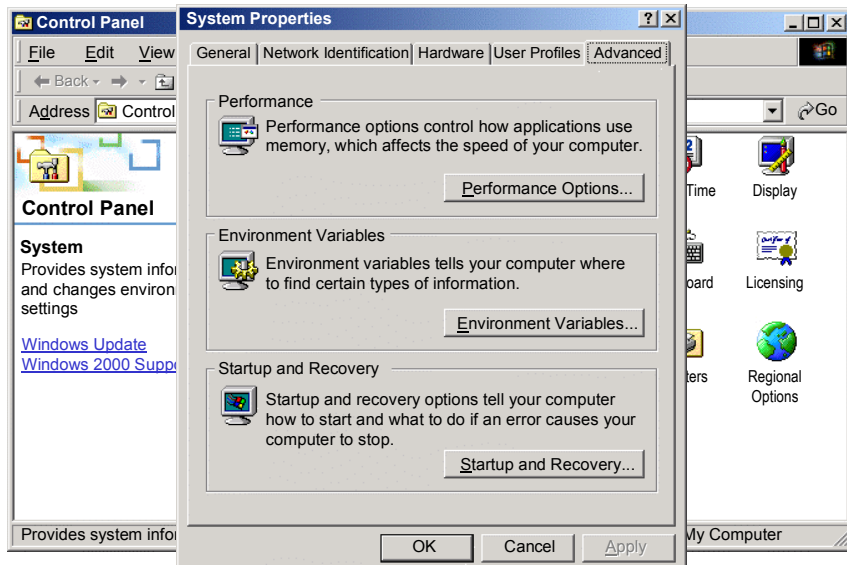
System Properties

Topic Objective

To describe the System Properties tool.

Lead-in

You can view and modify the system properties using the System Properties tool.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the animation slides to demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

System Properties is a tool you can use to view and change system properties on a local computer or on a remote computer.

Note To change certain system properties on a computer, you must have administrator privileges on the computer you are administering.

To access the System Properties tool

- From Control Panel, open **System**.

Organization of Information

The System Properties tool organizes information in five areas that can be accessed from the following tabs:

■ General

The **General** tab provides such information as the type of operating system running on the computer, the amount of memory installed, and to whom the computer is registered.

■ Network Identification

The **Network Identification** tab provides information about the name of the computer and the domain or workgroup to which it belongs. You can click **Properties** on the **Network Identification** tab to join a domain or to change the name of the computer and the domain or workgroup to which it belongs.

- Hardware

The **Hardware** tab provides the Add/Remove Hardware wizard for installing, uninstalling, and managing computer hardware. It also provides Device Manager, a tool that you use to change the properties of any device, and Driver Signing, an option that allows you to set security levels for new software installation. Finally, Hardware Profiles enables you to set up and store different hardware configurations from which you can choose when starting the computer.

- User Profiles

The **User Profiles** tab contains information about the different user *profiles* that exist on the computer. A profile contains information about a specific user's logon settings, such as desktop settings. Profiles are of two types: local and roaming. A local user profile is automatically created on each computer to which a user logs on. If the user has a roaming user profile, the same profile can be used on any other computer to which the user logs on.

- Advanced

The **Advanced** tab provides three sets of options. Performance options control how the microprocessor is utilized when running applications, which affects the computer's speed. Environment variables assist in locating such information as the Windows system files. Startup and recovery options tell the computer how long to delay startup and what to do if an error causes the computer to stop running unexpectedly.

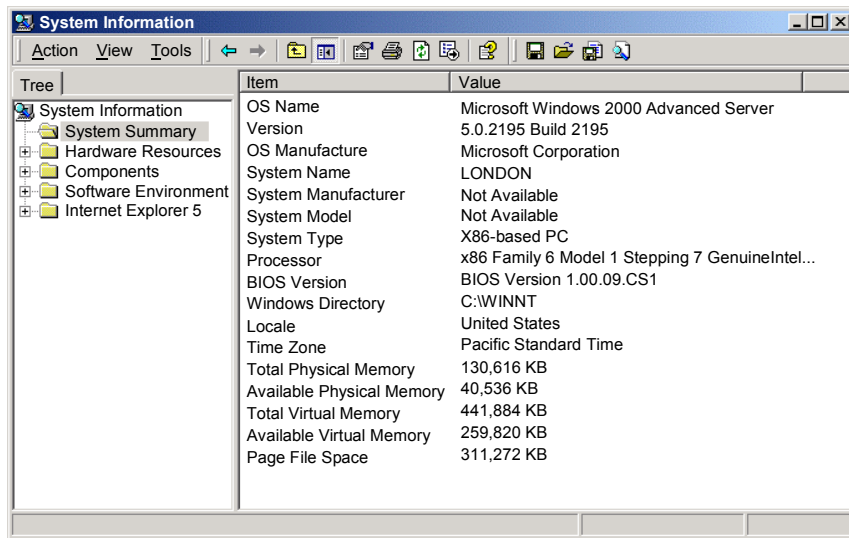
System Information

Topic Objective

To describe the functions of System Information.

Lead-in

Use the System Information tool to monitor the state of the system.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

System Information displays a comprehensive view of the hardware, system components, and software environment.

To access System Information

- From Control Panel, open **Administrative Tools**, **Computer Management**, **System Tools**, and then **System Information**.

Organization of Information

The displayed system information is organized into four top-level categories:

■ System Summary

The System Summary folder includes such information as the computer name, the processor name, and the version of the operating system and amount of memory installed on the computer.

■ Hardware Resources

The Hardware Resources folder includes subfolders that contain information about hardware settings and memory.

■ Components

The Components folder includes subfolders that contain information about display settings, network and modem settings, and printer settings.

■ Software Environment

The Software Environment folder includes subfolders that contain information about currently running tasks, network connections, startup applications, and the drivers loaded in the system.

When additional applications, such as Internet Explorer, are installed, the System Summary includes sections on versions and such application-specific settings as security settings for Internet Explorer.

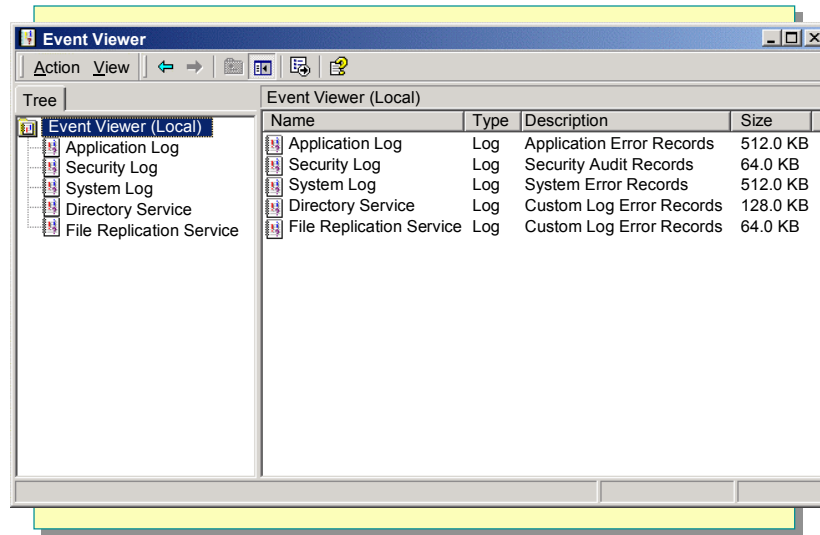
Event Viewer

Topic Objective

To explain the use of Event Viewer.

Lead-in

Event Viewer displays information about system events.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Event Viewer is a tool that gathers information about hardware, software, system problems, and security events. An *event* is any notable occurrence that happens in an application or within the operating system itself. Each time an event occurs, Windows 2000 records its occurrence in a log. Therefore, by using the event logs in Event Viewer, you can monitor the status of the system.

To access Event Viewer

- From Control Panel, open **Administrative Tools**, and then **Event Viewer**.

Types of Events

Event Viewer displays one of four types of events:

- **Error**
Indicates a significant problem, such as loss of data or functionality.
- **Warning**
May indicate a possible future problem.
- **Information**
Describes the successful operation of an application, driver, or service.
- **Auditing**
Indicates whether an attempt to access an audited resource was a success or a failure.

Event Viewer then records the occurrences of these types of events in event logs. Different types of event logs are created depending on the additional components installed on the system. Some common event logs are the application log, the system log, and the security log.

Application Log

The application log contains events logged by applications. For example, a database application might record a file error in the application log. The application log records Error, Warning, and Information events.

System Log

The system log contains events logged by Windows 2000 system components. For example, the system log records the failure of a system component to load during startup. The system log records Error, Warning, and Information events.

Security Log

The security log records Auditing events, including valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files.

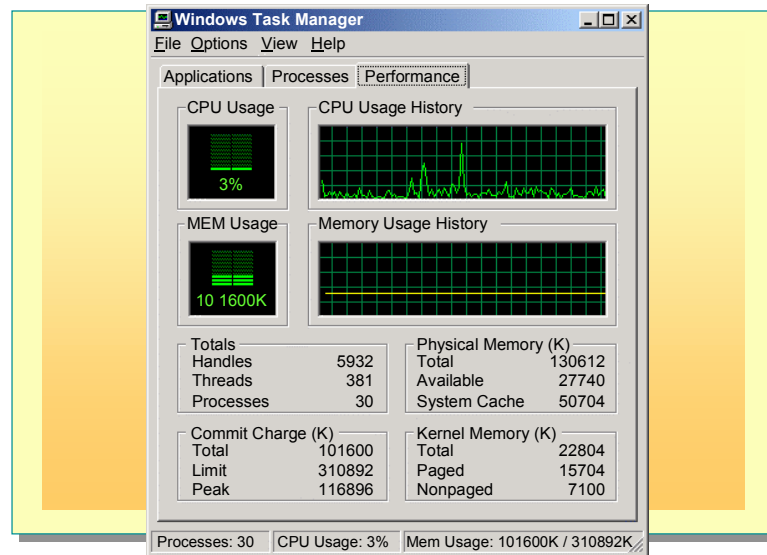
Windows Task Manager

Topic Objective

To explain the use of Windows Task Manager.

Lead-in

You can determine the current processes and applications running on your computer by using Windows Task Manager.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Windows Task Manager provides information about computer performance and the applications and processes running on the computer. Using Windows Task Manager, you can start applications, end applications or processes, and view a dynamic display of your computer's performance.

To access Windows Task Manager

- Right-click an empty space on the taskbar, and then click **Task Manager**.

The information displayed by Windows Task Manager is organized into three tabs: **Applications**, **Processes**, and **Performance**.

■ Applications

The **Applications** tab displays the status of the applications that are running on your computer. From this tab, you can end, switch to, or start an application.

■ Processes

The **Processes** tab displays information about the processes running on your computer. A process can be an application, such as Microsoft Windows Explorer, or a service, such as Event Log.

■ Performance

The **Performance** tab displays a dynamic overview of your computer's performance, including the CPU and memory usage.

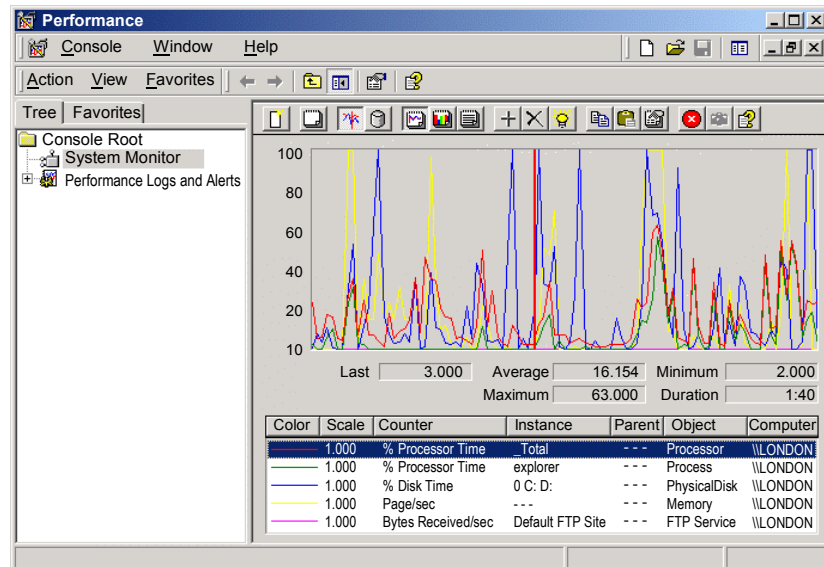
Performance

Topic Objective

To describe the Performance tool.

Lead-in

You can monitor system performance by using the Performance tool.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options. While explaining the Performance tool, do not attempt to generate data during the class.

Monitoring system performance is an important part of maintaining and administering your Windows 2000-based installation. Windows Task Manager is a simple tool you use to monitor the performance of your computer and view general system information.

A more detailed version of Windows Task Manager is the Performance tool. This tool provides data that you use to monitor the performance of your computer or the performance of other computers on the network.

Performance Data

The data provided by the Performance tool is used to:

- Analyze changes in your workload and evaluate its corresponding effect on system resources.
- Observe changes and trends in workloads and resource usage so that you can plan for future system upgrades.
- Evaluate changes to system configuration by monitoring the results.
- Diagnose problems and target components or processes for improvement.

To access the Performance tool

- From Control Panel, open **Administrative Tools**, and then **Performance**.

The Performance tool comprises two utilities: System Monitor and Performance Logs and Alerts. These utilities provide detailed data about the resources used by specific components of the operating system and by other applications and services running on the system.

System Monitor

With System Monitor, you can:

- Collect performance information on your computer and compare it with the performance of other computers on a network.
- Collect and view performance data being generated on a local computer or from several remote computers on the network.
- View data collected either currently or previously in a log file.
- Present data in a printable graph, histogram, or report view. The graph view is the default view and offers the widest variety of optional settings.
- Create a Web document from performance views.
- Create reusable monitoring configurations that can be installed on other computers.

Performance Logs and Alerts

The Performance Logs and Alerts utility:

- Supports the definition of performance objects, performance counters, and object instances.
- Sets sampling intervals for monitoring data about hardware resources and system services.
- Collects information over a period of time and archives data.
- Supports the configuration of alerts that notify you when a certain threshold is reached.

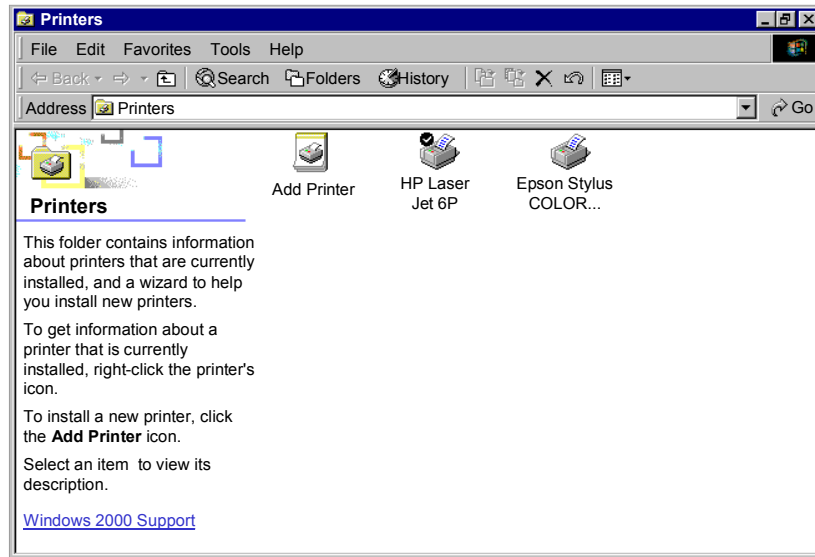
Printers

Topic Objective

To describe the tool to administer printers.

Lead-in

To administer printers, use the Printers tool in Control Panel.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

With Windows 2000, you can access printing resources across your entire network. Clients can use printers that are attached locally to a print server or they can access printers across the Internet. The printers may be connected to the network using internal or external network adapters or another server.

To access Printers

- From Control Panel, open **Printers**.

Windows 2000 supports several advanced features that aid in printer administration. For example, you can manage a print server that exists anywhere on your network without having to leave your office. In addition, you do not have to personally install a printer driver on a client computer to enable it to use a printer. Windows 2000 automatically downloads a driver when the client connects to a print server.

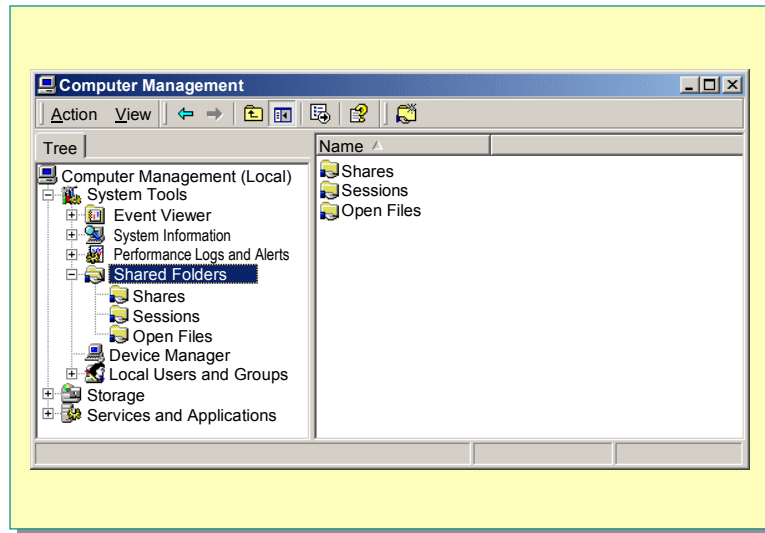
Shared Folders

Topic Objective

To introduce the Shared Folders utility.

Lead-in

The Shared Folders utility displays information about the files and folders shared across the network.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this utility. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Using Shared Folders, you can view the connections and resource use for local and remote computers. With Shared Folders, you can perform the following tasks:

- Create, view, and set permissions for *shares*. A share is a location on a computer that provides other computers with access to the information stored in it. The computer that needs to access the information on the share must have appropriate permissions to do so.
- View a list of all users who are connected to a computer network and disconnect one or all of them.
- View a list of files opened by remote users and close one or all of the open files.

To access Shared Folders

- From Control Panel, open **Administrative Tools**, **Computer Management**, **System Tools**, and then **Shared Folders**.

Shared Folders provides information, arranged in columns, about all the shares, sessions, and open files on the local computer.

- The Shares subfolder provides information about the shared resources available on the computer.
- The Sessions subfolder provides information about all network users connected to the computer.
- The Open Files subfolder provides information about all the open files on the computer.

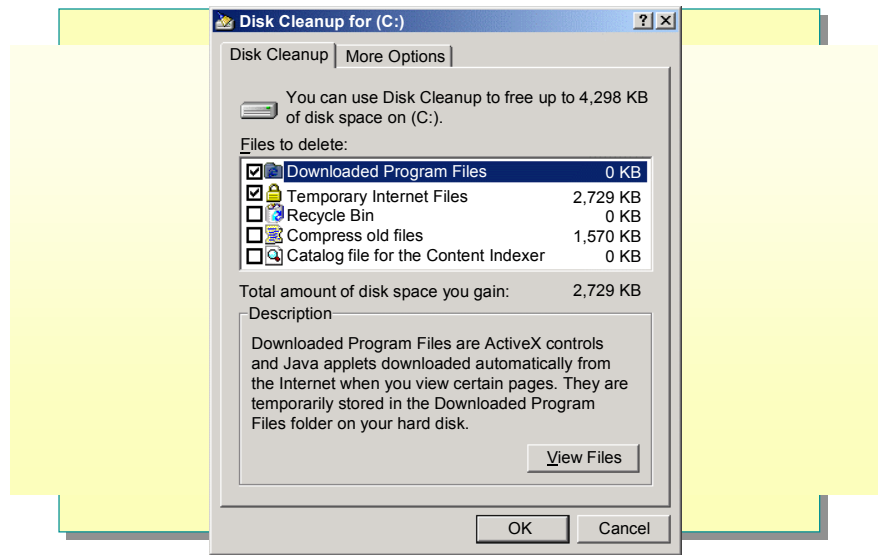
Disk Management

Topic Objective

To describe Disk Management.

Lead-in

You can manage the disk space on the system using the Disk Management utility.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Disk Management is a system utility for managing hard disks and the volumes, or partitions, they contain. With Disk Management, you can create volumes, format volumes with file systems, initialize disks, and create fault-tolerant disk systems.

When you right-click an object, the shortcut menu shows you which tasks you can perform on that object. Also, Disk Management has wizards, such as the Create Partition wizard, that guide you through the steps for creating volumes and initializing or upgrading disks.

To access Disk Management

- From Control Panel, open **Administrative Tools**, **Computer Management**, **Storage**, and then **Disk Management**.

Disk Defragmenter

Over a period of time, the files on the hard disk become fragmented. When fragmentation happens, pieces of a single file become located on different spots of the hard drive, much like a shredded document. Before the system can read the file, it must reassemble it, making the process much longer than when the file is intact. Disk Defragmenter reorganizes the files on your hard drive so that they are all contiguous pieces. As a result, the system can gain access to files and folders more rapidly and save new ones more efficiently.

To access Disk Defragmenter

- From Control Panel, open **Administrative Tools**, **Computer Management**, **Storage**, and then **Disk Defragmenter**.

Disk Cleanup

After a period of time, the hard disk may contain unnecessary files, which use up all the space on the hard disk. To free space occupied by unwanted files on the hard disk, you use the Disk Cleanup utility. Disk Cleanup searches your hard disk and then displays a list of temporary files, Internet cache files, and optional Windows components and applications that you do not use often that can be safely removed or deleted. You can direct Disk Cleanup to delete some or all of these files.

To access Disk Cleanup

- From **Start**, point to **Programs**, **Accessories**, and **System Tools**, and then click **Disk Cleanup**.

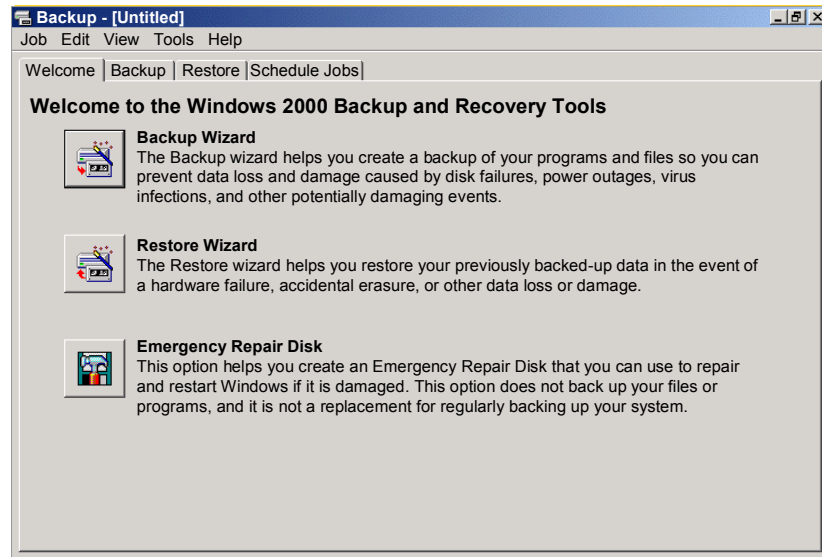
Backup

Topic Objective

To describe the functions of the Backup utility.

Lead-in

You can archive all system data using the Backup utility.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Explain that the Backup utility cannot be accessed from Control Panel, but all other tools can be. Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

The Backup utility helps you protect data from accidental loss if your system experiences hardware or storage media failure. You use the Backup utility to create a duplicate copy of the data that is stored on your hard disk, and then you store the data on another device, such as a hard disk or a tape. In the event that the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of hard disk malfunction, you can use the copy to restore your lost or damaged data.

The Backup utility provides wizards that prompt you through the steps to perform the backup and restore procedures. Using Backup, you can:

- Archive selected files and folders on your hard disk.
- Restore the archived files and folders to your hard disk or any other disk you have access to on the network.
- Create a disk that contains information about your current system settings. This disk is called the Emergency Repair Disk. You can use this disk to repair your computer if it will not start or if your system files are damaged or erased.
- Make a copy of important system-specific data, which includes the registry. Depending on the type of server and its role in the network, you can make a copy of the Microsoft Active Directory™ database and Certificate Services database.
- Schedule regular backups to update your stored data.

To access Backup

- From the **Start** menu, point to **Programs**, **Accessories**, and **System Tools**, and then click **Backup**.

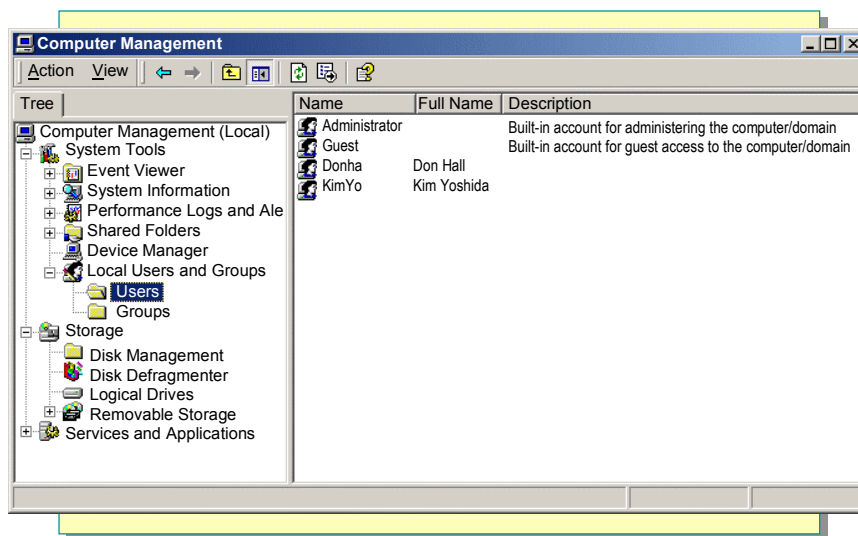
Security Management

Topic Objective

To describe the Security Management strategies.

Lead-in

Ensuring network security is one of the most important tasks of an administrator.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Mention that administrators can manage permissions to an object by using the **Security** tab in the **Properties** dialog box of each object that can be assigned permissions. Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Windows 2000 provides a number of utilities for monitoring and maintaining network security. These utilities include: the Local Users and Groups utility, the Active Directory Users and Computers utility, the Local Security Policy utility, and the Domain Security Policy utility.

Local Users and Groups

The Local Users and Groups utility allows administrators to manage the user and computer accounts on a local computer. Using this utility, you can add, disable, reset, and delete these accounts. You can use this utility only on Windows 2000-based computers that are not domain controllers.

To access Local Users and Groups

- On a local computer that is not part of a domain, from Control Panel, open **Administrative Tools**, **Computer Management**, and then **Local Users and Groups**.

Active Directory Users and Computers

Active Directory Users and Computers is a utility for managing user and computer accounts in a domain. Using this utility, the administrator can manage accounts from a central location. You can use this utility on Windows 2000-based computers that are domain controllers or on computers that have the administrative tools installed on them.

To access Active Directory Users and Computers

- From Control Panel, open **Administrative Tools**, and then **Active Directory Users and Computers**.

Local Security Policy

Local Security Policy is a utility used on individual computers that allows administrators to control how users interact with a computer. For example, you can create a policy to restrict the length of passwords, track access to areas of the system, and restrict the rights of users to log on to a computer or to gain access to computer resources.

To access Local Security Policy

- From Control Panel, open **Administrative Tools**, and then **Local Security Policy**.

Domain Security Policy

Domain Security Policy is a utility that allows administrators to control how users in the entire domain interact with the computers in the network and the domain. For example, you can control the length of passwords, track access to areas of the system, and restrict the rights of users to log on to a computer or to gain access to computer resources.

To access Domain Security Policy

- From Control Panel, open **Administrative Tools**, and then **Domain Security Policy**.

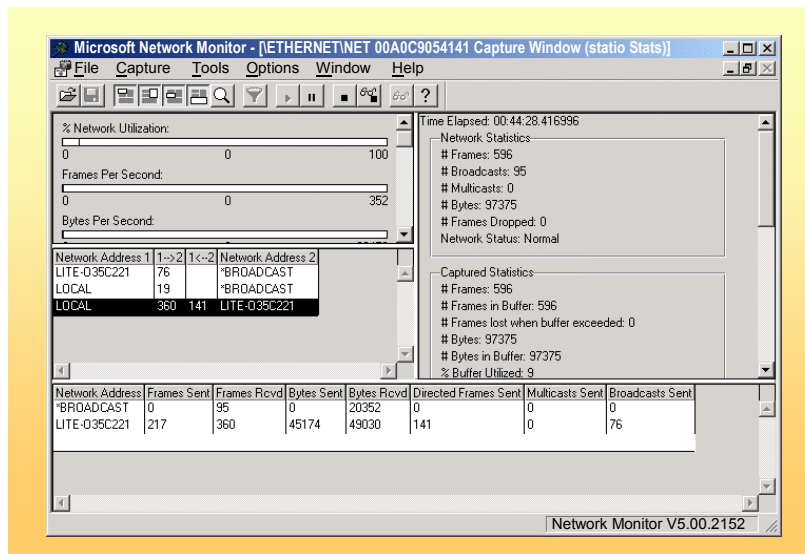
Network Tools

Topic Objective

To introduce the tools used to manage and monitor network activity.

Lead-in

You can monitor local and remote network connections by using the Network and Dial-up Connections feature.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Windows 2000 provides two tools—Network and Dial-up Connections and Network Monitor—for managing local and remote network connectivity and monitoring network activity.

Network and Dial-up Connections

Network and Dial-up Connections provides status or configuration information about connectivity between your computer and the Internet, a network, or another computer. You create, configure, store, and monitor all connections from within the Network and Dial-up Connections folder. With Network and Dial-up Connections, you can view the network connectivity configuration, whether you are physically located at the network or at a remote location.

To access Network and Dial-up Connections

- From Control Panel, open **Network and Dial-up Connections**.

Network Monitor

Network Monitor captures and displays the network traffic that a computer running Windows 2000 Server receives from a local area network (LAN). It enables you to monitor and, if desired, to save the information for later analysis. Network administrators use the information provided by Network Monitor to detect and troubleshoot networking problems experienced by the local computer. For example, you can use Network Monitor to diagnose problems that prevent a computer from communicating with other computers and to detect the reasons for delays in receiving data by portions of the network.

To access Network Monitor

- From **Start**, point to **Programs**, and **Administrative Tools**, and then click **Network Monitor**.

Additional Tools

Topic Objective

To describe the additional tools used by a network administrator.

Lead-in

In addition to the major administrative tools, you use specific tools to perform some useful tasks.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access this tool. Explain the text but do not go into detail. Provide only a high-level overview of the different options.

Some additional tools that perform useful tasks are the Configure Your Server and Add/Remove Programs utilities. You may also use non-Microsoft, third-party tools, such as virus-checking software.

Configure Your Server

This utility allows you to configure basic system information, including:

- Registering your copy of Windows 2000 so that you receive product updates.
- Upgrading to a domain controller by installing Active Directory.
- Running wizards that guide you in modifying and installing various services.

To access the Configure Your Server utility

- From Control Panel, open **Administrative Tools**, and then **Configure Your Server**.

Add/Remove Programs

This is a utility found on a client computer that helps you manage applications installed on the computer. It prompts you through the steps necessary to add a new application from a compact disc, floppy disk, or the network, or to change or remove an existing application.

Application-Specific Utilities

As a network administrator, you may occasionally need to use applications other than those available in Windows 2000 to meet specific server needs. Applications, such as Microsoft SQL Server™ and Microsoft Exchange, have their own utilities for managing the specific functions of these applications.

Third-Party Tools

Depending on the configuration and needs of your network, you may have third-party tools installed to provide additional functionality, such as protection from viruses. You use virus-checking applications to maintain the integrity of the data in the network.

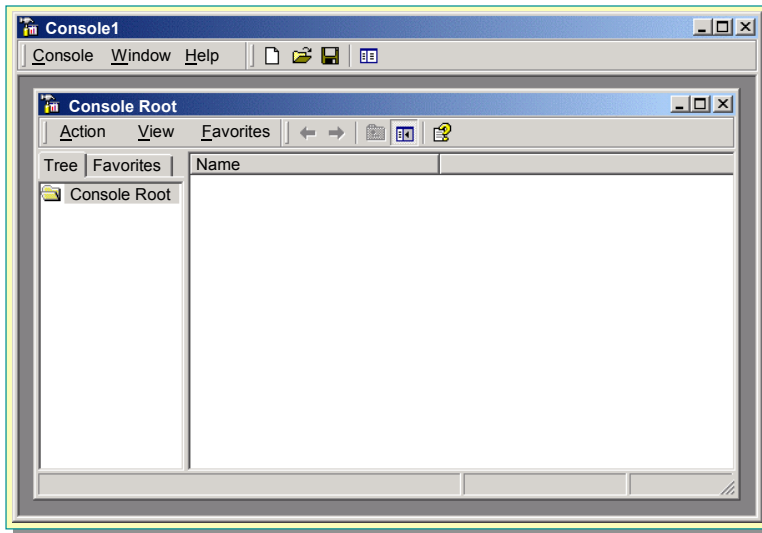
Microsoft Management Console

Topic Objective

To illustrate the Microsoft Management Console.

Lead-in

Windows 2000 provides the capability to customize a set of tools that meet your specific needs.



*****ILLEGAL FOR NON-TRAINER USE*****

Most of the tools that a network administrator needs to perform day-to-day tasks are available individually. Because all of the tools are not available in one location, Windows 2000 provides the capability to create a customized tool that contains all the required utilities. In this manner, the regularly accessed tools are all available at one location.

Another benefit of creating a customized tool is that an administrator can save the customized tool for later use and share the tool with other administrators and users. Also, administrators can create multiple tools of varying levels of complexity, which is useful for delegating tasks. To create a customized tool, you use the Microsoft Management Console (MMC). The customized tool that you create is called an MMC console and the primary tools that you add to it are called snap-ins. You can also add links to Web pages, folders, taskpad views, and tasks to an MMC console.

To create a customized console

1. In the **Run** dialog box, type **mmc**
2. On the **Console** menu, click **Add/Remove Snap-in**.

An MMC console consists of a window divided into two panes. The left pane is called the console tree and contains two tabs: **Tree** and **Favorites**. The console tree shows the items that are available in a given console. The right pane is called the details pane. The details pane shows information about the items in the console tree. The details pane can also display other types of information, including Web pages, graphics, charts, and tables.

Each console has its own set of menus and toolbars, separate from those of the main MMC window, that helps a user perform various tasks.

The Windows 2000 operating system has preconfigured and saved consoles available in the Administrative Tools folder in Control Panel. One such example is the Computer Management console.

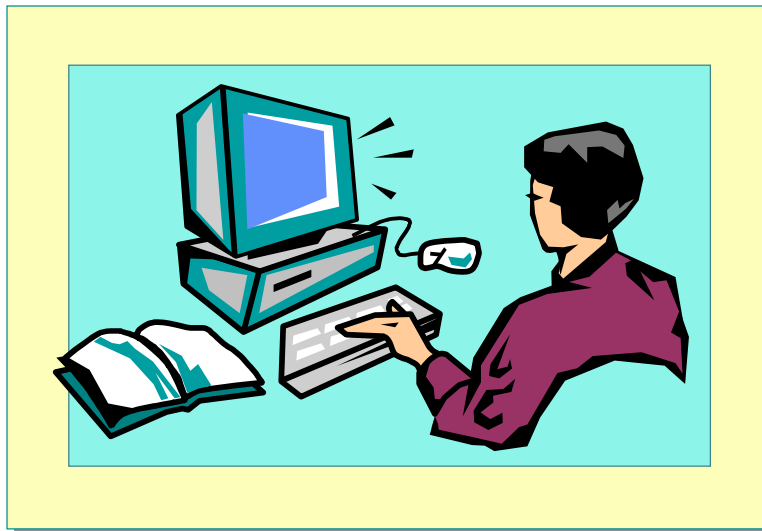
Lab B: Identifying Administrative Tools

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify various tools to perform administrative tasks.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify the common administrative tools in Windows 2000 and where they are located.

Estimated time to complete this lab: 15 minutes

Exercise 1

Identifying Administrative Tools

Scenario

As a new administrator, you need to familiarize yourself with the available administrative tools and their location in the interface.

Goal

In this exercise, you will open the various administrative tools and answer questions about them.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password , and then open Control Panel.	a. Log on to Windows 2000 as Administrator with a password of password . b. Click Start , point to Settings , and then click Control Panel .
 Which tool in Control Panel enables you to install additional printers or adjust the properties of existing ones? Printers. 	
 Which tool in Control Panel enables you to determine your computer name and enables you to adjust how applications use memory? System. 	
2. Open System in Control Panel.	a. In Control Panel, double-click the System icon.
 Which tab would you use to determine the domain to which the computer belongs? The Network Identification tab. 	

Tasks	Detailed Steps
3. Display the Network Identification tab.	a. Click the Network Identification tab.
? What domain is the computer a member of? Answers will vary.	
? Which tab in the System Properties dialog box enables you to install additional hardware? Hardware.	
4. Display the Hardware tab.	a. Click the Hardware tab.
? Which button do you click to install hardware? Hardware wizard.	
? Which button do you click to see the current status of devices installed on the system? Device Manager.	

Tasks	Detailed Steps
5. Display the User Profiles tab.	a. Click the User Profiles tab.
 How can you determine the number of users who have logged on to this computer? Because everyone who logs on to the computer has a profile, you can count the number of profiles stored on this computer. _____ _____ _____ _____	
6. Display the Advanced tab.	a. Click the Advanced tab.
 If you needed to adjust how the processor is utilized when running applications, which button on the Advanced tab would you click? The Performance Options button. _____ _____ _____ _____	
7. Close the System Properties dialog box to return to Control Panel.	a. Click Cancel .
 Which tool in Control Panel lets you modify or run tasks that have been set to run at a scheduled time? Scheduled Tasks. _____ _____ _____ _____	
 Which tool in Control Panel is actually a folder that contains additional administrative tools? Administrative Tools. _____ _____ _____ _____	

Tasks	Detailed Steps
8. Open the Administrative Tools folder.	a. Double-click the Administrative Tools folder.
? Which tool in the Administrative Tools folder (found on domain controllers) enables an administrator to manage domain user accounts? Active Directory Users and Computers. _____ _____ _____ _____	
9. Open Active Directory Users and Computers.	a. Double-click Active Directory Users and Computers.
? Which tool in the Administrative Tools folder enables you to manage shared folders on the server and administer the hard drive? Computer Management. _____ _____ _____ _____	
10. Open Computer Management.	a. Close Active Directory Users and Computers. b. Double-click Computer Management to open it. c. Maximize the Computer Management window.
? Which tool in Computer Management provides information about hardware, software, and system problems? Event Viewer. _____ _____ _____ _____	
11. Expand Event Viewer.	a. In the left pane, expand Event Viewer.  <i>The Event Viewer expands to show the various logs that it maintains.</i>

Tasks	Detailed Steps
 Which log contains events logged by Windows 2000 system components? System log.	
 Which tool in Computer Management enables you to create, view, and set permissions for shares on computers? Shared Folders.	
 Which tool in Computer Management enables you to manage partitions on your computer? Disk Management.	
 Which tool in Computer Management enables you to defragment your hard drive? Disk Defragmenter.	
12. Close Computer Management, and log off from Windows 2000.	a. Close Computer Management, and log off from Windows 2000.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Windows 2000 Help**
- **Administrative Tasks**
- **Administrative Tools**

*****ILLEGAL FOR NON-TRAINER USE*****

1. Mary wants to install some additional hardware in her computer but does not know the exact procedure to do so. How can she easily access information on installing additional hardware on her computer?

Mary can access information on installing a hardware device from Windows 2000 Help.

2. Which feature of Windows 2000 Help would you use to locate information on a specific topic?

The Search feature.

3. What is the purpose of user accounts?

User accounts enable users to log on to a server to access network resources or to log on to an individual computer to access resources on that computer.

4. You do not want to give all users on the network full access to resources. How can you ensure that users are able to access specific network resources depending on their job profile?

Assign user permissions so that you can control access to resources. This is done by determining the specific resources that each user can access and then specifying the kind of access that each user can have.

5. As an administrator, you perform some tasks that occur at frequent intervals. Which tool in Windows 2000 can you use to specify that these recurring tasks occur automatically?

Scheduled Tasks.

6. The System Information utility displays a comprehensive view of the hardware, system components, and software environment. What are the four top-level categories into which this information is organized?

System Summary.

Hardware Resources.

Components.

Software Environment.

7. While working with an application running on Windows 2000, the computer displays an Error event. By mistake, instead of reading the Error event, you close the application. How can you recover the Error event?

You use Event Viewer to locate the Error event. Information about the error is stored in the application log.

8. You are setting up a computer for a new employee. You need to create volumes, format volumes with file systems, and initialize disks. Which tool in Windows 2000 enables you to perform all of these tasks?

The Disk Management utility.

9. How can you protect crucial data from accidental loss if your system experiences hardware or storage media failure?

You can use the Backup utility to create a duplicate copy of data on a hard disk and store the data on another device, such as a different hard disk or a tape.

Module 3: Securing a Windows 2000 Network

Contents

Overview	1
User Accounts	2
Groups	7
Lab A: Examining Users and Groups	8
User Rights	10
Lab B: Examining User Rights	14
Permissions	17
Lab C: Examining File and Folder	
Permissions	27
Review	31



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
60 Minutes

Labs:
45 Minutes

This module provides students with a description of how Microsoft® Windows® 2000 protects network resources from unauthorized access. The module describes how the use of user accounts, passwords, and groups provides a secure network environment and how rights are granted to users and groups. The module also discusses permissions on files, folders, and printers.

At the end of this module, students will be able to:

- Describe the role and purpose of different types of user accounts.
- Describe the role and purpose of different types of groups.
- Identify common user and group rights.
- Describe file, folder, and shared folder permissions.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_03.ppt
- Module 3, “Securing a Windows 2000 Network”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Read the white paper, *Enterprise Class Storage in Windows 2000*, on the Trainer Materials compact disc.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **User Accounts**
Provide an overview of the different types of user accounts and their functions. Then introduce the tools used to create and modify the different types of user accounts.
- **Groups**
Define a group and describe how groups are used in a Microsoft Windows 2000 network. Explain the difference between groups located on computers that are domain controllers and groups located on computers that are not domain controllers.
- **User Rights**
Provide an overview of user rights. Then explain some of the common rights available in Windows 2000. Conclude by explaining how built-in groups are granted certain rights by default.
- **Permissions**
Explain how assigning permissions can control the type of access users have to network resources. Describe the objects to which you can apply permissions (printers, files and folders) and the different permissions that you can apply to each.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives

Lead-in

User accounts, groups, rights, and permissions are ways to establish security in a Windows 2000 network.

- User Accounts
- Groups
- User Rights
- Permissions

*****ILLEGAL FOR NON-TRAINER USE*****

To protect network resources from unauthorized access, the identity of each user accessing the network must be verified when logging on. Each user must have a valid account name and correct password. The account name identifies each unique user in a domain. The password keeps the use of that account private, so that only users who know the password can use the account. After the user's identity is verified, the user's access to computers on the network is authenticated.

To facilitate network administration, you can organize users into groups and assign permissions to these groups to access network resources. You can control the kinds of actions users perform on the network by granting appropriate user rights.

To further ensure security, you can protect network resources with file, folder, and shared folder permissions.

At the end of this module, you will be able to:

- Describe the role and purpose of different types of user accounts.
- Describe the role and purpose of different types of groups.
- Identify common user rights and rights for each built-in group.
- Describe file, folder, and shared folder permissions.

◆ User Accounts

Topic Objective

To introduce the concepts of local and domain user accounts.

Lead-in

In a Windows 2000 network, there are two kinds of user accounts: local user accounts and domain user accounts.

- Local User Accounts
- Domain User Accounts

*****ILLEGAL FOR NON-TRAINER USE*****

User accounts enable individual users to access network resources. A user account is the user's unique set of credentials that is recognized by the network. An administrator creates user accounts for each person who regularly uses the network. The administrator also assigns and maintains user names and passwords for each user account. Microsoft® Windows® 2000 provides two types of user accounts: local user accounts and domain user accounts.

With a local user account, an account is created in the local security database, which gives the user the ability to log on to a specific computer and gain access to resources on that computer. This typically occurs in a workgroup. If the computer is a member of a workgroup, the account is stored on the local computer. With this account, a user has access to only the resources on that computer.

With a domain user account, a user can log on to the domain to access network resources. A user with a domain account can access all of the resources in the domain.

In a domain, it is possible to have both a domain user account and a user account on the local computer. An administrator can create these accounts, which are called user-defined accounts. A user's account can be stored in one of two places: the local security database if the computer is not a domain controller or in the Microsoft Active Directory™ directory service.

In addition to the user-defined user accounts, Windows 2000 provides two default built-in user accounts. These accounts can be used to perform administrative tasks or to gain temporary access to network resources. There are built-in user accounts for both local computers and domains.

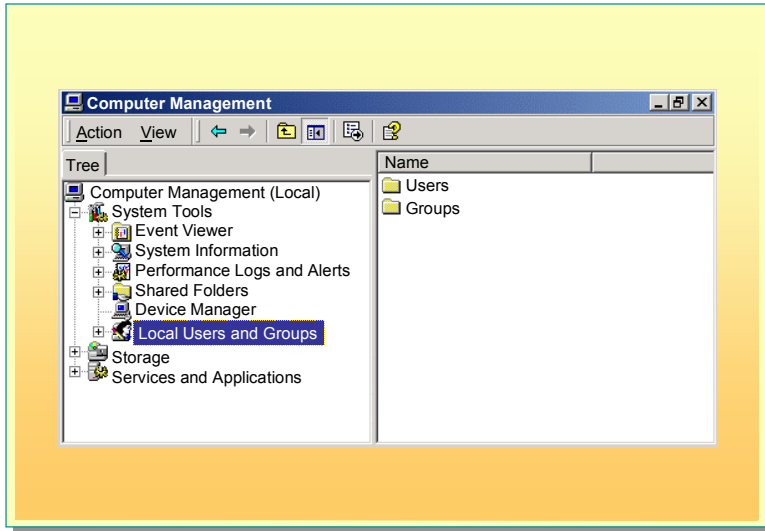
Local User Accounts

Topic Objective

To describe the use of local user accounts.

Lead-in

A person with a local user account can gain access only to the resources of a specific computer.



*****ILLEGAL FOR NON-TRAINER USE*****

To gain access to resources on a local computer, a user needs to have a local user account on the computer. There are two kinds of local user accounts: user-defined accounts and built-in accounts. When an account is created, it exists only in the local security database on that computer.

Delivery Tip

Remind the students that there are differences between a workgroup and a domain and that there are different tools for administering each.

User-defined Local User Accounts

User-defined local user accounts are those that an administrator creates to allow a user to gain access to only those computers where his or her user account exists. You can create local user accounts on member servers and computers running Microsoft Windows 2000 Professional, but not on computers that are domain controllers. A local user account is used only on stand-alone computers or on computers in a small network environment, such as a workgroup. It is possible to have an account on the local computer and another account in the domain; however, the user can use only one of the accounts at a time. The user determines which account to use when logging on the computer.

Built-in (Local) User Accounts

In addition to allowing user-defined accounts, Windows 2000 provides two built-in user accounts to aid administrators in performing administrative tasks and in providing users with temporary access to a local computer. Upon installation, Windows 2000 automatically creates two built-in user accounts—Administrator and Guest.

Administrator

Administrators use the built-in Administrator user account to create an account for themselves on computers on which Windows 2000 has been newly installed. The built-in Administrator account can never be deleted or disabled, thereby ensuring that the administrator is never locked out of the computer. This account requires a password, which an administrator provides at the time of installation.

Guest

Users who do not have a user account on a computer can log on using the Guest account. A user whose account is disabled can also use the Guest account. For a user to log on as a Guest, the administrator needs to enable the Guest account because it is disabled by default. This account does not require a password.

Local Users and Groups Utility

Windows 2000 provides a utility called Local Users and Groups that administrators can use to manage user accounts on a local computer. The Local Users and Groups utility is available on computers running Windows 2000 Professional and on member servers running Microsoft Windows 2000 Server. You can use the Local Users and Groups utility to perform the following tasks:

- Create a new user account or delete an existing user account
- Modify a user account by changing the user name or other account information, such as the password or description
- Reset the password for a user account
- Disable or enable a user account

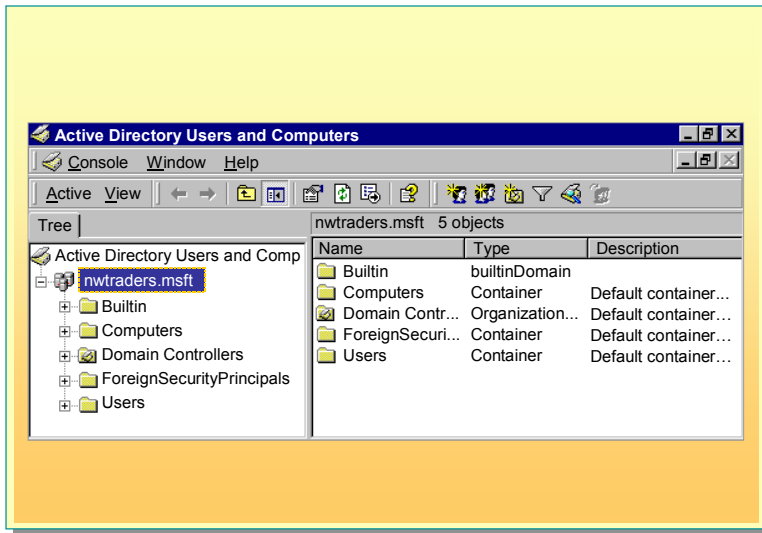
Domain User Accounts

Topic Objective

To describe the use of domain user accounts.

Lead-in

A person with a domain user account can access the resources of the domain.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Refresh the students' memory by asking questions about what a domain is and what its features are.

A local user account allows a user to log on to a local computer to access local resources. However, in a network environment, users need to access resources located anywhere on the network. To access these resources, you need to use a domain user account. When a domain user account is created, it exists in Active Directory and is accessible from anywhere in the domain. By contrast, in a workgroup, the user account exists only on the local computer.

User-defined Domain Accounts

User-defined domain accounts are those that an administrator creates to allow users to log on to a domain and access resources anywhere on the network. User-defined domain accounts are created on a domain controller. The domain controller replicates the new user account information to all domain controllers in the domain. During the logon process, the user provides the user name and password and identifies the domain in which the account exists. The first available domain controller uses this information to validate the user account.

Built-in (Domain) User Accounts

In addition to allowing administrators to define new domain user accounts, Windows 2000 provides two built-in domain user accounts—Administrator and Guest. These built-in user accounts are similar to the built-in user accounts available on local computers in workgroups. The main difference is that these accounts enable access to the entire domain.

Administrator

The built-in Administrator account manages the overall computer and domain configuration. Using this account, an administrator can create and modify user accounts and groups, manage security, administer printers, and assign permissions to user accounts. You can rename this account, but you cannot delete it.

Guest

The built-in Guest account enables occasional users to access network resources. For example, in a low security environment, an employee who needs to access resources for a short time can use the Guest account. This account is disabled by default.

Active Directory Users and Computers Utility

Windows 2000 provides a utility called Active Directory Users and Computers that administrators can use to manage user accounts in Active Directory.

This utility is installed on computers configured as domain controllers. To use the Active Directory Users and Computers utility, you must be logged on to a Windows 2000 domain (not the local computer) and have sufficient permissions to perform the particular operation.

You can use the Active Directory Users and Computers utility to perform the following tasks in the domain:

- Add or delete user accounts
- Enable or disable user accounts
- Find or move user accounts
- Rename user accounts
- Reset user passwords

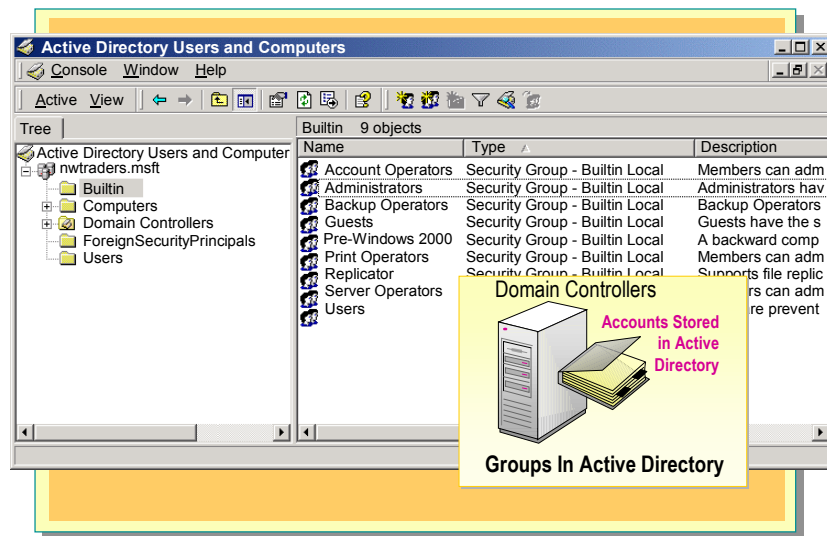
Groups

Topic Objective

To introduce the use of groups for Windows 2000 network administration.

Lead-in

You will find it easier to administer users by organizing them into groups.



*****ILLEGAL FOR NON-TRAINER USE*****

A *group* is a collection of user accounts. You can assign access permission to all members of a group at one time, so that you do not need to assign the permissions individually. After you provide access to a group, you can simply add appropriate users to that group. You can use the default, or built-in, groups that Windows 2000 provides, or you can create new groups to meet your organization's needs.

A group can exist on a local computer only, on computers within a single domain, or on computers across multiple domains.

Groups on a Local Computer

On local computers (computers that are not domain controllers), you can create only local groups in the local security database. A group located on a computer that is not a domain controller provides security and access for the local computer only. For example, to grant administrative permissions on a local computer to a user, you add the user to the Administrators group on that computer by using the Local Users and Groups utility.

Groups on a Domain Controller

On a domain controller, you create groups in Active Directory. A group that exists on a domain controller can include users throughout the entire domain or across multiple domains. For example, to provide users with administrative privileges, you add them to the Administrators group on a domain controller by using the Active Directory Users and Computers utility.

Lab A: Examining Users and Groups

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the key properties of user and group accounts.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify key properties of user and group accounts.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Examining Domain User and Group Accounts

Scenario

You have been assigned the task of managing the Sales and Managers organizational units and need to find out which objects are contained in them. You will use Active Directory Users and Computers to view the organizational units.

Goal

In this exercise, you will examine the various organizational units that exist in the domain and record selected information about them.

Tasks	Detailed Steps
1. Open Active Directory Users and Computers, and determine which objects are contained in the Managers organizational unit.	- Log on as Administrator with a password of password. - Click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers. - Maximize the Active Directory Users and Computers window. - In the console tree, click Managers.
 Examine the objects in the details pane of Active Directory Users and Computers. For which user accounts are you responsible? For which groups? You are responsible for the user accounts Jae Pak and Kim Yoshida, and for the Managers group. 	
2. Determine which accounts are contained in the Sales organizational unit.	In the console tree, click Sales.
 Examine the objects in the details pane of Active Directory Users and Computers. For which user accounts are you responsible? For which groups? You are responsible for the user accounts Anne Paper and Don Hall, and for the Sales group. 	
3. Close all windows and log off from Windows 2000	Close all windows and log off from Windows 2000.

◆ User Rights

Topic Objective

To introduce the concepts of user rights and of the rights assigned to built-in groups.

Lead-in

Rights apply to the entire system, rather than to a specific resource, and affect the overall operation of the computer or domain.

- **Common User Rights**
- **Rights Assigned to Built-in Groups**

*****ILLEGAL FOR NON-TRAINER USE*****

Rights apply to the entire system, rather than to a specific resource, and affect the overall operation of the computer or domain. All users accessing network resources need to have certain common rights on the computers they use, such as the right to log on to the computer or change the system time of the computer. Administrators can grant specific common user rights to user groups or to individual users. Additionally, Windows 2000 grants certain rights to built-in groups by default. User rights determine which users can perform a specific task on a computer or in a domain.

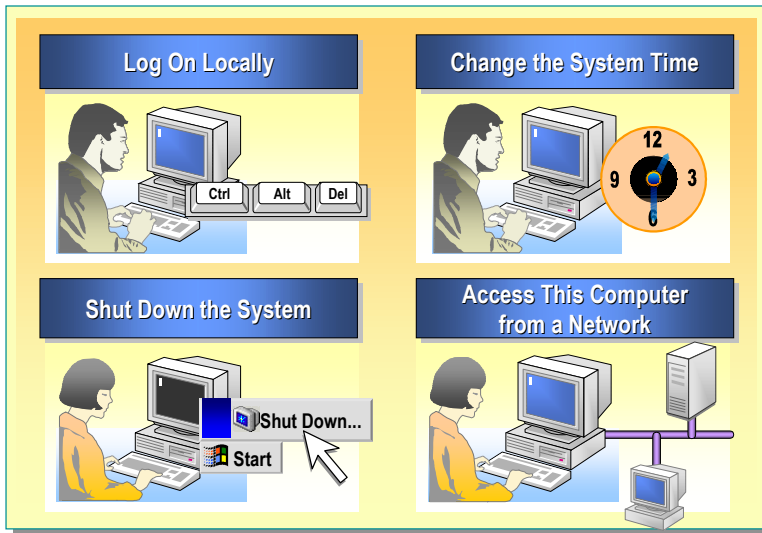
Common User Rights

Topic Objective

To identify common user rights.

Lead-in

Rights authorize users to perform certain actions on the system.



*****ILLEGAL FOR NON-TRAINER USE*****

A right authorizes a user who is logged on to a computer or a network to perform certain actions on the system. If a user does not have the appropriate rights to perform an action, attempts to carry out the action are blocked.

User rights can apply both to individual users and to groups. However, user rights are best administered on a group basis. This ensures that a user who logs on as a member of a group automatically receives the rights associated with that group. Windows 2000 allows an administrator to assign rights to users and user groups. Common user rights include the Log on locally user right, the Change the system time user right, the Shut down the system user right, and the Access this computer from a network user right.

- Log on locally

This right allows a user to log on to the local computer or to the domain from a local computer.

- Change the system time

This right allows a user to set the time for the internal clock of a computer.

- Shut down the system

This right allows a user to shut down a local computer.

- Access this computer from a network

This right allows a user to gain access to a computer running Windows 2000 from any other computer on the network.

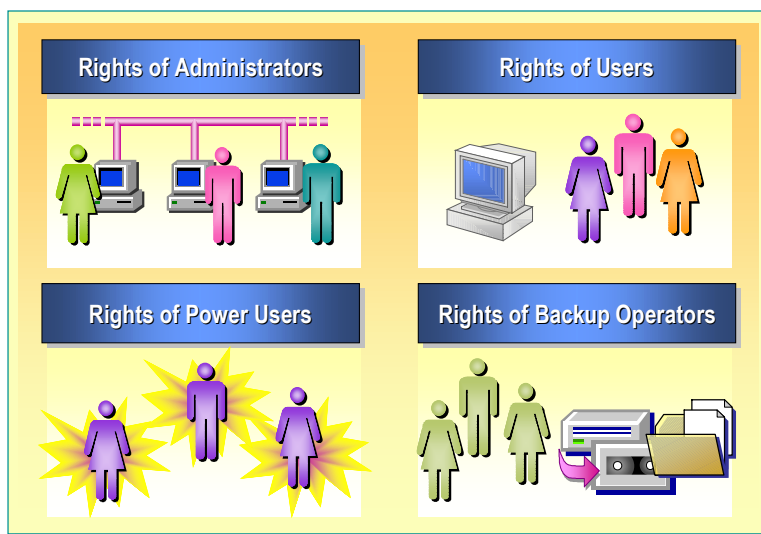
Rights Assigned to Built-in Groups

Topic Objective

To identify the rights of built-in groups.

Lead-in

Built-in groups have certain rights by default.



*****ILLEGAL FOR NON-TRAINER USE*****

By default, Windows 2000 grants certain rights to such built-in groups as Administrators, Users, Power Users, and Backup Operators.

Administrators

Administrators is a built-in group that exists both on computers that are domain controllers as well as on computers that are not domain controllers. Members of the Administrators group have full control over the computer or the domain. The Administrators group is the only built-in group that is automatically granted every built-in right in the system.

Users

Users is a built-in group that exists both on computers that are domain controllers as well as on computers that are not domain controllers. Members of the Users group can perform only those tasks for which they have been granted specific rights, such as running applications, using local and network printers, and shutting down and locking workstations. Members of the Users group can create local groups and can modify them, but they cannot share folders or create local printers.

Power Users

Power Users is a built-in group that exists on computers that are not domain controllers. Members of the Power Users group may perform specific administrative functions, but they do not have rights that grant them complete control over the system. Rights of the Power Users group include:

- Creating user accounts and groups on the local computer.
- Modifying and deleting the accounts that they create.
- Sharing resources.

However, members of the Power Users group cannot:

- Modify the Administrators or Backup Operators groups.
- Back up or restore folders.

Backup Operators

Backup Operators is a built-in group existing both on computers that are domain controllers and on computers that are not domain controllers. Members of the Backup Operators group can back up and restore files on the computer, regardless of the permissions that protect those files. Members of the Backup Operators group can also log on to the computer and shut down the computer, but they cannot alter security settings.

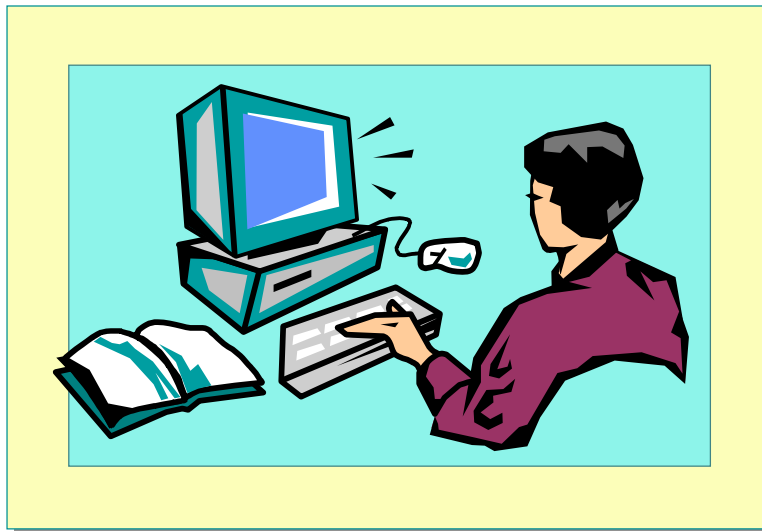
Lab B: Examining User Rights

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will examine user rights.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Describe the effect user rights has on user accounts.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Verifying User Rights

Scenario

Another administrator has created several user accounts for your domain. You now need to test the effects of the user rights assigned to those user accounts.

Goal

In this exercise, you will log on as two different users and test to see whether the users have specific user rights granted to them.

Tasks	Detailed Steps
1. Log on as Kimyo with a password of password . Attempt to change the system time.	a. Log on to the computer using the following credentials: Username: kimyo Password: password Domain: <i>domainname</i> (where <i>domainname</i> is the name of your domain). b. Click Start, point to Settings, and then click Control Panel. c. In Control Panel, double-click Date/Time.
 What message appears when you try to change the system time? Why? You do not have the proper privilege level to change the system time. Because the user Kimyo does not have the user right to change the system time. _____ _____	
2. Attempt to run the Add/Remove Hardware wizard.	a. In Control Panel, double-click Add/Remove Hardware .
 Does the user Kimyo have the right to add new hardware using the Add/Remove Hardware wizard? Why might you want to restrict this right? No. To prevent unauthorized users from making critical changes to the system, which can affect system operation and performance. _____ _____ _____ _____	

Tasks	Detailed Steps
3. Attempt to log on as user Donha.	a. Log off the computer. b. Log on to the computer using the following credentials: Username: donha Password: password Domain: <i>domainname.nwtraders.msft</i> (where <i>domainname</i> is the name of your domain).
 Can Donha log on to the computer? Why or why not? No. Donha does not have the right to log on interactively. _____ _____ _____ _____	
4. Close the message box.	a. Click OK to close the message box.

◆ Permissions

Topic Objective

To introduce the use of permissions in a network.

Lead-in

You use permissions to control user access to network resources.

- Introduction to Permissions
- NTFS File Permissions
- NTFS Folder Permissions
- Shared Folder Permissions
- Printer Permissions

*****ILLEGAL FOR NON-TRAINER USE*****

When you provide access to file resources on a computer running Windows 2000, you can control who has access to resources and the nature of their access by assigning the appropriate permissions. Permissions define the type of access assigned to a user or group for any resource. For example, users in the human resources (HR) department of an organization might need to modify the company's HR policies document. To facilitate this, the administrator needs to assign the appropriate permission to the members of the HR department.

In order to assign permissions to individual files and folders, Windows 2000 uses the NTFS file system. You can also control the permissions assigned to users for accessing shared folder resources and network printers.

Introduction to Permissions

Topic Objective

To describe object permissions.

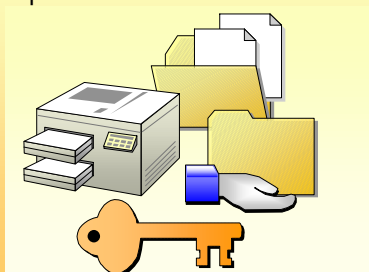
Lead-in

Permissions are used to control who has access to objects in the network and define what type of access is allowed.

Permissions to access an object may be assigned to either a user or a group.

■ Object Permissions

- Permissions granted for the object
- Object is an entity, such as a file, folder, shared folder, or printer



*****ILLEGAL FOR NON-TRAINER USE*****

Permissions define the type of access a user or a group has to an object. The type of permissions that you can assign to a user depends on the type of object.

Object Permissions

An object is defined as an entity, such as a file, folder, shared folder, or printer. The permissions that are assigned to a user for the objects are called object permissions.

You can assign permissions for objects in Active Directory or on a local computer. When assigning permissions, it is best to assign permissions to a group of users instead of to individual users. Using groups in this way eases the task of managing permissions on objects.

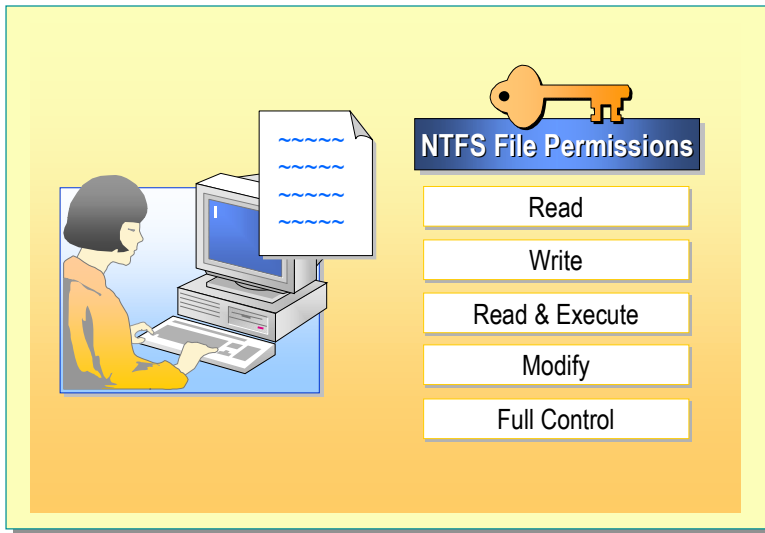
NTFS File Permissions

Topic Objective

To describe NTFS file permissions.

Lead-in

You can use NTFS file permissions to control user access to files on an NTFS partition.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to view NTFS file permissions. At this point it is not necessary to explain the details of how to set the permissions.

NTFS file permissions control access to individual files by specifying which users can access them and what kind of access the users can have.

Note For more information about NTFS, see *File and Print Services Technical Overview* under **Additional Reading** on the Web page on the Student Materials compact disc.

The following table lists the standard NTFS file permissions and the type of access that each permits, from the most restrictive to the least restrictive permissions.

NTFS file permission	Allows a user to
Read	Read the file and view file attributes, ownership, and permissions.
Write	Overwrite the file, change file attributes, and view file ownership and permissions.
Read & Execute	Run applications and perform the actions permitted by the Read permission.
Modify	Modify and delete the file and perform the actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, and perform the actions permitted by all other NTFS file permissions.

Verifying File Permissions

An administrator assigns permissions to a file from the **Security** tab of the **Properties** dialog box for the file. You can also view the current permissions to the file on the same tab.

To access the Security tab

1. In Windows Explorer, right-click the file.
2. Click **Properties**.
3. In the **Properties** dialog box, click the **Security** tab.

The **Security** tab consists of two sections—Name and Permissions. The Name section displays a list of existing users or groups who have permissions to the file. The Permissions section displays a list of permissions that you can grant or deny to the user or group.

You normally select the permissions that you want to grant. However, in some cases it may be easier to specify the permissions you want to deny. For example, although you allow everyone access to a file, you may need to restrict any users who connect to the resource using the Guest account. To do this, you deny permission to the Guest account.

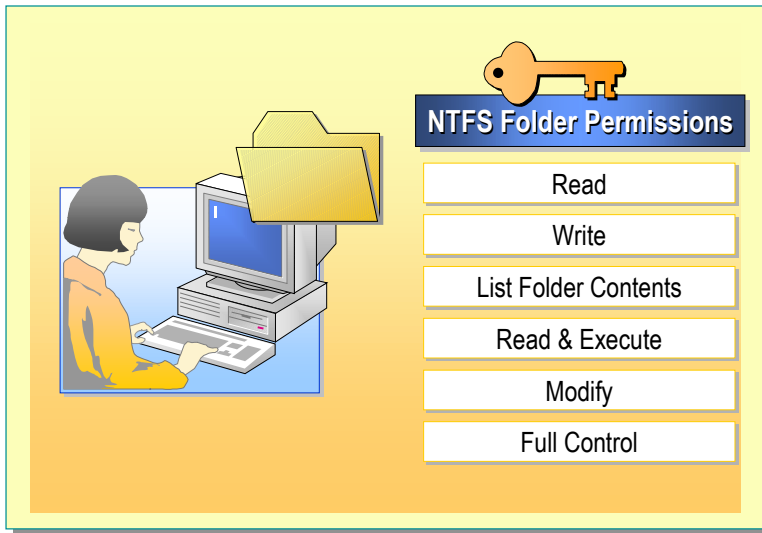
NTFS Folder Permissions

Topic Objective

To describe NTFS folder permissions.

Lead-in

You can use NTFS folder permissions to control user access to folders on an NTFS partition.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure for viewing NTFS folder permissions. Point out the permissions but do not explain how to set the permissions.

NTFS folder permissions control user access to folders and to the files and subfolders contained within them. If permission is denied to a file that is inside a folder that has an Allow permission, the Deny attribute takes precedence over the Allow permission applied to the folder.

The following table lists the standard NTFS folder permissions and the type of access that each provides, from the most restrictive to the least restrictive permissions.

NTFS folder permission	Allows a user to
Read	See files and subfolders in the folder and view folder ownership, permissions, and attributes, such as Read-Only, Hidden, Archive, and System.
Write	Create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
List Folder Contents	View the names of files and subfolders in the folder.
Read & Execute	Move through folders to reach other files and folders, plus perform actions permitted by the Read permission and the List Folder Contents permission.
Modify	Delete the folder and perform actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions.

Verifying Folder Permissions

An administrator assigns permissions to a folder from the **Security** tab of the **Properties** dialog box for the folder. You can also view the current folder permissions in the same dialog box.

To access the Security tab

1. In Windows Explorer, right-click the folder.
2. Click **Properties**.
3. In the **Properties** dialog box, click the **Security** tab.

The **Security** tab consists of two sections—Name and Permissions. The Name section displays a list of existing users or groups who have permissions to the folder. The Permissions section displays a list of permissions granted or denied to the user or group.

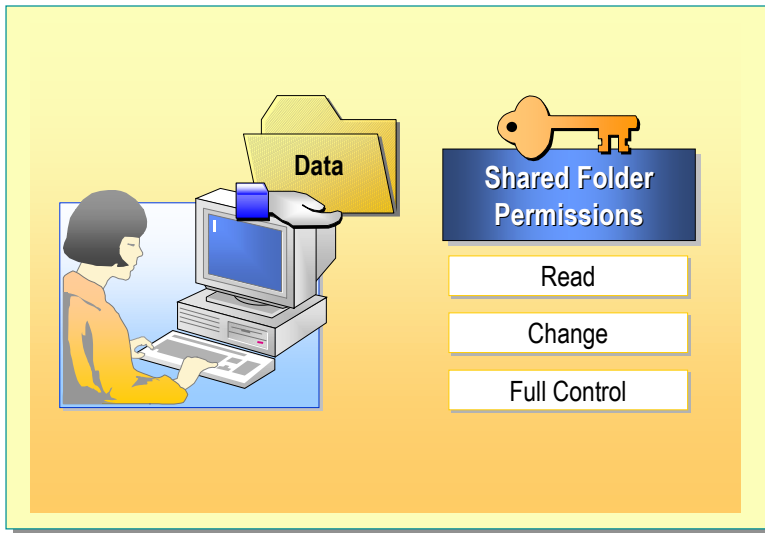
Shared Folder Permissions

Topic Objective

To describe shared folder permissions.

Lead-in

Use permissions to shared folders to provide access to network resources.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure for viewing shared folder permissions. Point out the shared resources but do not explain the details of how to set the permissions.

To provide multiple users with access to the same resource, such as a folder, you must share the folder. Sharing a folder refers to the process by which the folder is made accessible to multiple users simultaneously over the network. After a folder is shared, users can access all of the files and subfolders within the shared folder if they have been granted permission.

You can only share folders, not individual files. If multiple users need access to the same file, you must enclose the file in a folder and then share the folder.

Shared Folders

Shared folders are usually placed on a file server, but you can also place them on any computer on the network. You can store files in shared folders according to categories or functions. For example, you can place shared data files in one shared folder and shared application files in another.

Some of the characteristics of shared folders are listed below:

- A shared folder appears in Microsoft Windows Explorer with an icon of a hand holding the folder.
- Permissions are assigned to the entire folder only, not to individual files or subfolders within the shared folder.
- When a folder is shared, the Full Control permission is assigned to the Everyone group as the default permission.

- When a user is added to a shared folder, the user receives the Read permission by default.
- When a shared folder is copied, the original shared folder is still shared, but the copy is not shared. When a shared folder is moved to another location, the folder is no longer shared.

You can control the level of access to a shared folder by assigning permissions to it. The following table lists the shared folder permissions and the tasks they enable a user to perform.

Shared folder permission	Allows a user to
Read	Display folder names, file names, file data, and attributes; run application files; and change folders within the shared folder.
Change	Create folders, add files to folders, change data in files, append data to files, change file attributes, delete folders and files, and perform actions permitted by the Read permission.
Full Control	Change file permissions, take ownership of files, and perform all tasks permitted by the Change permission.

Note Shared folder permissions can be granted or denied to users. To deny all access to a shared folder, deny the Full Control permission.

Verifying Shared Folder Permissions

After creating a shared folder, an administrator can assign shared folder permissions to users and groups from the **Permissions** dialog box of the shared folder. You can view existing shared folder permissions in this dialog box as well.

To verify permissions assigned to users and groups for a shared folder

1. In Windows Explorer, right-click the shared folder.
2. Click **Properties**.
3. On the **Sharing** tab of the **Properties** dialog box, click **Permissions**.
4. Select the user account or group for which you want to view permissions.

Printer Permissions

Topic Objective

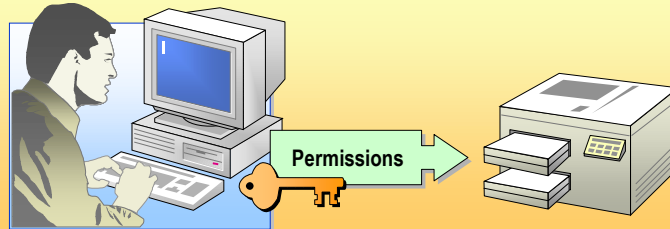
To describe the levels of printer permissions.

Lead-in

You can assign three levels of printer permissions.

Three levels of printer permissions

- Print
- Manage Documents
- Manage Printers



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the user interface for printer permissions.

In addition to assigning permissions on shared folders, an administrator also needs to assign permissions on printers. These permissions are assigned to users who are not administrators. Printer permissions control the types of printing activities users may perform and also can be used to limit user access to certain printers for security reasons.

Levels of Printer Permissions

Windows 2000 provides three levels of printer permissions—Print, Manage Documents, and Manage Printers.

Print

The Print permission allows you to connect to a printer. It also allows you to print and cancel your own documents.

Manage Documents

The Manage Documents permission allows you to connect to a printer. It also allows you to pause, resume, restart, and cancel printing of all documents.

Manage Printers

The Manage Printers permission allows you to perform all of the tasks that the Print and Manage Documents permissions allow. In addition, this permission allows you to share a printer, change printer properties, delete a printer, and change printer permissions.

Verifying Printer Permissions

You can assign printer permissions to individual users or to groups. By default, Windows 2000 assigns the Print permission for each printer to the built-in Everyone group, thereby allowing all users to send documents to each printer. However, an administrator can change these permissions if there is a need to restrict printer access to specific users or groups. For example, an administrator might need to limit the use of a color printer to users from the marketing department. In this case, the default permission of the Everyone group can be removed and permission can be assigned exclusively to the Marketing group.

To view existing printer permissions

1. On the **Start** menu, point to **Search**, and then click **For Printers** to display the **Find Printers** dialog box.
2. In the **Name** box on the **Printers** tab, type the printer name, and then click **Find Now**.
3. Right-click the printer name, and then click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab. Here you can view existing printer permissions for users and groups.

Lab C: Examining File and Folder Permissions

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will explore file and folder permissions.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Describe the function of file and folder permissions.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Microsoft Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Examining File and Folder Permissions

Scenario

You want to determine whether you are able to create files within various folders.

Goal

In this exercise, you will examine the permissions on files and folders and verify the effect of those permissions on day-to-day tasks. You will use the following chart to determine which users are in the different groups for the exercise.

Groups	Users in the Groups
Sales	Don Hall Anne Paper
Managers	Jae Pak Kim Yoshida

Tasks	Detailed Steps
1. Log on as user Kimyo with a password of password . Create a text file called Meeting.txt in the folder C:\MOC\WIN2151A\labfiles\lab03\managers.	a. Log on to the computer using the following credentials: Username: kimyo Password: password Domain: <i>domainname.nwtraders.msft</i> (where <i>domainname</i> is the name of your domain). b. Using Windows Explorer, open the folder C:\moc\win2151a\labfiles\lab03\managers. c. Right-click the Managers window, point to New , and then click Text Document . d. Type meeting and then press ENTER.
 To create the file in this folder, you must have the appropriate permissions for the Managers folder. What permissions should be assigned to the user Kimyo for the Managers folder? Read and Write permissions. 	
2. Examine the permissions for the folder C:\MOC\WIN2151A\labfiles\lab03\managers.	a. Using Windows Explorer, open the folder C:\MOC\WIN2151A\labfiles\lab03. b. Right-click the Managers folder, and then click Properties . c. Click the Security tab.

Tasks	Detailed Steps
? Notice the entries in the Security tab. Are the entries for users or for groups? How can you tell? Groups. The entries have the icon representing groups. Which group has Full Control permissions? Is the user Kimyo a member of that group? Managers. Yes, Kimyo is a member of the Managers group. This can be verified in the table at the beginning of the exercise.	
2. (continued)	d. Click Cancel to close the Managers Properties window.
3. Attempt to create a file called Meetings1.txt in the folder C:\MOC\WIN2151A\labfiles\lab03\sales.	a. Using Windows Explorer, open the folder C:\MOC\WIN2151A\labfiles\lab03\sales. b. Right-click the Sales window, point to New, and then click Text Document.
? Can user Kimyo create a file in this folder? What permission does Kimyo need to create a file in this folder? No. Kimyo will need at least the Write permission to create a file in this folder.	
3. (continued)	c. Click OK to close the Sales message box.
4. Examine the permissions for the folder C:\MOC\WIN2151A\labfiles\lab03\sales.	a. Using Windows Explorer, open the folder C:\MOC\WIN2151A\labfiles\lab03. b. Right-click the Sales folder, and then click Properties. c. Click the Security tab. d. Click Managers in the Name window.
? Which permissions does the Managers group have for the Sales folder? Read and Execute, List Folder Contents, and Read permissions.	

Tasks	Detailed Steps
 Which permissions does the Sales group have for the Sales folder? Full Control permissions. _____ _____ _____ _____	
4. (continued)	e. Click Cancel to close the Sales Properties dialog box. f. Close all open windows and log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- User Accounts
- Groups
- User Rights
- Permissions

*****ILLEGAL FOR NON-TRAINER USE*****

1. Two new employees have joined the marketing department. The network administrator needs to create user accounts for them, so that they can access such network resources as shared folders and printers. Which type of user accounts should the network administrator create for the new employees?
 - a. Domain user accounts.
 - b. Local user accounts.
 - c. Built-in Administrator accounts.
 - d. Built-in Guest accounts.

A is the correct answer. With the domain account, the new employees will be able to access resources throughout the network. If they have an account on only the local computer, they will be able to access resources on only the local computer.

2. The network administrator has set up a computer to run Windows 2000 Server. Which of the following accounts does she use to access the computer, before creating an account for herself?
 - a. Domain user account.
 - b. Local user account.
 - c. Built-in Administrator account.
 - d. Built-in Guest account.

C is the correct answer. When the computer is first installed, only two accounts exist—the built-in Administrator account and the built-in Guest account. Of the two, only the Administrator account has the appropriate rights to log on and manage the computer.

3. A new trainee has joined the network administration team. The network administrator wants this trainee to be able to perform all common administrative tasks in the domain, such as creating and modifying user accounts and user groups and sharing resources. However, he does not want the trainee to have full control over the system. The trainee should not be able to modify the Administrator or Backup Operators group or to manage the security auditing logs. What can the administrator do to achieve this? Select all that apply.
- a. Grant appropriate rights directly to the trainee.
 - b. Add the trainee to the built-in Power Users group.
 - c. Add the trainee to the Administrators group.
 - d. Create a new group and add the trainee to the group. Then grant appropriate rights to the group.

A & D are the correct answers. The administrator can grant the appropriate rights directly to the trainee, but trainee permissions will be easier to manage if the administrator creates a group, puts the appropriate users in the group, and then grants rights to the group a single time instead of multiple times. The Power Users group exists only on computers that are not domain controllers and does not provide any rights in the domain, only on the local computer. If the administrator adds the trainee to the Administrators group, the trainee will have full control over the domain.

4. The annual audit is going to take place in your organization. The head of the finance department wants only certain authorized users from the department to view the balance sheets of the organization. These documents are stored in the Balance Sheets folder. Which of the following approaches would be the best for assigning permissions to the users from the finance department?
- a. All of the users in the finance department should be assigned permission to the folder.
 - b. The Finance group, containing all users in the finance department, should be assigned permission to the folder.
 - c. Permissions should be assigned individually to each authorized user.
 - d. A group of authorized users should be created. This group should then be assigned appropriate permission to the folder.

D is the correct answer. Because only certain members of the finance department need access to this information, the administrator should create a group that contains only the users that need access, and then grant that group the permissions to the folder.

5. Users in the products department constantly need to refer to product-related information stored in a folder on the server. This folder also contains some applications that the users might need to run. However, users are not allowed to make any modifications to the files in the folder. What permissions should be assigned for this folder?
- a. Read.
 - b. Read & Execute.
 - c. List Folder Contents.
 - d. Read & Write.

B is the correct answer. While all of the answers enable the users to see the information, only B enables the users to open the files and run any applications contained in the folder, but not to make any changes to the files or folder.

6. The network administrator wants you to administer the color printer, which has been set up for the sales department. What printer permission should be assigned to you, so that you can manage the printing of documents as well as share the printer and change its properties?
- a. Print.
 - b. Full Control.
 - c. Manage Documents.
 - d. Manage Printer.

D is the correct answer. The Manage Printer permission enables a user to perform all of the actions necessary. The Print permission enables a user only to print a document. Manage Documents enables a user to affect all of the documents that the printer currently has in its queue. The Full Control permission does not exist for printers.

7. The network administrator of the engineering department needs to limit the use of the printer purchased exclusively for the department. What should be done to ensure that only employees from the Engineering group are able to access the printer?
- a. Add the Print permission to all of the users in the engineering department.
 - b. Add the Print permission to the Engineering group. However, retain the default permission of the Everyone group.
 - c. Remove the default Print permission of the Everyone group and assign permission only to the Engineering group.
 - d. Remove the default Print permission of the Engineering group and assign the Print permission to the Everyone group.

C is the correct answer. The default permissions on a printer give Print permission to the Everyone group. The administrator must first remove this group and then add only the group that needs access to the printer, in this case the Engineering group.

Module 4: Examining the Network

Contents

Overview	1
Scope of Networks	2
Basic Connectivity Components	3
Network Topologies	9
Network Technologies	15
Expanding the Network	21
Lab A: Examining the Network Architecture	34
Review	36



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
120 Minutes

Lab:
30 Minutes

This module provides students with information about the hardware aspects of network communication, such as the requirements for incorporating network components, and explores how the structure of a network can affect communication. The module begins with a description of the scope of a network, comparing a Local Area Network (LAN) to a Wide Area Network (WAN).

The module then examines some of the basic connectivity components of a network. Students will learn about network adapters, the different cable types, and wireless communication devices. The module next focuses on the different topologies that can be used in a network. Students will learn to distinguish the features and roles of the various topologies.

The module continues with an overview of the different network technologies, such as Ethernet, token ring, asynchronous transfer mode (ATM), Fiber Distributed Data Interface (FDDI), and frame relay. The module concludes with a description of the hardware used to expand a network. Students will learn about the features of repeaters and hubs, bridges, routers, and gateways. In addition, remote connectivity types, such as Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), X.25, and asymmetric digital subscriber line (ADSL), will be introduced to the students.

A lab in which students examine the components that make up a network infrastructure follows the last section of the module.

At the end of this module, students will be able to:

- Describe the scope of a network.
- Describe some of the components used in a network.
- Describe the topologies used in a network.
- Describe the technologies used in a network.
- Describe the components used in expanding the network.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2151A_04.ppt
- Module 4, “Examining the Network”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Review the Delivery Tips and Key Points for each section and topic.
- Read the white paper, *Windows 2000-based Virtual Private Networking: Supporting VPN Interopability*, on the Trainer Materials compact disc.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Scope of Networks**
Introduce the scope of networks and distinguish between a LAN and a WAN.
- **Basic Connectivity Components**
Provide an overview of the need for basic connectivity components in a network. Then describe the purpose of the network adapter. Discuss the types of network cables and the characteristics of the wireless communication devices used in a network infrastructure. If time permits, show students samples of different connectivity components.
- **Network Topologies**
Explain the various types of network topologies and discuss the features of bus, star, ring, mesh, and hybrid topologies.
- **Network Technologies**
Introduce the network technologies used to communicate between computers within LANs and WANs. Differentiate the characteristics of Ethernet, token ring, ATM, FDDI, and frame relay technologies with reference to their access methods and transfer speeds.
- **Expanding the Network**
Introduce the tools used to expand a network. Discuss the features of repeaters and hubs, bridges, switches, routers, and gateways. In addition, explain the remote connectivity methods and the features of the physical components of remote access, such as PSTN, ISDN, X.25, and ADSL.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

This module includes only a computer-based interactive lab exercise. As a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about the network infrastructure.

- **Scope of Networks**
- **Basic Connectivity Components**
- **Network Topologies**
- **Network Technologies**
- **Expanding the Network**

*****ILLEGAL FOR NON-TRAINER USE*****

To understand a network running Microsoft® Windows® 2000, you need to know what makes up a network. In examining a network, you must first determine the size of the network. You then need to become familiar with the basic connectivity components, such as the cables and communication tools, which are used to build the network. You must be able to differentiate between the multiple network topologies and then determine the suitability of applying a specific network technology to any given network design. You will need to select specific network components that allow for future expansion of the network.

At the end of this module, you will be able to:

- Describe the scope of a network.
- Describe some of the basic connectivity components used in a network.
- Describe the topologies used in a network.
- Describe the technologies used in a network.
- Describe the components used in expanding the network.

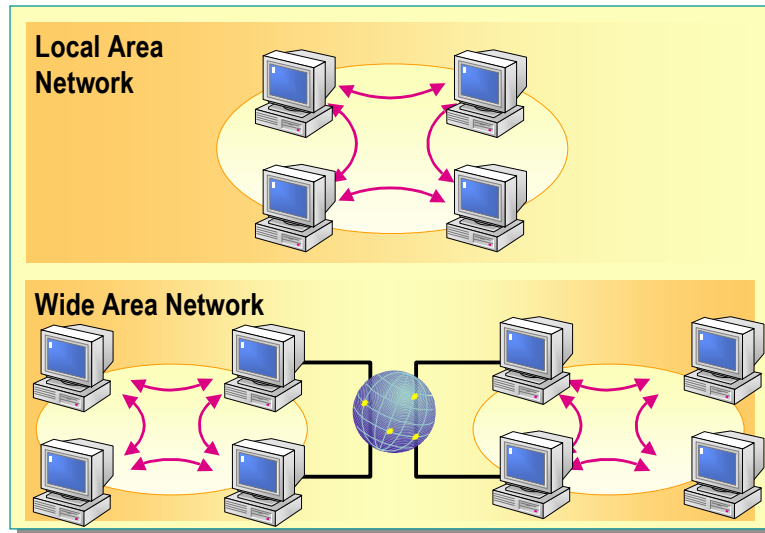
Scope of Networks

Topic Objective

To introduce the scope of networks.

Lead-in

The size of your network is defined by its scope.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

When a WAN has been properly implemented, it appears indistinguishable from a local area network and functions like a LAN.

Delivery Tip

Point out to the students that the scope of a network does not refer merely to the number of computers on the network; it also refers to the distance between computers.

The scope of a network refers to its geographical size. A network can range in size from just a few computers in one office to thousands of computers linked together over great distances.

Network scope is determined by the size of the organization or the distance between users on the network. The scope determines how the network is designed and what physical components are used in its construction.

There are two general types of network scope:

- Local Area Networks
- Wide Area Networks

Local Area Network

A local area network (LAN) connects computers that are located near each other.

For example, two computers connected together in an office or two buildings connected together by a high-speed wire can be considered a LAN. A corporate network that includes several adjacent buildings can also be considered a LAN.

Wide Area Network

A wide area network (WAN) connects a number of computers located at a greater distance from one another.

For example, two or more computers connecting opposite sides of the world is considered a WAN. A WAN can be made up of a number of interconnected LANs. For example, the Internet is really a WAN.

◆ Basic Connectivity Components

Topic Objective

To introduce the basic connectivity components of a network.

Lead-in

The basic connectivity components of a network include the cables, network adapters, and wireless devices that connect the computers to the rest of the network.

- Network Adapters
- Network Cables
- Wireless Communication Devices

*****ILLEGAL FOR NON-TRAINER USE*****

The basic connectivity components of a network include the cables, network adapters, and wireless devices that connect the computers in the network.

These components enable data to be sent to each computer on the network, thereby permitting the computers to communicate with each other.

Common connectivity components of a network are:

- Network adapters.
- Network cables.
- Wireless communication devices.

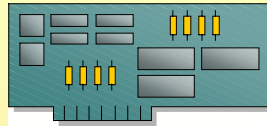
Network Adapters

Topic Objective

To describe the purpose of the network adapter.

Lead-in

Network adapters act as the physical interface, or connection, between the computer and the network cable.



- Receive data and convert it into electrical signals
- Receive electrical signals and convert them into data
- Determine if the data received is for a particular computer
- Control the flow of data through the cable

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Each network adapter has a unique address, called the media access control (MAC), address, that is incorporated into chips on the card.

Network adapters convert data into electrical signals that can be transmitted over a cable.

Network adapters convert electrical signals into data packets that the computer's operating system can understand.

Network adapters constitute the physical interface between the computer and the network cable. Network adapters, also known as network interface cards, are installed into an expansion slot in each computer and server on the network. After the network adapter is installed, the network cable is attached to the adapter's port to physically connect the computer to the network.

As the data passes through the cable to the network adapter, it is formatted into *packets*. A packet is a logical grouping of information that includes a header, which contains location information and user data. The header contains address fields that include information about the data's origin and destination. The network adapter reads the destination address to determine if the packet is to be delivered to this computer. If it is, the network adapter then passes the packet on to the operating system for processing. If not, the network adapter discards the packet.

Each network adapter has a unique address that is incorporated into chips on the card. This address is called the physical, or media access control (MAC), address.

The network adapter performs the following functions:

- Receives data from the computer's operating system and converts it into electrical signals that are transmitted onto the cable
- Receives electrical signals from the cable and translates them into data that the computer's operating system can understand
- Determines whether data received from the cable is intended for the computer
- Controls the flow of data between the computer and the cabling system

To ensure compatibility between the computer and the network, the network adapter must meet the following criteria:

- Fit in the computer's expansion slot
- Use the correct type of cable connector for the cabling
- Be supported by the computer's operating system

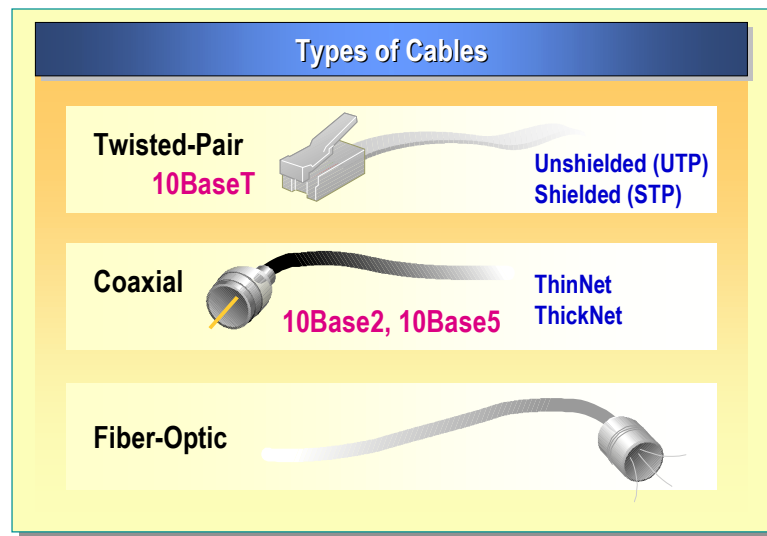
Network Cables

Topic Objective

To describe the network cables that are used in a network infrastructure.

Lead-in

You connect computers to form a network by using cables that act as a network transmission medium to carry signals between computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Twisted-pair cable is the most common type of cable used in networks.

Coaxial cable is used when the data travels long distances.

Fiber-optic cable is used when you have a need for data to travel at the speed of light.

You connect computers together in a network by using cables to carry signals between computers. A cable that connects two computers or network components is called a *segment*. Cables differ in their capabilities and are categorized according to their ability to transmit data at varying speeds, with different error rates. The three major categories of cables that connect most networks are:

- Twisted-pair
- Coaxial
- Fiber-optic

Twisted-Pair Cable

Twisted-pair cable (10baseT) consists of two insulated strands of copper wire twisted around each other. There are two types of twisted-pair cable: unshielded twisted pair (UTP) and shielded twisted pair (STP). These are the most common cables used in networks and can carry signals for 100 meters (about 328 feet).

- UTP cable is the most popular type of twisted-pair cable and is the most popular LAN cable.
- STP cable uses a woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. STP also uses a foil wrap around each of the wire pairs. This gives STP excellent shielding that protects the transmitted data from outside interference, which in turn allows STP to support higher transmission rates over longer distances than UTP.

Twisted-pair cabling uses Registered Jack 45 (RJ-45) connectors to connect to a computer. These are similar to Registered Jack 11 (RJ-11) connectors.

Coaxial Cable

Coaxial cable consists of a copper wire core surrounded by insulation, a braided metal shielding, and an outer cover. The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. There are two types of coaxial cable: ThinNet coaxial cable (10Base2) and ThickNet coaxial cable (10Base5). Coaxial cabling is a good choice when transmitting data over long distances and for reliably supporting higher data rates when using less sophisticated equipment.

Coaxial cable must be terminated at each end.

- ThinNet coaxial cable can carry a signal for approximately 185 meters (about 607 feet).
- ThickNet coaxial cable can carry a signal for 500 meters (about 1,640 feet).

Both ThinNet and ThickNet cable use a connection component, known as a BNC connector, to make the connections between the cable and the computers.

Fiber-Optic Cable

Fiber-optic cable uses optical fibers to carry digital data signals in the form of modulated pulses of light. Because fiber-optic cable carries no electrical impulses, the signal cannot be tapped and its data cannot be stolen. Fiber-optic cable is good for very high-speed, high-capacity data transmission because the signal is transmitted very quickly and with very little interference.

A disadvantage of fiber-optic cable is that it breaks easily if you are not careful during installation. It is more difficult to cut than other cables and requires special equipment to cut it.

Selecting Cables

The following table lists considerations for use of the three categories of network cables.

Cable categories	Use if	Do not use if
Twisted-pair	You want a relatively easy installation in which computer connections are simple.	Your LAN requires a high level of signal shielding to protect it from electromagnetic waves that may interfere with the electrical signal carried in the cable. You must transmit data over long distances at high speeds.
Coaxial	You need to transmit data for greater distances than is possible with less expensive cabling.	You need to change the network cables frequently due to relocations.
Fiber-optic	You need to transmit secure data at very high speeds over long distances.	You have a small budget. You do not have the expertise to properly install it and connect devices to it.

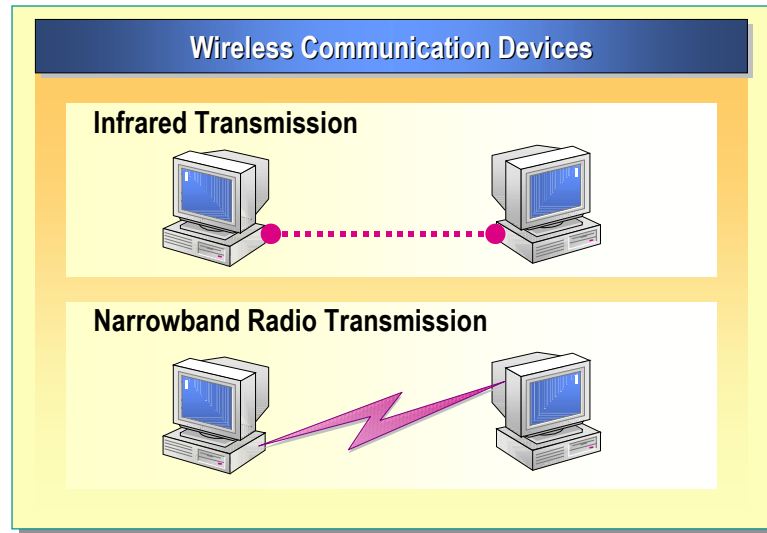
Wireless Communication Devices

Topic Objective

To describe the characteristics of the wireless communication devices used in a network infrastructure.

Lead-in

You use wireless components to connect to networks over distances that make using standard network adapters and cabling options technically or economically unfeasible.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Except for the technology it uses, a typical wireless network operates almost like a cabled network: a wireless network adapter with a transceiver is installed in each computer, and users communicate with the network just as if they were using cabled computers.

You use wireless components to connect networks over distances for which standard network adapters and cable options are not technically or economically feasible. Wireless networks consist of wireless components communicating with LANs.

Except for the fact that a cable does not connect the computers, a typical wireless network operates almost like a cabled network: a wireless network adapter with a *transceiver* (a device that both transmits and receives analog and digital signals) is installed in each computer. Users communicate with the network as if they were using cabled computers.

There are two common techniques for wireless transmission in a LAN: infrared transmission and narrowband radio transmission.

■ Infrared transmission

Operates by using an infrared light beam to carry the data between devices. There must be a clear line of sight between the transmitting and receiving devices; anything that blocks the infrared signal prevents communication. These systems must generate very strong signals because weak transmission signals are susceptible to interference from light sources, such as windows.

■ Narrowband radio transmission

The user tunes both the transmitter and the receiver to a certain frequency. Narrowband radio does not require line-of-sight focusing because it uses radio waves. However, narrowband radio transmission is subject to interference from steel and load-bearing walls. Narrowband radio is a subscription service. Users pay a fee for radio transmission.

◆ Network Topologies

Topic Objective

To introduce the various types of network topologies.

Lead-in

A network topology describes the arrangement of computers, cables, and other components on a network.

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Hybrid Topologies

*****ILLEGAL FOR NON-TRAINER USE*****

A network topology is the arrangement of computers, cables, and other components on a network. It is a map of the physical network. The type of topology you use affects the type and capabilities of the network's hardware, its management, and possibilities for future expansion.

Topology is both physical and logical:

- Physical topology describes how the physical components on a network are connected.
- Logical topology describes the way network data flows through the physical components.

There are five basic topologies:

- *Bus*. Computers are connected to a common, shared cable.
- *Star*. Computers are connected to cable segments that branch out from a central location, or hub.
- *Ring*. Computers are connected to a cable that forms a loop around a central location.
- *Mesh*. Computers on the network are connected to every other computer by cable.
- *Hybrid*. Two or more topologies are used together.

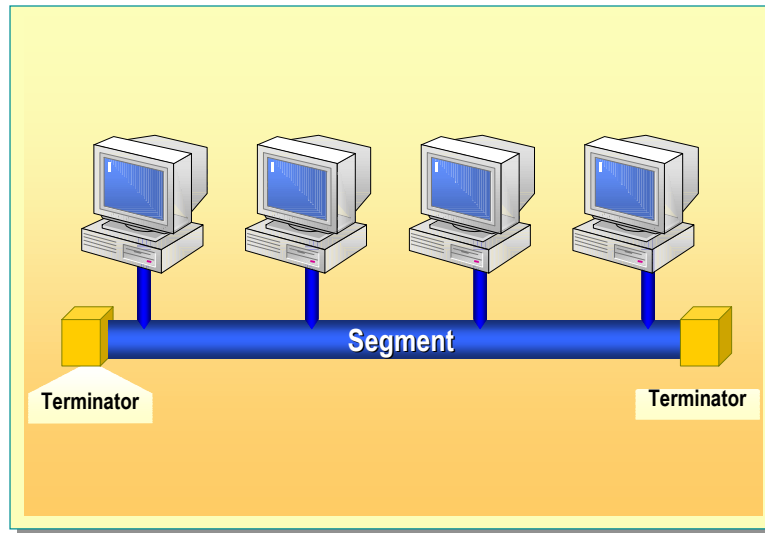
Bus Topology

Topic Objective

To illustrate a bus topology.

Lead-in

In a bus topology, each computer is attached to a continuous cable called a backbone, which is a segment that connects the entire network in a straight line.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Both ends of the cable must be terminated.

All network adapters on the cable receive the data packet.

In a bus topology, all of the computers in a network are attached to a continuous cable, or segment, that connects them in a straight line. In this straight-line topology, a packet is transmitted to all network adapters on that segment.

Because of the way electrical signals are transmitted over this cable, the ends of the cable must be terminated by hardware devices called terminators, which act as the boundaries for the signal and define the segment. If there is a break anywhere in the cable or if an end is not terminated, the signal will travel back and forth across the network and all communication will stop.

The number of computers attached to a bus also affects network performance. The more computers there are on the bus, the greater the backup of computers waiting to put data on the bus, and consequently, the slower the network. In addition, because of the way computers communicate in a bus topology, there may be a lot of *noise*. Noise is the traffic generated on the network when computers attempt to communicate with each other simultaneously. An increase in the number of computers results in an increase in noise and a corresponding decrease in network efficiency.

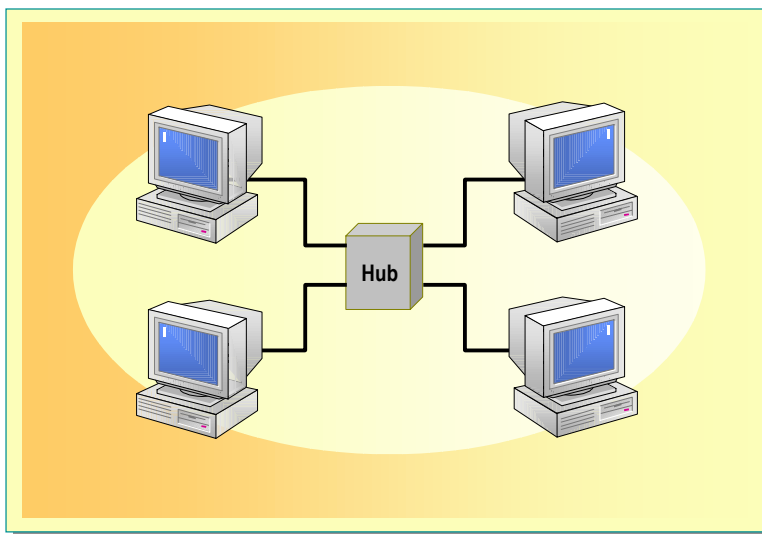
Star Topology

Topic Objective

To illustrate a star topology.

Lead-in

In a star topology, cable segments from each computer on the network are connected to a centralized component.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

In a star topology, if a single computer fails, only the failed computer is unable to send or receive data.

In a star topology, cable segments from each computer on the network are connected to a central component, or *hub*. A hub is a device that connects several computers together. In a star topology, signals are transmitted from the computer, through the hub, to all computers on the network. On a larger scale, multiple LANs can be connected to each other in a star topology.

An advantage of the star topology is that if one computer on the star topology fails, only the failed computer is unable to send or receive data. The remainder of the network functions normally.

The disadvantage of using this topology is that because each computer is connected to a hub, if the hub fails, the entire network fails. In addition, noise is created on the network in a star topology.

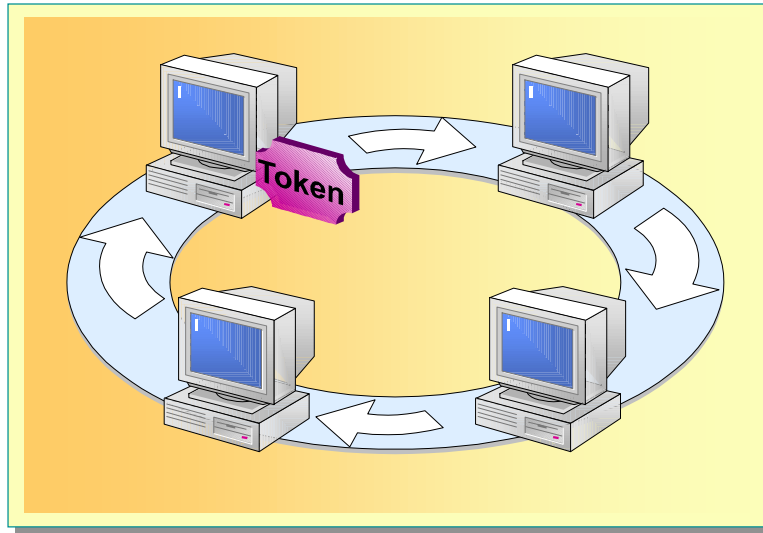
Ring Topology

Topic Objective

To illustrate a ring topology.

Lead-in

In a ring topology, computers are connected on a single circle of cable.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

In a ring topology, each computer acts as a repeater, regenerating the signal and sending it on to the next computer. This preserves signal strength.

In a ring topology, computers are connected on a single circle of cable. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which acts as a repeater to boost the signal and send it to the next computer. On a larger scale, multiple LANs can be connected to each other in a ring topology by using ThickNet coaxial or fiber-optic cable.

The advantage of a ring topology is that each computer acts as a repeater, regenerating the signal and sending it on to the next computer, thereby preserving signal strength.

Token Passing

The method of transmitting data around the ring is called token passing. A *token* is a special series of bits that contains control information. Possession of the token allows a network device to transmit data to the network. Each network has only one token.

The sending computer removes the token from the ring and sends the requested data around the ring. Each computer passes along the data until the packet finds the computer that matches the address on the data. The receiving computer then returns a message to the sending computer indicating that the data has been received. After verification, the sending computer creates a new token and releases it to the network.

The advantage of a ring topology is that it can handle high-traffic environments better than bus networks. In addition, the impact of noise is reduced in the ring topology.

The disadvantage of a ring topology is that only one computer at a time can send data on a single token ring. Also, ring topologies are usually more expensive than bus technologies.

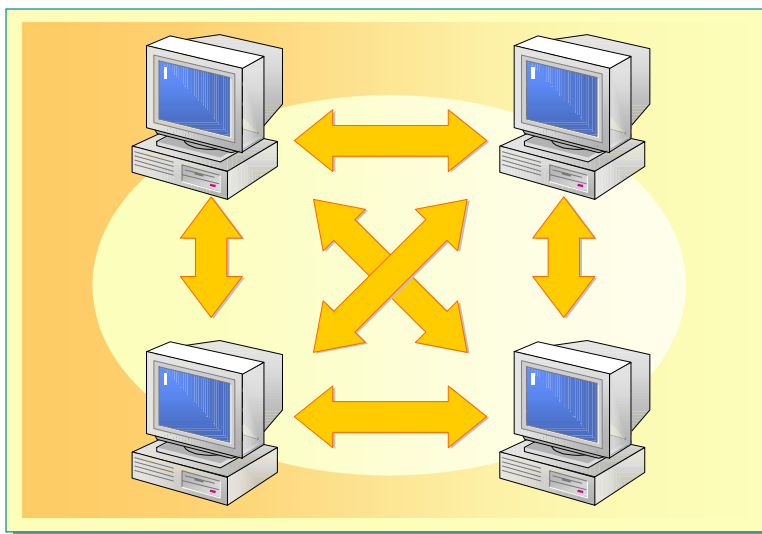
Mesh Topology

Topic Objective

To illustrate a mesh topology.

Lead-in

In a mesh topology, each computer is connected to every other computer by separate cabling.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

A mesh topology provides redundant paths through the network so that if one cable fails, another picks up the traffic and the network continues to function.

In a mesh topology, each computer is connected to every other computer by a separate cable. This configuration provides redundant paths through the network so that if one cable fails, another carries the traffic and the network continues to function. On a larger scale, multiple LANs can be connected to each other in a mesh topology by using leased telephone lines, ThickNet coaxial cable, or fiber-optic cable.

An advantage of a mesh topology is its back-up capabilities by providing multiple paths through the network. Because redundant paths require more cable than is needed in other topologies, a mesh topology can be expensive.

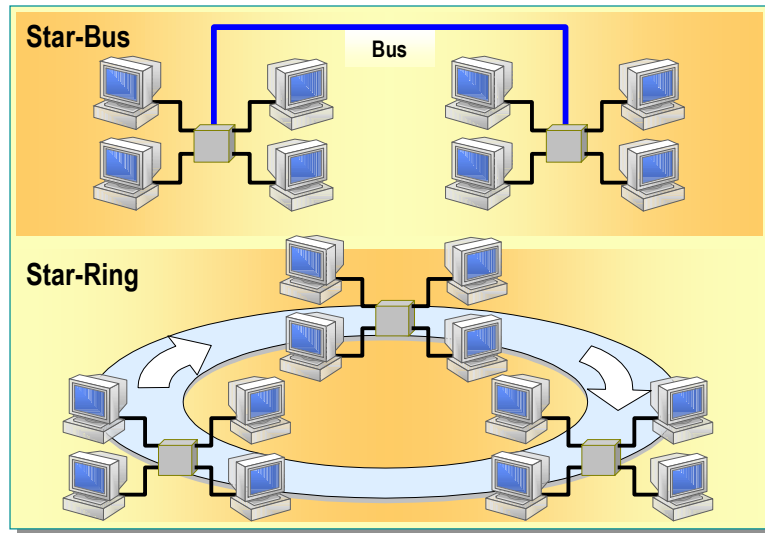
Hybrid Topologies

Topic Objective

To illustrate hybrid topologies.

Lead-in

In a hybrid topology, two or more topologies are combined to form a complete network design.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

In a hybrid topology, if a single computer fails, it does not affect the remainder of the network.

In a hybrid topology, two or more topologies are combined to form a complete network design. Networks are rarely designed using only one type of topology. For example, you may want to combine a star with a bus topology to benefit from the advantages of each.

Two types of hybrid topologies are commonly in use: star-bus topology and star-ring topology.

Star-Bus

In a star-bus topology, several star topology networks are linked to a bus connection. After a star configuration is full, you can add a second star and use a bus connection to connect the two star topologies.

In a star-bus topology, if a single computer fails, it will not affect the rest of the network. However, if the central component, or hub, that attaches all computers in a star fails, all computers attached to that component fail and are unable to communicate.

Star-Ring

In the star-ring topology, the computers are connected to a central component as in a star network. These components, however, are wired to form a ring network.

Like the star-bus topology, if a single computer fails, it will not affect the rest of the network. By using token passing, each computer in a star-ring topology has an equal chance of communicating. This allows for greater network traffic between segments than in a star-bus topology.

◆ Network Technologies

Topic Objective

To introduce the technologies used in a network.

Lead-in

You use different network technologies to communicate between computers within LANs and WANs.

- Ethernet
- Token Ring
- Asynchronous Transfer Mode (ATM)
- Fiber Distributed Data Interface (FDDI)
- Frame Relay

*****ILLEGAL FOR NON-TRAINER USE*****

You use different network technologies to communicate between computers within LANs and WANs. You may use a combination of technologies to get the best cost-benefit and maximum efficiency from your network design.

Many network technologies are available, including:

- Ethernet.
- Token ring.
- Asynchronous transfer mode (ATM).
- Fiber Distributed Data Interface (FDDI).
- Frame relay.

One of the ways in which these technologies differ is the set of rules that each uses to place data onto the network cable and to remove data from the cable. This is called *access method*. When data moves on the network, these various access methods regulate the flow of network traffic.

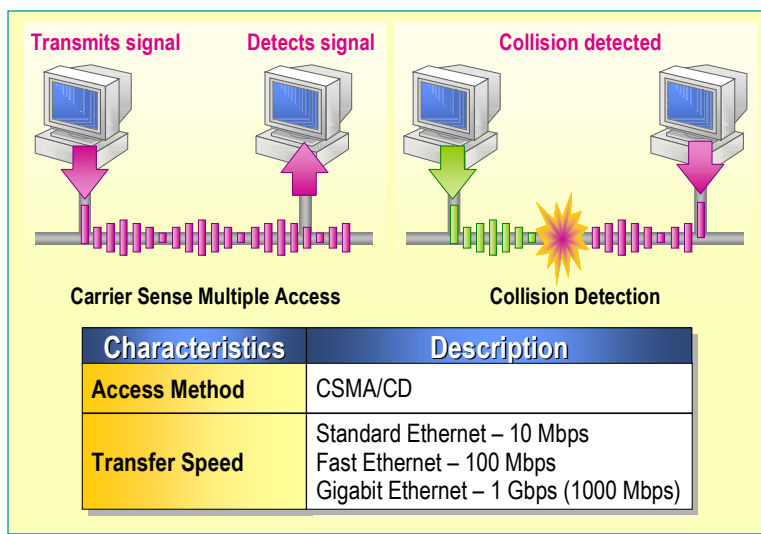
Ethernet

Topic Objective

To describe how Ethernet works.

Lead-in

Ethernet is a popular LAN technology that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) between clients and runs over a variety of cable types by using a bus topology.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe the Ethernet technology. Use the student notes and the slide for supportive details

Define the CSMA/CD data access method and describe how it works in an Ethernet network.

Key Points

Ethernet is passive, which means it requires no power source of its own, and thus does not fail unless the cable is physically cut or improperly terminated.

Ethernet can use multiple communication protocols and can connect mixed computing environments, including Netware, UNIX, Windows, and Macintosh.

Ethernet is a popular LAN technology that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) between clients over a variety of cable types. Ethernet is passive, which means it requires no power source of its own, and thus does not fail unless the cable is physically cut or improperly terminated. Ethernet is connected by using a bus topology in which the cable is terminated at both ends.

Ethernet uses multiple communication protocols and can connect mixed computing environments, including Netware, UNIX, Windows, and Macintosh.

Access Method

The network access method used for Ethernet is Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD is a set of rules that determines how network devices respond when two devices attempt to send data on the network simultaneously. Transmission of data by multiple computers simultaneously over the network causes a collision. Each computer on the network, including clients and servers, checks the cable for network traffic. Only when a computer detects that the cable is free and that there is no traffic on the cable does it send data. After the computer has transmitted data on the cable, no other computer can transmit data until the original data has reached its destination and the cable is again free.

After detecting a collision, a device waits a random delay time and then attempts to retransmit the message. If the device detects a collision again, it waits twice as long before trying to retransmit the message.

Transfer Speed

Standard Ethernet, called 10BaseT, supports data transfer rates of 10 Mbps over a wide range of cabling. Faster versions of Ethernet are also available. Fast Ethernet (100BaseT) supports data transfer rates of 100 Mbps, and Gigabit Ethernet supports data rates of 1 Gbps (gigabits per second) or 1,000 Mbps.

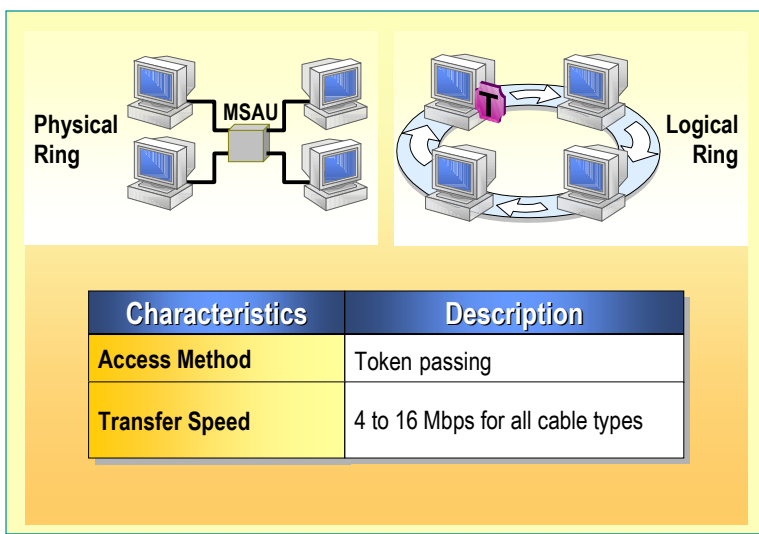
Token Ring

Topic Objective

To describe how a token ring network functions.

Lead-in

Token ring networks are implemented in a star-wired ring; computers on the network are connected to a central component.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe the token ring technology. Use the student notes and slide for supportive details.

Explain the token passing access method and how it works in a token ring network.

Key Points

The logical ring represents the token's path between computers. The physical ring is wired through a central component called a multistation access unit (MSAU).

Token ring networks are implemented in a ring topology. The physical topology of a token ring network is the star topology, in which all computers on the network are physically connected to a hub. The physical ring is wired through a hub called a multistation access unit (MSAU). The logical topology represents the token's path between computers, which is similar to a ring.

Access Method

The access method used in a token ring network is token passing. A token is a special series of bits that travels around a token ring network. A computer cannot transmit unless it has possession of the token; while the token is in use by a computer, no other computer can transmit data.

When the first computer on the token ring comes online, the network generates a token. The token travels around the ring to each computer until one of the computers takes control of the token.

When a computer takes control of the token, it sends a data frame out on the network. The frame proceeds around the ring until it reaches the computer with the address that matches the destination address in the frame. The destination computer copies the frame into its memory and marks the frame in the frame status field to indicate that the information was received.

The frame continues around the ring until it arrives at the sending computer, where the transmission is acknowledged as successful. The sending computer then removes the frame from the ring and transmits a new token back on the ring.

Transfer Speed

The transfer speed in a token ring network is between 4 and 16 Mbps.

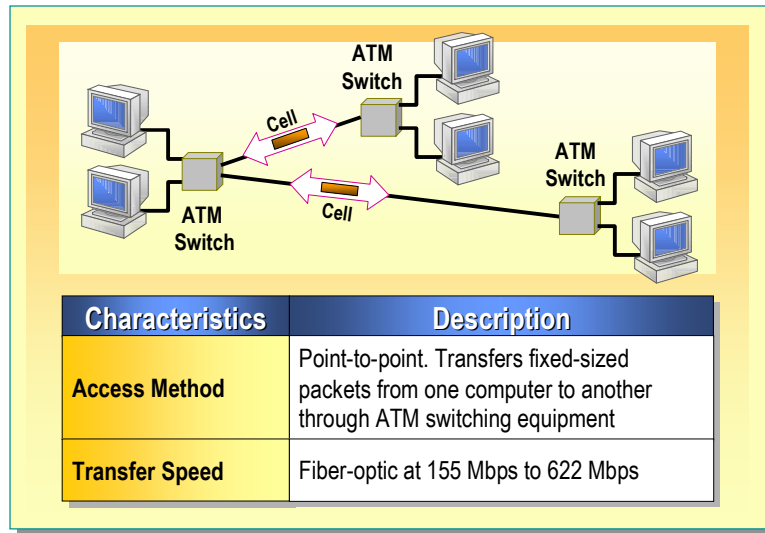
Asynchronous Transfer Mode

Topic Objective

To describe how asynchronous transfer mode works.

Lead-in

Asynchronous transfer mode is an advanced implementation of packet switching that sends fixed-size packets over LANs or WANs.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe the asynchronous transfer mode technology. Use the student notes and slide for supportive details.

Describe the cell relay access method and how it is applied in ATM.

Key Points

ATM's transmission speed enables it to transmit voice, real-time video, CD-quality audio, imaging, and megabit data transmission.

Asynchronous transfer mode (ATM) is a packet-switching network that sends *fixed-length packets* over LANs or WANs, instead of the variable-length packets used in other technologies. Fixed-length packets, or cells, are data packets that contain only basic path information, allowing switching devices to route the packet quickly. Communication occurs over a point-to-point system that provides a permanent and virtual data path between each station.

Using ATM, you can send data from a main office to a remote location. The data travels from a LAN over a digital leased line to an ATM switch and into the ATM network. It passes through the ATM network and arrives at another ATM switch in the destination LAN.

Because of its expanded bandwidth, ATM can accommodate:

- Voice.
- Real-time video.
- CD-quality audio.
- Imaging data, such as real-time radiology.
- Megabit data transmission.

Access Method

An ATM network uses the point-to-point access method. This access method transfers fixed-length packets from one computer to another through ATM switching equipment. The result is a technology that transmits a small, compact data packet at a high speed.

Transfer Speed

The transfer speed in an ATM network is between 155 and 622 Mbps.

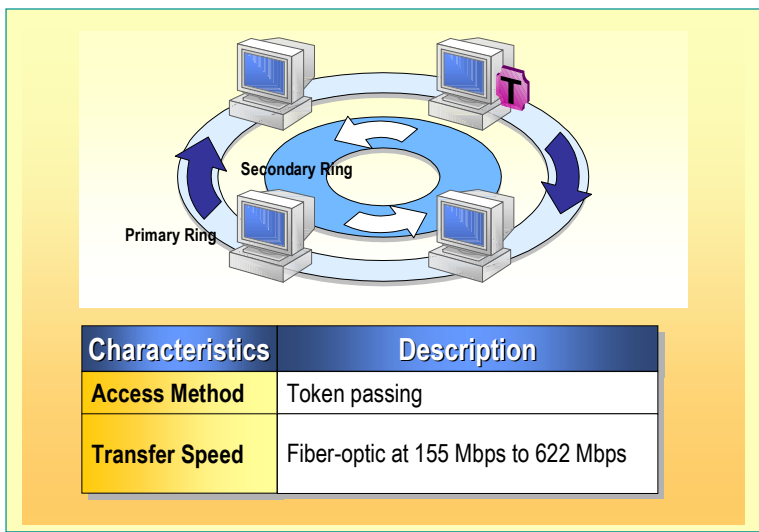
Fiber Distributed Data Interface

Topic Objective

To describe how Fiber Distributed Data Interface works.

Lead-in

A Fiber Distributed Data Interface network is used to provide high-speed connections for various types of networks.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe the Fiber Distributed Data Interface technology. Use the student notes and the slide for supportive details.

Describe the token passing access method and how it is used in FDDI.

Key Points

FDDI provides a fast backbone to an existing LAN or WAN.

A Fiber Distributed Data Interface (FDDI) network provides high-speed connections for various types of networks. FDDI was designed for use with computers that required speeds greater than the 10 Mbps available from Ethernet or the 4 Mbps available from existing token ring architectures. An FDDI network can support several low-capacity LANs that require a high-speed backbone.

An FDDI network consists of two similar streams of data flowing in opposite directions around two rings. One ring is called the primary ring and the other is called the secondary ring. If there is a problem with the primary ring, such as a ring failure or a cable break, the ring reconfigures itself by transferring data to the secondary ring, which continues transmitting.

Access Method

The access method used in an FDDI network is token passing. A computer on an FDDI network can transmit as many packets as it can produce within a predetermined time before releasing the token. As soon as a computer has finished transmitting or after a predetermined transmittal time is up, the computer releases the token.

Because a computer releases the token when it finishes transmitting, several packets can circulate on the ring at the same time. This method of token passing is more efficient than that on a standard token ring network, which allows only one frame at a time to circulate. This method of token passing also provides greater data throughput at the same transmission rate.

Transfer Speed

The transfer speed in an FDDI network is between 155 and 622 Mbps.

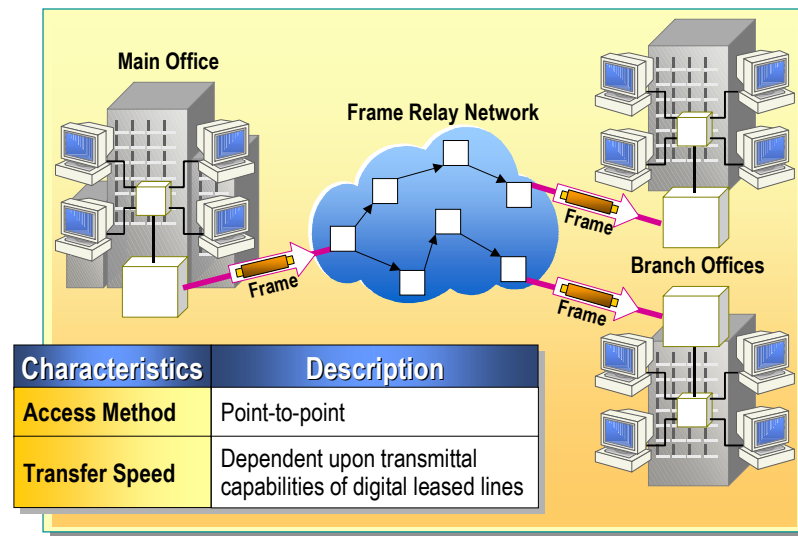
Frame Relay

Topic Objective

To describe how frame relay works.

Lead-in

Frame relay is a packet-switching network that sends variable-length data packets over LANs or WANs.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe the frame relay technology. Use the student notes and slide for supportive details.

Define the point-to-point access method and how it works in a frame relay network.

Key Points

This type of network gives you quick access to data transfer that you pay for only as you need it.

Frame relay is a packet-switching network that sends *variable-length packets* over LANs or WANs. Variable length packets, or frames, are data packets that contain additional addressing and error handling information necessary for delivery.

Communication occurs over a network that provides a permanent and virtual data path between each station. This type of network uses wide area digital or fiber-optic links and gives you quick access to data transfer that you pay for only as you need it.

Packet switching is a method used to send data over a WAN by dividing a large package of data into smaller pieces (packets). These pieces are sent through a packet switch, which sends the individual packets across the WAN using the best route currently available. Although these packets may travel along different paths, the receiving computer can reassemble the pieces into the original data frame.

However, you could have a permanent virtual circuit (PVC) established, which would use the same path for all of the packets. This allows for a faster transmission than by normal frame relay networks and eliminates the need for packet disassembly and reassembly.

Access Method

Frame relay uses the point-to-point access method. This access method transfers variable-sized packets from one computer directly to another, instead of between several computers and peripherals.

Transfer Speed

Frame relay allows for data transfer that is as fast as the provider can supply over digital leased lines.

◆ Expanding the Network

Topic Objective

To introduce the tools you use to expand the network.

Lead-in

There are several tools that you can use to expand an existing network.

- Repeater and Hubs
- Bridges
- Switches
- Routers
- Gateways
- Remote Access Connectivity Types
- Public Switched Telephone Network (PSTN)
- Integrated Services Digital Network (ISDN)
- X.25
- Asymmetric Digital Subscriber Line (ADSL)

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This is only an introduction to the topics that follow. Do not spend too much time on this page.

To cater to the growing networking needs of an organization, you need to expand the size or improve the performance of a network. You cannot make networks larger just by adding new computers and more cable. Each network topology or architecture has limits. You can, however, install components to increase the size of the network within its existing environment.

Components that enable you to expand the network include:

- Repeater and Hubs
Repeaters and hubs retransmit an electrical signal received on one connection point (port) to all ports in order to maintain the integrity of the signal.
- Bridges
Bridges enable data to be passed between LANs.
- Switches
Switches enable high-speed passing of data to LANs.
- Routers
Routers enable passing of data through LANs or WANs, depending on the destination network of the data.
- Gateways
Gateways enable passing of data through LANs or WANs and function so that computers using different protocols can communicate with each other.

You can also expand a network by allowing users to connect to the network from a remote location. To establish a remote connection, the three components required are a remote access client, a remote access server, and physical connectivity. Microsoft Windows 2000 enables remote client computers to connect to remote access servers by using:

- Public Switched Telephone Network (PSTN).
- Integrated Services Digital Network (ISDN).
- X.25.
- Asymmetric Digital Subscriber Line (ADSL).

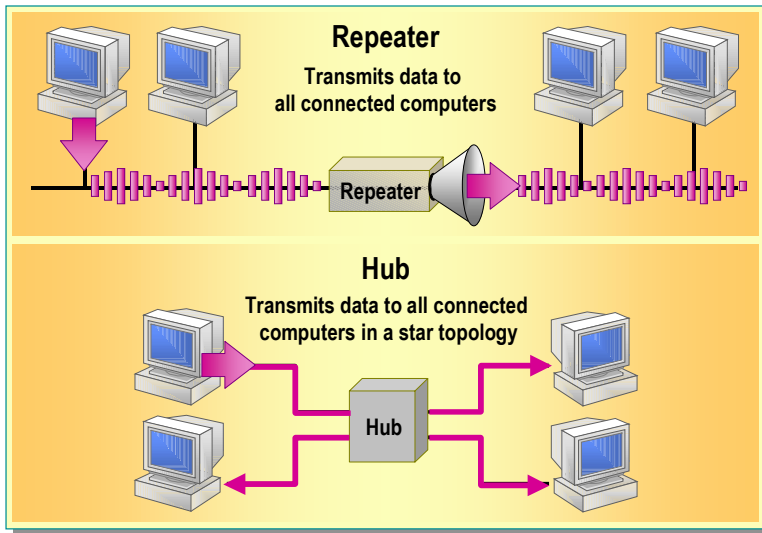
Repeaters and Hubs

Topic Objective

To illustrate how repeaters and hubs work.

Lead-in

Repeaters and hubs are used to expand a network by adding two or more segments of cabling.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe how to use repeaters and hubs to expand a network.

Use the student notes and the animated slides for supportive details.

Key Points

Repeaters are inexpensive ways to expand cable length without sacrificing data loss.

Hubs enable you to connect several computers to a central point without data loss.

A hub broadcasts the data packet to all of the computers and segments that are attached to it.

You can use repeaters and hubs to expand a network by adding two or more segments of cabling. These commonly used devices are inexpensive and easy to set up.

Repeaters

Repeaters receive signals and retransmit them at their original strength and definition. This increases the practical length of a cable. (If a cable is very long, the signal weakens and becomes unrecognizable.) Installing a repeater between cable segments enables signals to travel farther.

Repeaters do not translate or filter signals. For a repeater to work, both segments connected to the repeater must use the same access method. For example, a repeater cannot translate an Ethernet packet into a token ring packet.

Repeaters do not act as filters to restrict the flow of problem traffic. Repeaters send every bit of data from one cable segment to another, even if the data consists of malformed packets or packets not destined for a computer on another segment.

Use a repeater to:

- Connect two segments of similar or dissimilar cabling.
- Regenerate the signal to increase the distance transmitted.
- Transmit all traffic in both directions.
- Connect two segments in the most cost-effective manner.

Hubs

Hubs are connectivity devices that connect computers in a star topology. Hubs contain multiple ports for connecting to network components. If you use a hub, a break in the network does not affect the entire network; only the segment and the computer attached to that segment fail. A single data packet sent through a hub goes to all connected computers.

There are two types of hubs:

- *Passive Hubs*. Send the incoming signal directly through their ports without any signal processing. These hubs are usually wiring panels.
- *Active Hubs*. Sometimes called *multiport repeaters*, receive incoming signals, process the signals, and retransmit them at their original strengths and definitions to the connected computers or components.

Use a hub to:

- Easily change and expand wiring systems.
- Use different ports to accommodate a variety of cable types.
- Enable central monitoring of network activity and traffic.

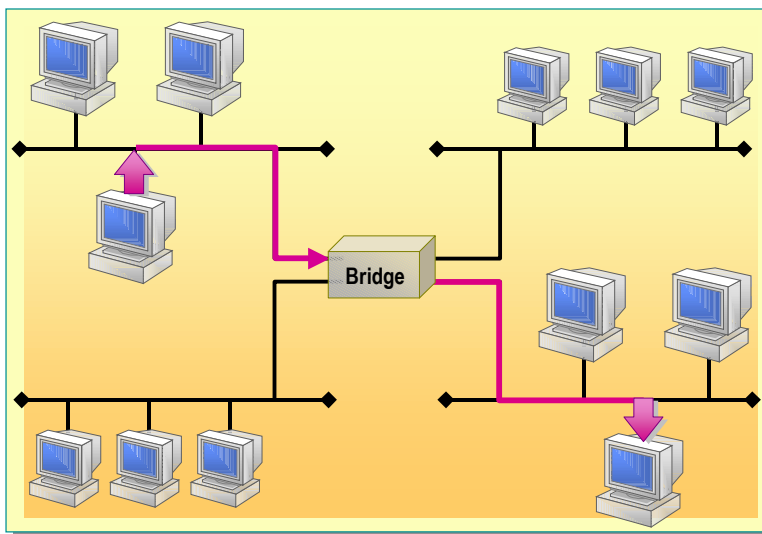
Bridges

Topic Objective

To illustrate how bridges work.

Lead-in

A bridge is a device that passes data packets between multiple network segments that use the same communications protocol.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe how a bridge is used to expand a network. Use the student notes and animated slide for supportive details.

Key Points

A bridge broadcasts packets to a computer if it recognizes the location of the destination address. If it does not recognize the destination address, it forwards the packets to all segments attached to the bridge.

A bridge is a device that passes data packets between multiple network segments that use the same communications protocol. A bridge passes one signal at a time. If a packet is destined for a computer within the sender's own network segment, the bridge retains the packet within that segment. If the packet is destined for another segment, it passes the packet to that segment.

MAC Addresses

As traffic passes through the bridge, information about the sending computers' MAC addresses is stored in the bridge's memory. The bridge uses this information to build a table based on these addresses. As more data is sent, the bridge develops a bridging table that identifies each computer and its location on network segments. When the bridge receives a packet, the source address is compared to the source address listed in the table. If the source address is not present in the table, it is added to the table. The bridge then compares the destination address with the destination address listed in the table. If a bridge recognizes the location of the destination address, it forwards the packet to this address. If it does not recognize the destination address, it forwards the packet to all segments.

Use a bridge to:

- Expand the length of a segment.
- Provide for an increased number of computers on the network.
- Reduce traffic bottlenecks resulting from an excessive number of attached computers.
- Split an overloaded network into two separate networks, thereby reducing the amount of traffic on each segment and making each network more efficient.
- Link dissimilar physical cables, such as twisted-pair and coaxial Ethernet cables.

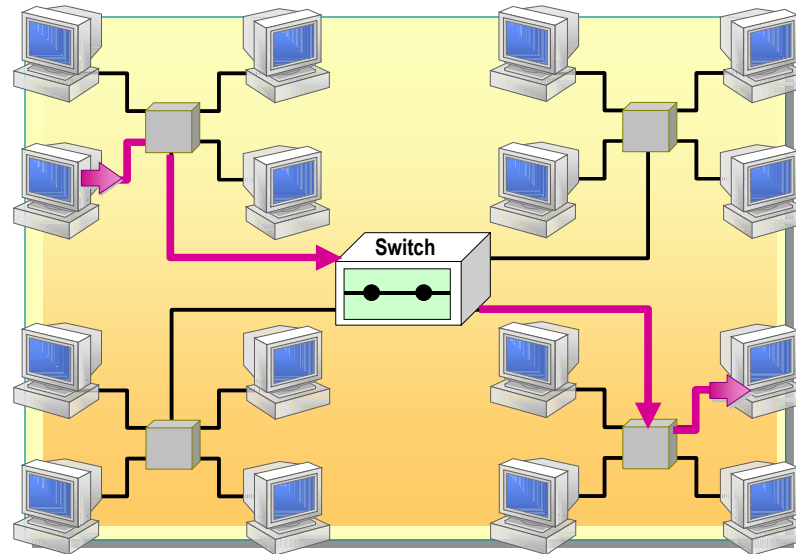
Switches

Topic Objective

To illustrate how switches function.

Lead-in

Switches are similar to bridges but offer a more direct network connection between the source and destination computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe how switches are used to expand a network. Use the student notes and the animated slide for supportive details.

Key Points

When a switch receives a data packet, it forwards the data packet to the destination computer only.

Switches are similar to bridges but offer a more direct network connection between the source and destination computers. When a switch receives a data packet, it creates a separate internal connection, or segment, between any two of its ports and forwards the data packet to the appropriate port of the destination computer only, based on information in each packet's header. This insulates the connection from the other ports and gives the source and destination computers access to the full bandwidth of a network.

Unlike a hub, switches are comparable to a telephone system with private lines. In such a system, if one person calls someone, the operator or telephone switch connects them on a dedicated line. This allows more conversations to take place at any one time.

Use a switch to:

- Send a packet directly from the source computer to the destination computer.
- Provide for a greater rate of data transmission.

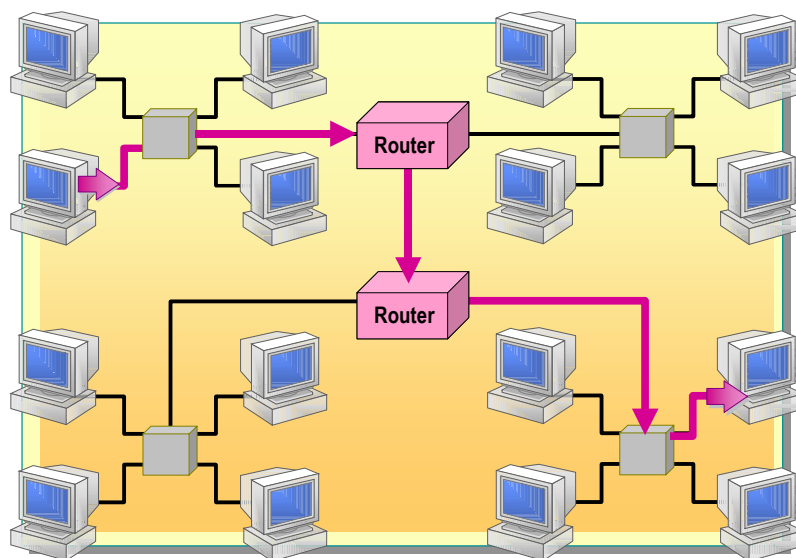
Routers

Topic Objective

To illustrate how routers function.

Lead-in

A router is a device that acts like a bridge or switch but provides increased functionality.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Describe how a router is used to expand a network. Use the student notes and the animated slide for supportive details.

Key Points

Using the network addresses of computers and sophisticated routing information, a router can send data over the most direct path between the source and destination computers.

A router is a device that acts like a bridge or switch but provides more functionality. In moving data between different network segments, routers examine a packet header to determine the best path for the packet to travel. A router knows the path to all of the segments on the network by accessing information stored in the routing table. Routers enable all users in a network to share a single connection to the Internet or a WAN.

Use a router to:

- Send packets directly to a destination computer on another network or segment.

Routers use a more complete packet address than do bridges, for example, to determine which router or client should next receive each packet. Routers ensure that packets travel the most efficient paths to their destinations. If a link between two routers fails, the sending router can determine an alternate route to keep traffic moving.

- Reduce stress on the network.

Routers read addressed network packets only and pass information only if the network address is known. Therefore, they do not pass corrupted data. This ability to control the data passing through the router reduces the amount of traffic between networks and enables routers to use these links more efficiently than bridges can.

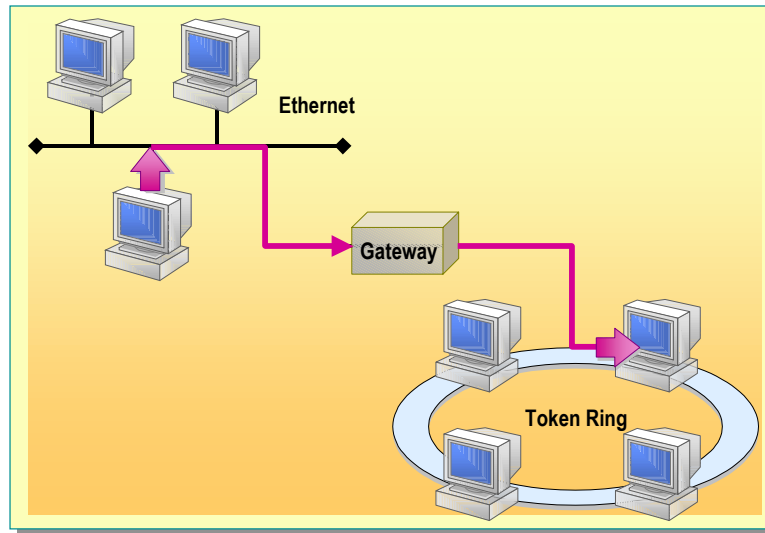
Gateways

Topic Objective

To illustrate how a gateway functions.

Lead-in

Gateways enable communication between different architectures and environments.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Use a gateway to communicate between two networks that have different communication protocols, data-formatting structures, languages, and architecture.

Gateways enable communication between different network architectures. A gateway takes the data from one network and repackages it, so that each network can understand the other network's data.

A gateway is like an interpreter. For example, if two groups of people can physically talk to each other but speak different languages, they need an interpreter to communicate. Similarly, two networks can have a physical connection but need a gateway to translate network communication.

Use a gateway to link two systems that do not use the same:

- Architecture.
- Set of communication rules and regulations.
- Data-formatting structures.

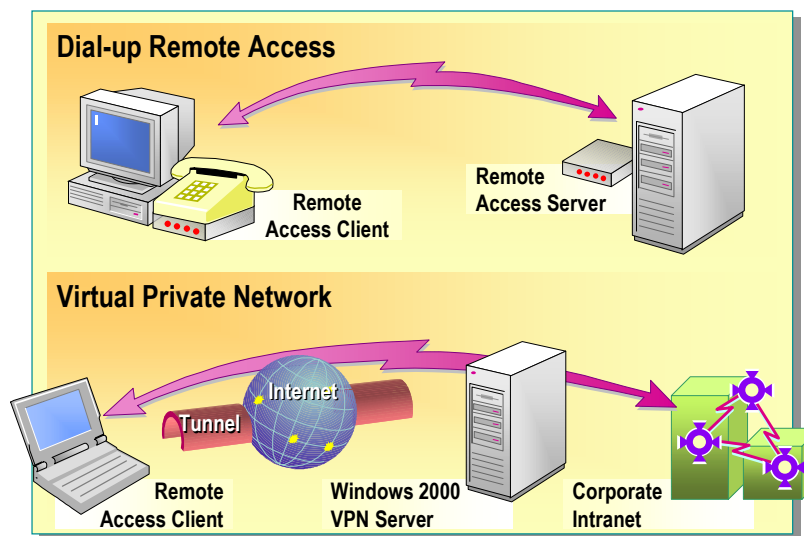
Remote Access Connectivity Types

Topic Objective

To illustrate the different types of remote access connectivity.

Lead-in

When connecting to a network from a remote location, you can either connect using a dial-up connection that requires telephone lines or create a virtual private line that uses the existing connections.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Dial-up remote access enables a client to use the telecommunications infrastructure to connect to a remote access server.

A virtual private network (VPN) connects the components and resources of one network to another network by allowing the user to tunnel through the Internet or another public network without any additional hardware.

Windows 2000 enables users to connect to a network from a remote location through a variety of hardware, such as modems. A modem enables a computer to communicate over telephone lines. The remote access client connects to the remote access server, which acts as a router, or a gateway, for the client to the remote network. A telephone line commonly provides the physical connectivity between the client and server. The remote access server runs the Routing and Remote Access feature in Windows 2000 to support remote connections and to provide interoperability with other remote access solutions.

The two types of remote access connectivity provided in Windows 2000 are dial-up remote access and virtual private network (VPN).

Dial-up Remote Access

Windows 2000 Server provides dial-up remote access to users who dial corporate intranets. Dial-up equipment installed on a remote access server running Windows 2000 answers incoming connection requests from dial-up networking clients. The dial-up equipment answers the call, verifies the caller's identity, and transfers data between the dial-up networking client and the corporate intranet.

Virtual Private Network

A virtual private network (VPN) uses encryption technology to provide security and other features formerly available only in private networks. VPNs provide this security through a process called *tunneling*. Tunneling is a method of using an internetwork infrastructure to securely transfer data from one network to another network. A VPN enables telecommuters and employees at remote locations to establish a secure connection to a corporate server that is connected to both the corporate LAN and a public internetwork, such as the Internet. From the user's perspective, the VPN provides a point-to-point connection between the user's computer and a corporate server. The intermediate internetwork is transparent to the user because it appears as if the remote access client is connected directly to the corporate LAN/remote access server.

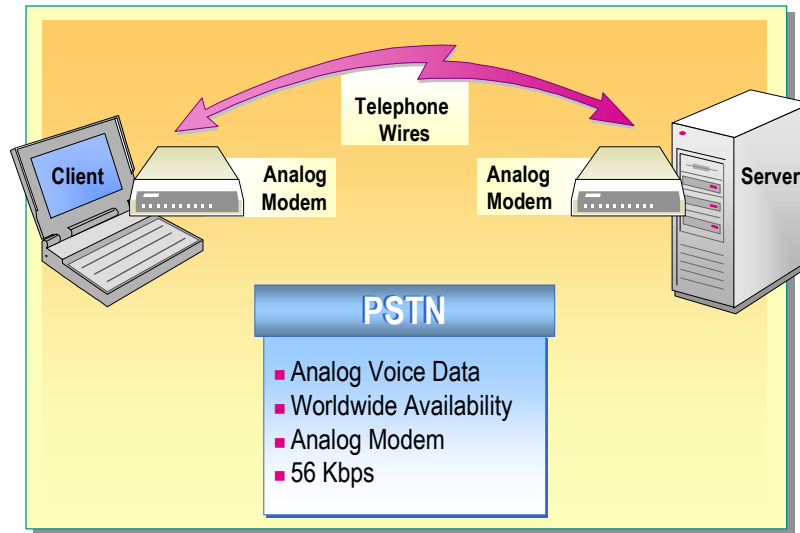
Public Switched Telephone Network (PSTN)

Topic Objective

To illustrate how a PSTN connection functions in remote access.

Lead-in

PSTN is the most common communication method because it uses inexpensive modems. It supports analog communication at speeds of up to 56 Kbps.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

PSTN is universally available and inexpensive.

Public Switched Telephone Network (PSTN) refers to the international telephone standard based on using copper wires for transmitting analog voice data. This standard was designed to carry only the minimal frequencies necessary to distinguish human voices. Because PSTN was not designed for data transmissions, there are limits to the maximum data transmission rate of a PSTN connection. In addition, analog communication is susceptible to line noise that causes a reduction in the data transmission rate.

A key advantage of PSTN is its worldwide availability and low-cost hardware due to mass-production.

Analog Modem

Dial-up remote access equipment consists of an analog modem for the remote access client and another for the remote access server. An analog modem is a device that enables a computer to transmit information over a standard telephone line. Because a computer is digital and a telephone line is analog, analog modems are needed to convert digital to analog and vice versa. For large organizations, the remote access server is attached to a modem bank containing hundreds of modems. With analog modems at both the remote access server and the remote access client, the maximum bit rate supported by PSTN connections is 56,000 bits per second, or 56 kilobits per second.

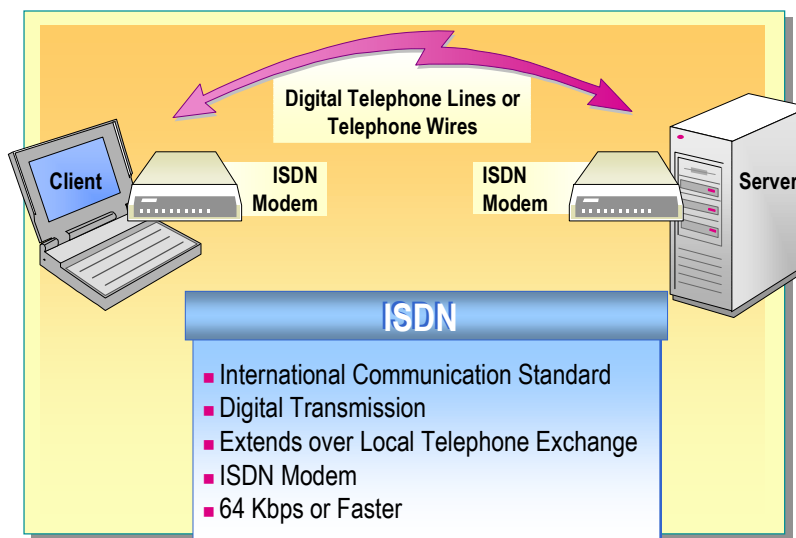
Integrated Services Digital Network (ISDN)

Topic Objective

To illustrate how the ISDN connection is used in remote access.

Lead-in

ISDN communication is much faster than PSTN. ISDN supports communication speeds of up to 128 Kbps by using two B channels.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

ISDN is faster than most PSTN connections and is widely available in urban areas.

Integrated Services Digital Network (ISDN) is an international communications standard for sending voice, video, and data over digital telephone lines and standard telephone wires. ISDN has the ability to simultaneously deliver two connections over a single pair of telephone lines. The two connections may be in any combination of data, voice, video, or fax. The single line uses an ISDN subscriber service, which is called Basic Rate Interface (BRI). BRI has two channels, called B channels, at 64 Kbps each, which carry the data, and one data channel at 16 Kbps for control information. The two B channels can be combined to form a single 128 Kbps connection.

The other ISDN transmission rate service, Primary Rate Interface (PRI), has 23 B channels and one 64 Kbps D channel and uses more wire pairs. PRI is much more expensive to run than BRI and is not commonly selected by individual remote access users. In most cases, BRI is preferred when using ISDN for remote access.

Digital Transmission

ISDN is a digital transmission, as opposed to the analog transmission of PSTN. ISDN lines must be used at both the server and remote site. In addition, you must install an ISDN modem in both the server and the remote client.

Extends over Local Telephone Exchange

ISDN is not simply a point-to-point connection as a leased line. ISDN networks extend from the local telephone exchange to the remote user and include all of the telecommunications and switching equipment lying between them.

ISDN Modem

Dial-up remote access equipment consists of an ISDN modem each for the remote access client and the remote access server. ISDN offers much faster communication than PSTN, communicating at speeds of 64 Kbps or faster.

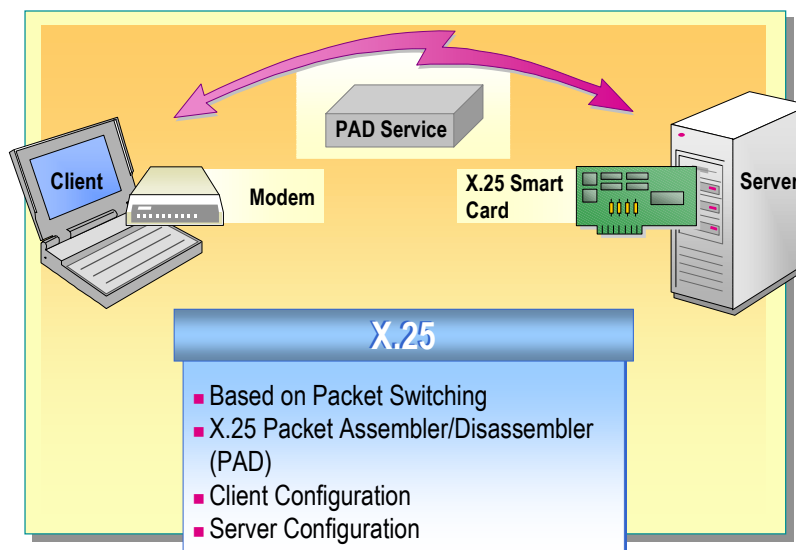
X.25

Topic Objective

To illustrate the X.25 connection that is used in remote access.

Lead-in

X.25 provides a secure and dedicated network service that allows client and server to communicate at different speeds.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

X.25 is a secure and dedicated network.

In an X.25 network, data is transmitted using packet switching. X.25 utilizes data communications equipment to create an elaborate, worldwide network of packet-forwarding nodes that deliver an X.25 packet to its designated address.

X.25 Packet Assembler/Disassembler (PAD)

Dial-up remote access clients can directly access an X.25 network by using an X.25 packet assembler/disassembler (PAD). A PAD allows the use of terminals and modem connections without necessitating expensive client hardware and connectivity to talk directly to X.25. Dial-up PADs are a practical choice for remote access clients because they do not require that you plug an X.25 line into the back of the computer. The only requirement for a dial-up PAD is the telephone number of the PAD service for the carrier.

In Windows 2000, Routing and Remote Access provides access to the X.25 network in one of two configurations shown in the following table.

Dial-up configuration

You can make a dial-up connection to the X.25 network by using asynchronous PADs. The PAD converts serially transmitted data into X.25 packets. When the PAD receives a packet from an X.25 network, it puts the packet out on a serial line, making communication possible between the client and the X.25 network.

Direct configuration

You can make a direct connection to the X.25 network through an X.25 smart card. An X.25 smart card is a hardware card with a PAD embedded in it. The smart card acts like a modem. To the personal computer, a smart card looks like several communication ports attached to PADs.

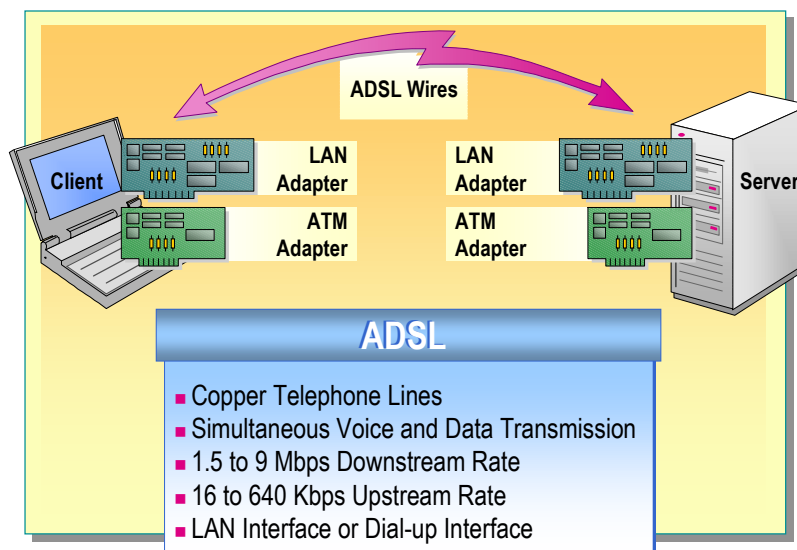
Asymmetric Digital Subscriber Line (ADSL)

Topic Objective

To illustrate the ADSL connection that is used in remote access.

Lead-in

ADSL is a new, high-speed technology that usually has a much higher rate of data transmission downstream than upstream.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Asymmetric digital subscriber line (ADSL) is a technology that allows more data to be sent over existing copper telephone lines.

When receiving data, ADSL supports data rates from 1.5 to 9 Mbps. When sending data, ADSL supports data rates from 16 to 640 Kbps.

When an ADSL adapter appears as a LAN interface, the ADSL connection operates in the same way as a LAN connection to the Internet.

Asymmetric digital subscriber line (ADSL) is a technology that allows more data to be sent over existing copper telephone lines. ADSL accomplishes this by using the portion of a telephone line's bandwidth not utilized by voice, thereby allowing for simultaneous voice and data transmission.

Typical remote access users receive much more information than they send. The asymmetric nature of the ADSL connection fits well with most Internet and remote business use. When receiving data, ADSL supports data rates from 1.5 to 9 Mbps. When sending data, ADSL supports data rates from 16 to 640 Kbps. Although ADSL provides higher data transmission rates than do PSTN and ISDN connections, the client computer can receive data at a faster rate than it can send data.

LAN Interface or Dial-up Interface

ADSL equipment can appear to Windows 2000 as either a LAN interface or a dial-up interface. When an ADSL adapter appears as a LAN interface, the ADSL connection operates in the same way as a LAN connection to the Internet. When an ADSL adapter appears as dial-up interface, ADSL provides a physical connection and the individual packets are sent using asynchronous transfer mode (ATM). An ATM adapter with an ADSL port is installed in both the remote access client and remote access server.

Lab A: Examining the Network Architecture

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will examine the components that make up a network infrastructure.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Describe the principles and components of network architecture.
- Describe the scope of Local Area Networks (LANs) and Wide Area Network (WANs).
- Describe the basic connectivity components, such as the different types of cabling and the network adapters.
- Describe network topologies: bus, star, ring, mesh, and hybrid (a combination of two or more topologies in a single network design).
- Describe the different network technologies: Ethernet, token ring, FDDI, ATM, and frame relay.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors. (16-bit recommended)
- Microsoft Internet Explorer 5 or later.

► **To start the lab**

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Examining the Network Architecture**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 30 minutes

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Scope of Networks**
- **Basic Connectivity Components**
- **Network Topologies**
- **Network Technologies**
- **Expanding the Network**

*****ILLEGAL FOR NON-TRAINER USE*****

1. The organization you work for has just merged with another company, which has offices in five countries in Europe and Asia. Your job is to expand the network so that all offices of the newly merged organization are connected. What will the resulting network be called, and which network components could you use to connect the offices?

Wide Area Network (WAN). You can use packet-switching networks, ISDN, microwave transmitters or satellite links to connect the remote offices.

2. You are sending a file from your computer to another computer on your network. Which functions does the network adapter perform to send this file across the network?

The network adapter receives the data from the operating system, converts the data into electrical signals, and transmits it onto the network.

3. You are troubleshooting a network that is experiencing intermittent connectivity problems. You trace the cables back to a location in the center of your office, where all of the cables are connected to a central wiring closet. What is the term used to describe the physical topology of this network?

Star topology.

4. Your organization uses an Ethernet network at its headquarters. What happens to this network as more and more computers are added to it if bridges, switches, or routers are not added as well?

As more computers are added, more collisions occur, and less data can be transmitted on the network.

5. Your network has expanded from several computers to several hundred computers, and users are now complaining that the network is slow. You do not have the budget to upgrade the cabling or to change the type of network, so you choose to divide the network into segments to increase the data throughput on each segment. You want to do this without making any changes to the computers on the network. Which network component(s) can you use?

A bridge or a switch. A router could be used, but it would require that you change the network configuration of the computers on your network.

6. Your users need access to the company's intranet from their homes. Which methods are available to provide this access?

Dial-up remote access.

Virtual private network.

7. You want to provide fast Internet access to the users in your intranet so that the rate of receiving data is much higher than the rate of sending data. Which method will enable you to provide this access?

ADSL.

Module 5: Examining Network Protocols

Contents

Overview	1
Introduction to Protocols	2
Protocols and Data Transmissions	6
Common Protocols	10
Other Communication Protocols	15
Remote Access Protocols	18
Lab A: Identifying Protocol Capabilities	23
Review	24



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

This module provides students with information about common network protocols supported by Microsoft® Windows® 2000. The module begins with an introduction to protocols, types of protocols, the OSI reference model, and protocol stacks.

Lab:
15 Minutes

The module then describes routable and non-routable protocols and the types of data transmissions in a network. The module next discusses the common protocols supported by Windows 2000, such as TCP/IP, IPX/SPX, NetBEUI, and AppleTalk, and examines their characteristics.

The module continues with a discussion of other communication technologies, such as ATM and IrDA, which are supported by Windows 2000. The module concludes with a description of remote access protocols supported by Windows 2000, such as dial-up protocols and VPN protocols.

A lab in which students identify protocol capabilities follows the last section of the module.

At the end of this module, students will be able to:

- Define a protocol and describe the types of protocols.
- Describe the protocol characteristic that determines if a computer can communicate with other computers in a network.
- Name the common network protocols supported by Windows 2000 and describe their characteristics.
- Name the communication protocols and technologies that are compatible with Windows 2000 and describe their characteristics.
- Describe the protocols used for remote access: dial-up protocols and virtual private network (VPN) protocols.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_05.ppt
- Module 5, “Examining Network Protocols”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Introduction to Protocols**
Introduce the concept of a protocol and explain the two types of protocols—open and vendor-specific. Briefly discuss the OSI reference model. Explain protocol stacks but do not attempt to map the types of protocols in a stack to the OSI model.
- **Protocols and Data Transmissions**
Explain the difference between routable and non-routable protocols. Describe the three types of data transmissions.
- **Common Protocols**
Discuss the common protocols supported by Windows 2000 by examining the characteristics of TCP/IP, IPX/SPX, NetBEUI, and AppleTalk.
- **Other Communication Protocols**
Describe the characteristics of other communications technologies supported by Windows 2000, such as ATM and IrDA. Discussion of these protocols should be at a high level.
- **Remote Access Protocols**
Discuss the two types of remote access protocols that Windows 2000 supports. Provide high-level descriptions of the characteristics of the different dial-up and VPN protocols.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

This module includes only a computer-based interactive lab exercise, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about communication protocols, their characteristics, the common protocols used for network communication, and other protocols compatible with Windows 2000 networks.

- Introduction to Protocols
- Protocols and Data Transmissions
- Common Protocols
- Other Communication Protocols
- Remote Access Protocols

*****ILLEGAL FOR NON-TRAINER USE*****

To ensure that computers in a network are able to communicate, they must share a common language known as a *protocol*. A protocol is a set of rules or standards that enables communication between computers in a network. A number of protocols are available today, each having its own set of characteristics and capabilities. However, not every protocol is compatible with all computers and operating systems. To determine if a client computer in a Microsoft® Windows® 2000 network can communicate with other computers in the network, you must be familiar with the protocols supported by the Windows 2000 operating system.

Windows 2000 supports many of the common network protocols available today, as well as other communication protocols, including protocols for remote access. The compatibility of Windows 2000 with different types of protocols enhances the usability of Windows 2000 in different network environments.

At the end of this module, you will be able to:

- Define a protocol and describe the types of protocols.
- Describe the protocol characteristic that determines if a computer can communicate with other computers in a network.
- Name the common network protocols supported by Windows 2000 and describe their characteristics.
- Name the communication protocols and technologies that are compatible with Windows 2000 and describe their characteristics.
- Describe the protocols used for remote access: dial-up protocols and virtual private network (VPN) protocols.

◆ Introduction to Protocols

Topic Objective

To introduce the types of protocols, the OSI model, and the concept of protocol stacks.

Lead-in

Protocols are the rules and procedures that govern the communication between computers in a network.

- Types of Protocols
- Open Systems Interconnection (OSI) Reference Model
- Protocol Stacks

*****ILLEGAL FOR NON-TRAINER USE*****

Protocols are software and must be installed on network components that need them. Computers can communicate with each other only if they use the same protocol. If the protocol used by a computer in a network is not compatible with the protocol used by another computer, the two computers cannot exchange information. A variety of protocols are available for use in specific network environments. Although each protocol facilitates basic network communication, each has a different function and accomplishes different tasks.

You can understand the function of different protocols by examining the standard model for networks—the Open Systems Interconnection (OSI) reference model. This model is built around a set of seven protocol layers, and each layer is responsible for some function that assists in the transmission of data over the network.

According to the OSI conceptual model, several protocols must work together to ensure the proper transmission of data. In reality, this is achieved with the help of a *protocol stack*. A protocol stack is a collection of protocols that function together to transmit data across a network of computers.

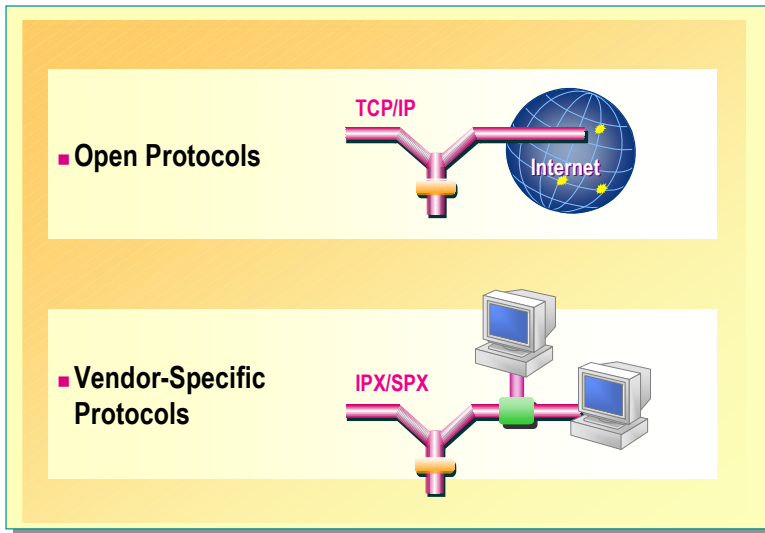
Types of Protocols

Topic Objective

To introduce the two types of network protocols.

Lead-in

Protocols are either open or vendor-specific.



*****ILLEGAL FOR NON-TRAINER USE*****

Two types of protocols are available today: open and vendor-specific.

Open Protocols

Open protocols are protocols that are written to publicly known industry standards. A protocol that adheres to these industry standards is compatible with other protocols written to the same standards. Open protocols are nonproprietary (not privately owned). A common example of an open protocol is Transmission Control Protocol/Internet Protocol (TCP/IP), which is used as the standard for communication over the Internet.

Vendor-Specific Protocols

Vendor-specific protocols are proprietary and have been developed by different vendors for use in specific environments. For example, Novell provides a set of protocols, such as Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), developed specifically for its NetWare architecture.

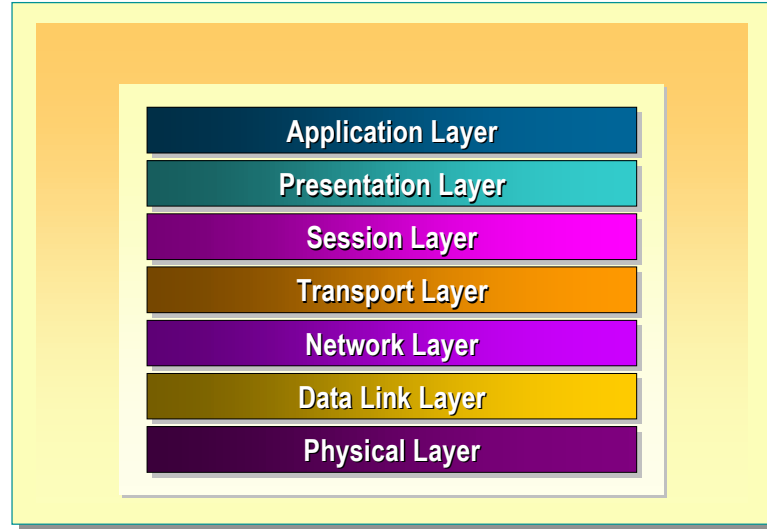
Open Systems Interconnection (OSI) Reference Model

Topic Objective

To introduce the seven layers of the OSI model.

Lead-in

The OSI model is built around a set of seven protocol layers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

The OSI model divides network communications into seven layers, with each layer having specific functionality for transmitting data on the network.

Delivery Tip

Explain to the class that the function of the protocols working at each layer of the OSI model is defined by the role of that layer in transmitting data.

The need for worldwide standardization of technologies led to the creation of the International Organization for Standardization (ISO). ISO is responsible for standardizing the methods by which computers communicate worldwide. To do so, ISO created a model for network communication, called the Open Systems Interconnection (OSI) reference model, or the OSI model.

OSI Model

The OSI model divides network communications into seven layers. Each layer carries out specific functions in transmitting data on the network.

Before data is moved through the layers of the OSI model, it must be divided into *packets*. A packet is a unit of information that is transmitted as a whole from one computer to another on a network. The network passes a packet from layer to layer, and at each layer some additional formatting is added to the packet.

The layer at which a protocol works describes the function of the protocol. Some protocols work only at particular layers of the OSI model.

OSI layer	Function
Application Layer	Defines how applications interact with each other
Presentation Layer	Adds common formatting for data representation
Session Layer	Establishes and maintains communications channels
Transport Layer	Ensures error-free delivery of data
Network Layer	Addresses messages both within and between networks
Data Link Layer	Defines access methods for the physical medium, such as the network cable
Physical Layer	Puts the data on the physical medium

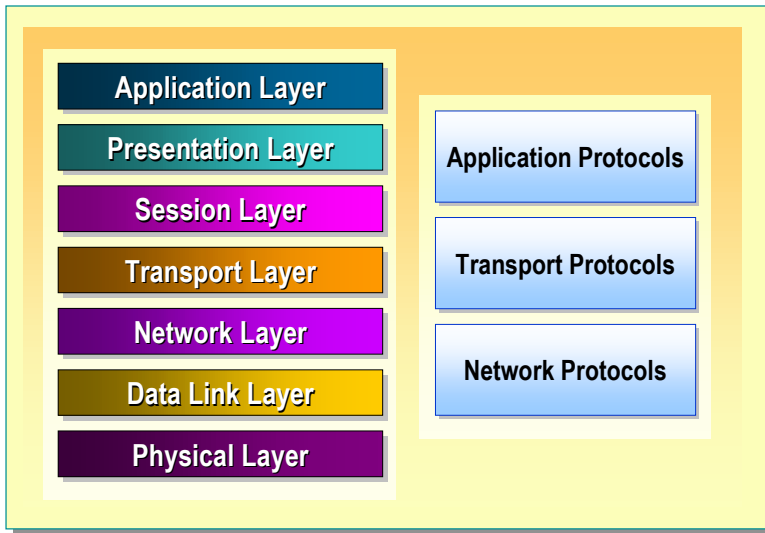
Protocol Stacks

Topic Objective

To introduce the concept of protocol stacks.

Lead-in

A protocol stack is a collection of protocols that work together to transmit data between computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

A protocol stack is a layered set of related protocols that ensure data is properly transmitted in a network.

Delivery Tip

Do not map the types of protocols in a stack to the OSI model layers. Use the graphics to explain to the class that each protocol stack compares to the basic OSI model but may have a different number of layers.

The OSI model defines distinct layers related to packaging, sending, and receiving data transmissions in a network. A layered set of related protocols actually carries out these services. This layered set of protocols running on a network is called a protocol stack. Together, the protocols in the stack handle all tasks required in packaging, sending, and receiving transmissions.

Several protocol stacks are designated as standard protocol models. Some of the common protocol stacks are TCP/IP, IPX/SPX, and AppleTalk. Protocols exist at each layer of these stacks, performing the tasks specified by that layer. Generally, however, the responsibility for performing specific communication tasks in the network is assigned to protocols working as one of three types: application protocols, transport protocols, and network protocols.

Application Protocols

Application protocols provide data exchange between applications in a network. Examples of common application protocols include File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).

Transport Protocols

Transport protocols provide for communication sessions between computers and ensure that data moves reliably between computers. A common transport protocol is Transmission Control Protocol (TCP).

Network Protocols

Network protocols provide what are called *link services*. These protocols define the rules for communicating in a particular network environment. A common protocol that provides network services is Internet Protocol (IP).

◆ Protocols and Data Transmissions

Topic Objective

To introduce routable and non-routable protocols and the types of data transmissions.

Lead-in

Protocols may or may not support data transmission between network segments through any available path.

- **Routable/Non-Routable Protocols**
- **Types of Data Transmission**

*****ILLEGAL FOR NON-TRAINER USE*****

In a large network, it is difficult to manage communication efficiently because of the large volume of network traffic. Network administrators can bypass this problem by dividing large networks into *network segments*. Network segments are smaller networks, which, when combined, form a large network.

Within a network, data may be transmitted from one network segment to another along any of several available paths. The transmission of data between network segments is called *routing*. However, not every protocol supports routing. Protocols are categorized as routable or non-routable based on their ability or inability to support routing.

The ability of protocols to support routing enables data transmission between computers in different network segments. There are different types of data transmissions. Each transmission type determines which computers in a network receive the transmitted data. Because not all computers on the network may need to receive the transmitted data, you can control to a certain degree which computers receive and process the transmitted data by controlling the type of transmission.

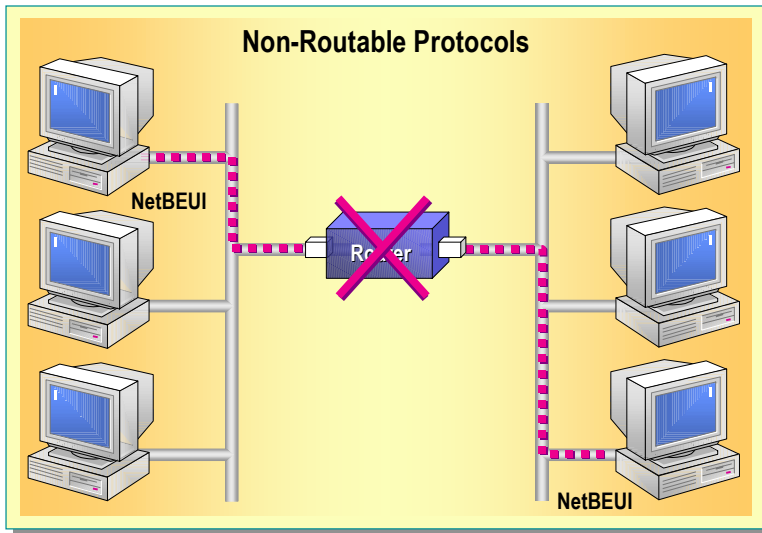
Routable/Non-Routable Protocols

Topic Objective

To illustrate routable and non-routable protocols.

Lead-in

Protocols may or may not support communication between different network segments based on whether the protocols are routable or non-routable.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Routable protocols enable computers in one network segment to communicate with those in another segment.

Only computers running routable protocols can transmit data to computers in other network segments.

Delivery Tip

Use the animation to explain the difference between routable and non-routable protocols.

Based on whether or not protocols support routing, they can be categorized as routable or non-routable protocols.

Routable Protocols

Routable protocols support communication between LANs or network segments that may be spread throughout a building, across a small geographic area, such as a college campus, or across the globe, such as the Internet. Routable protocols support the transmission of data from one network segment to another along any of several paths connecting the two network segments. Examples of routable protocols are TCP/IP and IPX/SPX.

Non-Routable Protocols

Non-routable protocols, unlike routable protocols, do not support the transmission of data from one network segment to another. Computers that use non-routable protocols can communicate only with other computers in the same network segment. NetBEUI and Data Link Control (DLC) are examples of non-routable protocols.

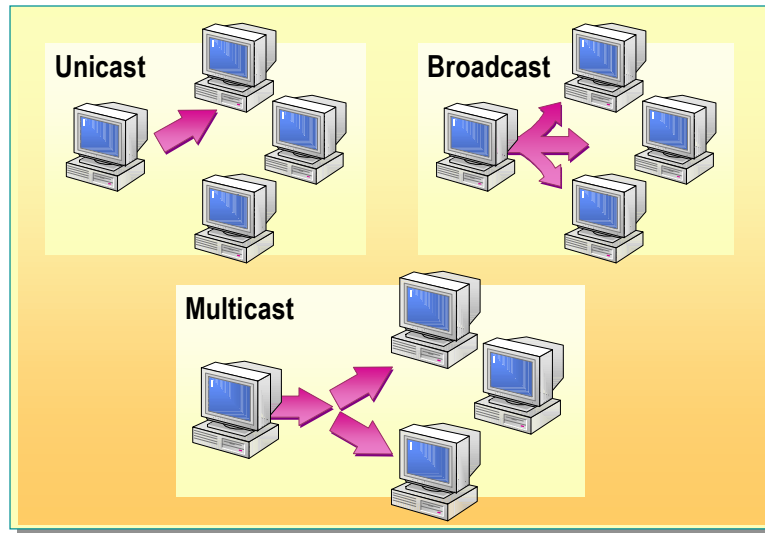
Types of Data Transmissions

Topic Objective

To explain the three types of data transmissions.

Lead-in

Data is transmitted over a network in three ways: unicast, broadcast, and multicast.



*****ILLEGAL FOR NON-TRAINER USE*****

Routable protocols enable the transmission of data between computers in different segments of a network. However, high volumes of certain kinds of network traffic, such as the deployment of multimedia applications, can affect network efficiency because it slows down transmission speed. The amount of network traffic generated varies with the three types of data transmissions: unicast, broadcast, or multicast. To understand how each transmission type affects network traffic, you must be familiar with the characteristics of each type of transmission.

Unicast

In a unicast transmission, a separate copy of the data is sent from the source to each client computer requesting it. No other computer on the network needs to process the traffic. However, unicast transmission is not as efficient when multiple computers request the same data because the source transmits multiple copies of the data. Unicast transmission works best when just a small number of client computers request the data. Unicast transmission is also referred to as directed transmission. Most traffic on networks today is unicast.

Broadcast

When data is broadcast, a single copy of the data is sent to all clients on the same network segment as the sending computer. However, if that data must be sent to only a portion of the network segment, broadcast transmission is not an efficient transmission method because data is sent to the whole segment irrespective of whether it is required. This needlessly slows the performance of the network because each client must process the broadcast data.

Multicast

In a multicast transmission, a single copy of the data is sent only to client computers requesting it. Multiple copies of data are not sent across the network. This minimizes the network traffic and enables the deployment of multimedia applications on the network without overburdening the network. Many Internet services use multicasting to communicate with client computers.

◆ Common Protocols

Topic Objective

To introduce common network protocols.

Lead-in

Windows 2000 supports many of the commonly used network protocols.

- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)**
- **NetBIOS Enhanced User Interface (NetBEUI)**
- **AppleTalk**

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 supports many different networking protocols. Different protocols are needed for communication with systems, devices, and computers in various environments. Some protocols are routable, and others are not. Based on which protocols are used by a client computer, you can determine whether or not that computer can communicate with other computers in a routed Windows 2000 network. The common network protocols that you can use with Windows 2000 are:

- Transmission Control Protocol/Internet Protocol (TCP/IP).
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
- NetBIOS Enhanced User Interface (NetBEUI).
- AppleTalk.

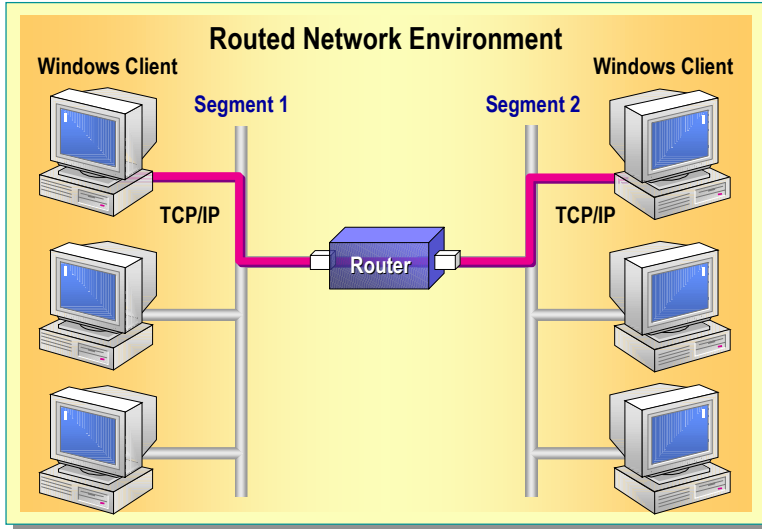
Transmission Control Protocol/Internet Protocol (TCP/IP)

Topic Objective

To illustrate how TCP/IP functions in a routed network environment.

Lead-in

TCP/IP is an industry-standard protocol stack that most networks support for its interoperability among different types of computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

TCP/IP is a standard protocol stack that is supported by most networks for its interoperability.

Delivery Tip

Use the graphic on the slide to explain to the class that TCP/IP enables computers to communicate between segments in a routed network environment.

TCP/IP is an industry-standard protocol stack (a layered set of protocols) that enables communication in different networking environments. Because of the interoperability of TCP/IP among different types of computers, most networks support TCP/IP.

TCP/IP supports routing and enables computers to communicate across network segments. Because of this feature, TCP/IP is the standard protocol for communications over the Internet. Its reliable delivery and global use have made TCP/IP a necessity for accessing worldwide information networks, such as the Internet. However, you must configure TCP/IP on all computers with which you want to use the protocol to communicate.

TCP/IP offers the following advantages:

- It is an industry standard. As an industry standard, it is an open protocol that is not controlled by a single organization.
- It contains a set of utilities for connecting dissimilar operating systems. Connectivity between two computers does not depend on the network operating system of either computer.
- It uses scalable, cross-platform, client-server architecture. TCP/IP can expand or shrink to meet the future needs of a network.

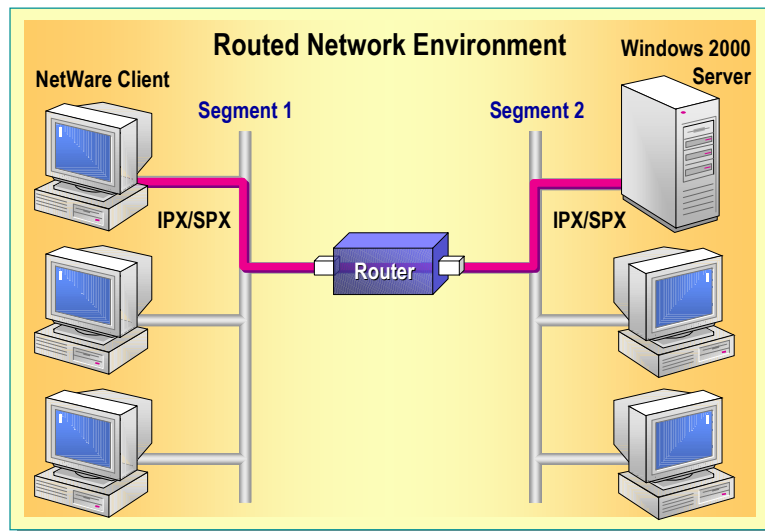
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Topic Objective

To illustrate how IPX/SPX functions.

Lead-in

Windows 2000 supports IPX/SPX, a common protocol used with NetWare.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

IPX/SPX is a routable protocol stack used in NetWare environments.

Delivery Tip

Use the graphic on the slide to explain to the class that IPX/SPX enables a NetWare client computer to communicate with a Windows 2000 server in a routed network environment.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a protocol stack developed specifically for NetWare architecture. The IPX/SPX stack includes IPX and SPX. IPX defines the addressing schemes used on a NetWare network, and SPX provides security and reliability to the IPX protocol. IPX is a network-layer protocol that is equivalent to the IP of the TCP/IP protocol stack. SPX provides reliable service at the transport layer.

IPX/SPX has the following characteristics:

- It is used on networks with NetWare servers.
- It is routable. IPX/SPX enables computers in a routed networking environment to exchange information across segments.

Note NWLink IPX/SPX/NetBIOS Compatible Transport Protocol is a Microsoft version of IPX/SPX and is included with Windows 2000. Client computers running Windows 2000 can use NWLink to access client and server applications running on NetWare servers. NetWare clients can use NWLink to access client and server applications running on Windows 2000-based servers. With NWLink, computers running Windows 2000 can communicate with other network devices, such as printers, that use IPX/SPX. You can also use NWLink in small networks that only use Windows 2000 and other Microsoft client software.

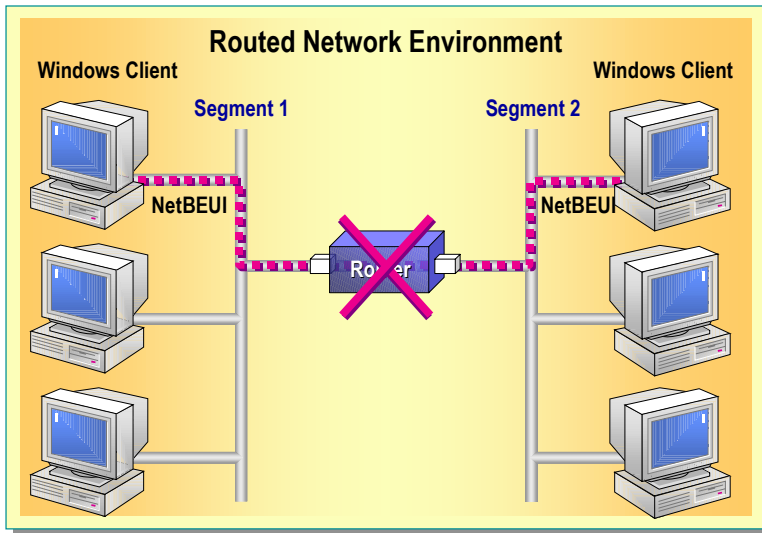
NetBIOS Enhanced User Interface (NetBEUI)

Topic Objective

To illustrate how NetBEUI functions.

Lead-in

NetBEUI is a protocol that is supported by all Microsoft network products, including Windows 2000.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

NetBEUI is a non-routable protocol supported by all Microsoft network products, including Windows 2000.

Delivery Tip

Use the graphic on the slide to explain to the class that NetBEUI enables communication between Windows-based client computers on the same segments of a routed network environment.

NetBIOS Enhanced User Interface (NetBEUI) was one of the earliest protocols available for use on networks composed of personal computers. It was designed around the Network Basic Input/Output System (NetBIOS) interface to be a small, efficient protocol for use in department-sized LANs of 20 to 200 computers, which would not need to be routed to other subnets.

At present, NetBEUI is used almost exclusively on small, non-routed networks consisting of computers running a variety of operating systems.

Windows 2000-based NetBEUI, known as NetBIOS Frame (NBF), is the underlying implementation of the NetBEUI protocol and is installed on computers running Windows 2000. It provides compatibility with existing LANs that use the NetBEUI protocol.

The advantages of NetBEUI include:

- Small stack size.
- No configuration requirement.
- High speed of data transfer on the network.
- Compatibility with all Microsoft-based operating systems, including Windows 2000.

The major disadvantage of NetBEUI is that it does not support routing. Because of this, computers running NetBEUI can communicate only with other computers in the same network segment.

Note Network Basic Input/Output System (NetBIOS) allows applications to access the network functionality of the operating system and manage the network names used to communicate on a network.

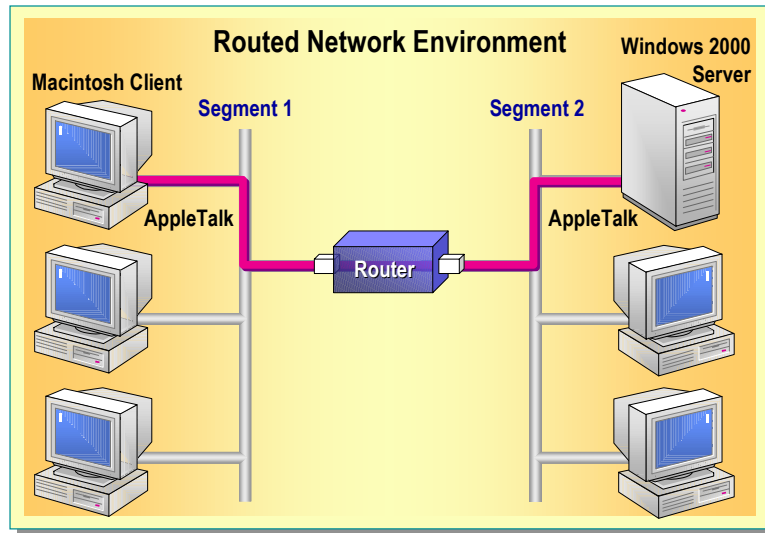
AppleTalk

Topic Objective

To illustrate how AppleTalk functions.

Lead-in

Windows 2000 supports AppleTalk, a routable protocol used with Apple Macintosh networks.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

AppleTalk is a routable protocol stack used in Apple Macintosh environments.

Delivery Tip

Use the graphic on the slide to explain to the class that AppleTalk enables a Macintosh client computer to communicate with a Windows 2000-based server in a routed network environment.

AppleTalk is Apple Computer's proprietary protocol stack designed to enable Apple Macintosh computers to share files and printers in a network environment.

Some of the characteristics of the AppleTalk protocol are:

- It enables Macintosh clients to access a server running Windows 2000.
- It is routable. Computers running AppleTalk can communicate across segments in a routed network environment.
- It enables Macintosh clients to access print services provided by a server running Windows 2000 if Print Server for Macintosh is installed on the server.

◆ Other Communication Protocols

Topic Objective

To introduce other communication technologies supported by Windows 2000.

Lead-in

In addition to supporting most commonly used networking protocols, the Windows 2000 operating system supports other communication protocols and technologies, such as ATM and IrDA.

- **Asynchronous Transfer Mode (ATM)**
- **Infrared Data Association (IrDA)**

*****ILLEGAL FOR NON-TRAINER USE*****

In addition to supporting most commonly used networking protocols, the Windows 2000 operating system supports other communication protocols and technologies, such as:

- Asynchronous transfer mode (ATM).
- Infrared Data Association (IrDA).

ATM and IrDA are both international standards for communication technologies. ATM was developed for the high-speed transmission of multimedia content, and IrDA was developed for wireless connectivity.

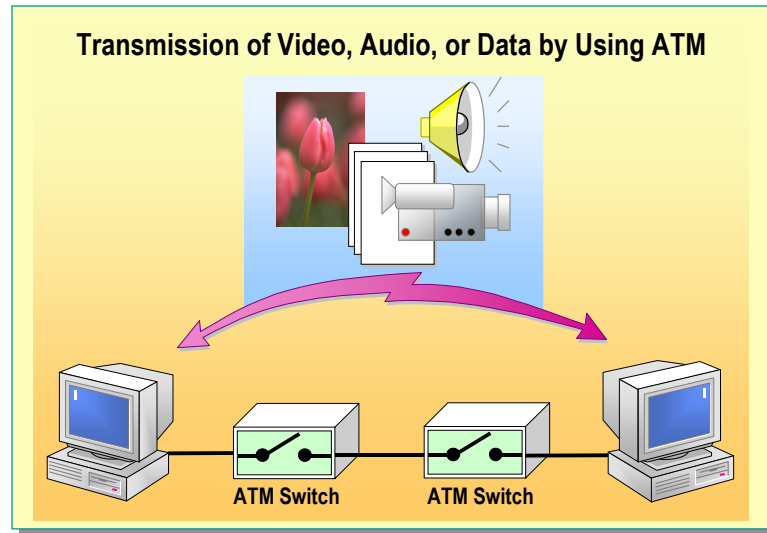
Asynchronous Transfer Mode (ATM)

Topic Objective

To illustrate how ATM functions.

Lead-in

ATM is a high speed, connection-oriented protocol that transports multiple types of traffic across a network.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

ATM is a high-speed, connection-oriented protocol that transports multiple types of traffic across a network.

Delivery Tip

Use the graphic on the slide to explain to the class that ATM enables a high-speed transmission of multimedia applications between computers in a network.

Asynchronous transfer mode (ATM) is a high-speed protocol that transports multiple types of traffic across a network. The ATM technology was developed from international standards for the simultaneous transmission of data, voice, and video over a network at high speed. A device called an ATM switch is used to enable network communication by using the ATM protocol. Client computers communicate with each other by means of a network of ATM switches.

Some of the characteristics of ATM are:

- It provides a single network connection that can reliably mix voice, video, and data. ATM can simultaneously transport such electronic communication as telephone calls, movies, and the e-mail and files contained on a Web server.
- It provides high-speed communication.
- It assures that no single type of data overuses the line. It efficiently allocates network bandwidth, thereby guaranteeing the reliability of the connection.

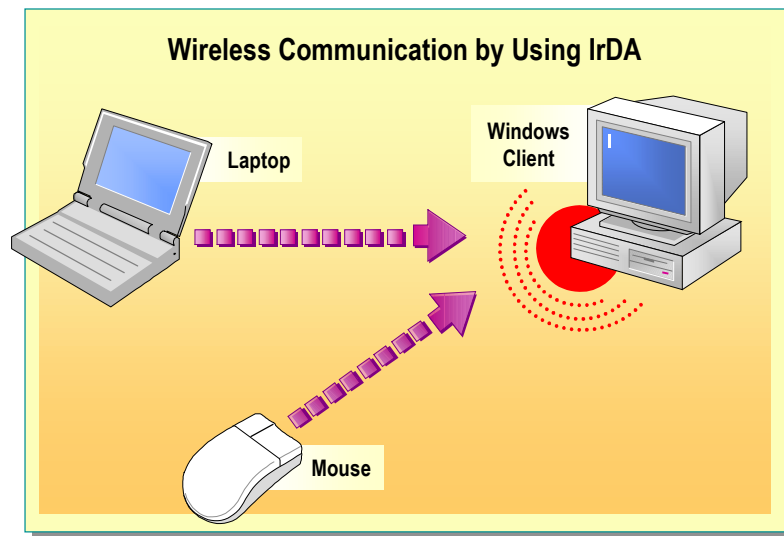
Infrared Data Association (IrDA)

Topic Objective

To illustrate how IrDA functions.

Lead-in

IrDA enables wireless communication between a variety of devices, such as cameras, laptops, and printers.



*****ILLEGAL FOR NON-TRAINER USE*****

The Infrared Data Association (IrDA) is an association that defined the group of short-range, high speed, bidirectional wireless infrared protocols, generically referred to as IrDA. The IrDA protocol stack enables computers running Windows 2000 to connect easily to peripheral devices or other computers without the use of connecting cables. For example, Windows 2000 automatically detects infrared devices, such as other computers or cameras, which are within range of each other. IrDA enables users to transfer information and share resources, such as printers, cameras, portable computers, desktop computers, and personal digital assistants (PDAs).

IrDA enables wireless communication between any two infrared devices within range of each other. For example, two users traveling with laptop computers can transfer files by setting up an IrDA connection, instead of by using cables or floppy disks. IrDA automatically configures the connection when the portable computers are placed within close proximity. In addition, IrDA enables a computer to access resources that are attached to another computer. For example, if a user with a laptop computer needs to print a document, the user can create an IrDA connection with a computer that is connected to a printer, either locally or on a network. When that connection is established, the user, with appropriate permissions, can print over the IrDA connection.

The characteristics of IrDA wireless communication include:

- A worldwide standard for wireless infrared connectivity.
- Ease of implementation and use.
- No risk of radiation from infrared rays.
- No electromagnetic noise.
- No government regulatory issues.
- Minimum crosstalk (signal overflow from adjacent cable).

◆ Remote Access Protocols

Topic Objective

To introduce the topics related to remote access protocols.

Lead-in

Remote access requires protocols that enable the connection between the client and the server. Depending on your requirements, you can choose the appropriate protocol.

- Dial-up Protocols
- VPN Protocols

*****ILLEGAL FOR NON-TRAINER USE*****

In Windows 2000, you can establish a remote connection by using either dial-up remote access or a virtual private network (VPN). To establish a remote access connection to a Windows 2000 network, you can select from the following remote access protocols:

- Dial-up protocols
- VPN protocols

These remote access protocols are supported by Windows 2000 and provide interoperability with third party remote access components. Understanding the features of each protocol will help you decide which protocol is appropriate for your network.

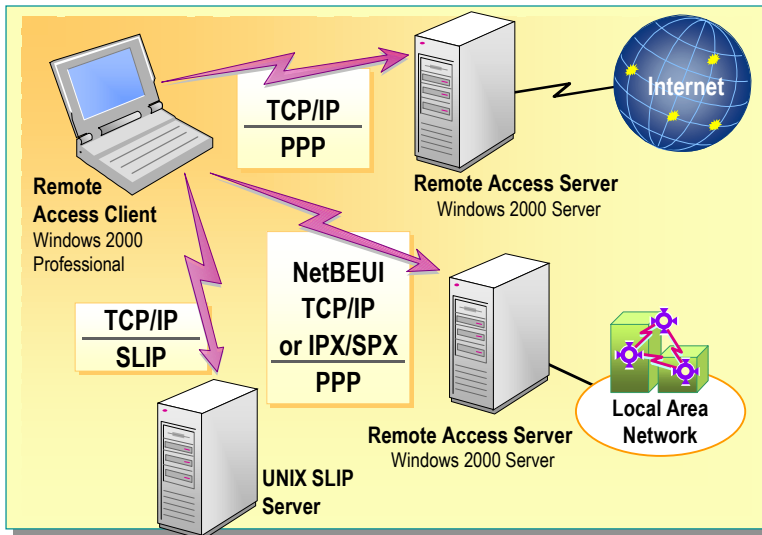
Dial-up Protocols

Topic Objective

To illustrate the dial-up remote access protocols used by remote access clients and servers.

Lead-in

In dial-up connectivity, you can use either the SLIP protocol or the PPP protocol to provide clients with access to a variety of remote access servers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Windows 2000 does not provide a SLIP server because SLIP servers are less secure and less efficient than PPP servers.

Windows 2000 supports dial-up remote access protocols, such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP), to provide clients with access to a variety of remote access servers.

SLIP

SLIP allows remote access clients to connect to a remote access server through a modem. This allows client computers running Windows 2000 to connect to SLIP servers. A SLIP server is a remote access protocol component on the remote access server that services connection requests from SLIP clients. Although client computers running Windows 2000 can connect to SLIP servers, Routing and Remote Access does not itself include a SLIP server component. Therefore, you cannot use a computer running Windows 2000 as a SLIP server. Instead, you can use a server running UNIX as a SLIP server.

SLIP is an industry standard protocol that addresses TCP/IP connections made over serial lines. SLIP is supported by Routing and Remote Access and gives clients running Windows 2000 access to Internet services. SLIP has several limitations:

- Support is limited to TCP/IP. You cannot use SLIP to directly transfer other network protocols, such as IPX/SPX or NetBEUI.
- A static IP address is required. SLIP requires the client to configure all of the TCP/IP configuration parameters, such as the IP address, prior to establishing a connection to the server.
- It typically relies on text-based logon authentication sessions and usually requires a scripting system to automate the logon process.
- It transmits authentication passwords as clear text. This might result in a security compromise because passwords are not encrypted during user authentication.

PPP

PPP is a set of industry-standard protocols that enable remote access clients and servers to operate in a network consisting of components manufactured by multiple vendors. PPP supports encrypted password authentication. PPP is an enhancement to the original SLIP specification and provides a standard method for sending network data over a point-to-point link.

PPP support enables computers running Windows 2000 to connect to remote networks through any server that complies with PPP standards. PPP compliance also enables a server to receive calls from, and provide access to, other vendors' remote access software.

The PPP architecture enables clients to use any combination of NetBEUI, TCP/IP, and IPX/SPX network transport protocols. You can run applications written to the IPX/SPX, NetBIOS, or Windows Sockets (WinSock) interface on a remote computer running Windows 2000. The PPP architecture enables a server to download and configure TCP/IP parameters.

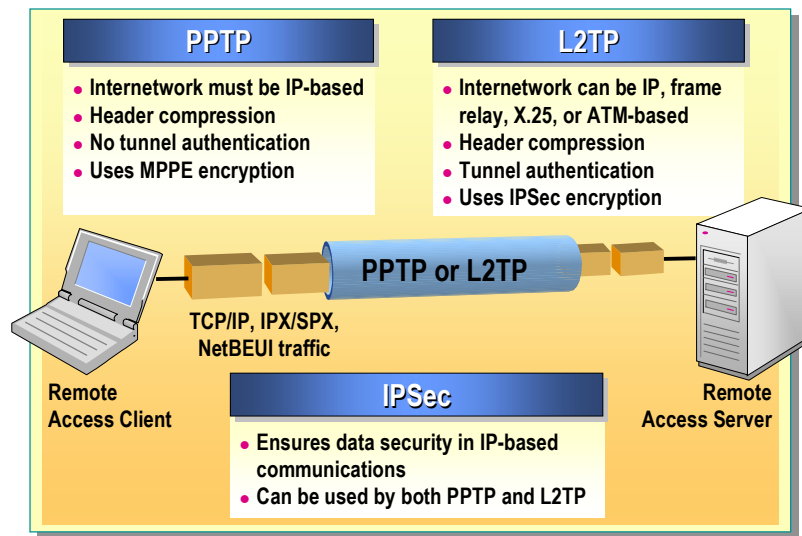
VPN Protocols

Topic Objective

To list the features of the VPN protocols used by remote access clients and servers.

Lead-in

Virtual private networks (VPNs) provide remote access without relying on hardware by using an additional protocol that allows users to connect to LANs over their existing Internet or dial-up connections.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic is animated. First display the graphic, and then display the features of PPTP, L2TP, and IPSec as you talk about them.

Key Point

VPNs work by putting normal data packets inside encrypted PPP packets.

You can use virtual private networks (VPNs) to provide remote access without having to rely on dial-up networking hardware, such as modems, on the remote access servers. VPNs use an additional protocol that allows users to connect to LANs over their existing Internet or dial-up connections. These connections can be secure even though the connection may use public Internet hardware.

VPN protocols encapsulate TCP/IP, IPX/SPX, or NetBEUI data packets inside PPP data packets. The remote access server, with the help of the client, performs all security checks and validations and enables data encryption, making it safe to send data over non-secure networks, such as the Internet. Typically, users connect to the VPN by first connecting to an Internet service provider (ISP) and then connecting to the VPN ports through that Internet connection.

VPNs use either Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to establish connections.

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) enables the secure transfer of encapsulated data from a PPTP client to a PPTP server across a TCP/IP internetwork, such as the Internet. PPTP encapsulates PPP frames in TCP/IP packets for transmission over an internetwork. Because of this encapsulation, you can use all features of PPP, including TCP/IP, IPX/SPX, NetBEUI, and Microsoft Point-to-Point Encryption (MPPE), in a PPTP virtual private network.

Windows 2000 supports PPTP, which you can use in private LAN-to-LAN networking.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an industry standard tunneling protocol. Like PPTP, L2TP uses the authentication and compression mechanisms of PPP. Unlike PPTP, L2TP does not utilize MPPE to encrypt PPP frames. Instead, L2TP relies on Internet Protocol Security (IPSec) for encryption services. The result is that L2TP-based virtual private network connections are typically a combination of L2TP and IPSec. For an encrypted L2TP virtual private network, both the client and the server must support L2TP and IPSec.

L2TP allows any combination of TCP/IP, IPX/SPX, or NetBEUI traffic to be encrypted and then sent over any medium that supports point-to-point packet delivery, such as Ethernet, X.25, frame relay, or asynchronous transfer mode (ATM).

IPSec

Internet Protocol Security (IPSec) ensures data security in TCP/IP-based communications by providing an additional layer of network security. IPSec integrates with the security inherent in Windows 2000 to safeguard intranet and Internet communications. The VPN protocols, PPTP and L2TP, can be combined with the security provided by IPSec to provide data security.

IPSec provides data integrity and encryption. It is superior to PPTP, which uses MPPE encryption. Using IPSec results in both increased demands on the CPU resources of the client and the server and an increased network payload.

Lab A: Identifying Protocol Capabilities

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify which protocols are used to communicate with other computers on another segment and the different types of transmissions made by computers on the network.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Identify which protocols are used to enable communication with other computers on another segment of a network.
- Identify the different types of transmissions made by computers on the network.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors. (16-bit recommended).
- Microsoft Internet Explorer 5 or later.

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Protocol Capabilities**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 15 minutes

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Protocols
- Protocols and Data Transmissions
- Common Protocols
- Other Communication Protocols
- Remote Access Protocols

*****ILLEGAL FOR NON-TRAINER USE*****

1. You want to modify an existing protocol to better suit your networking needs. You realize that you can use an open protocol for this purpose. Which of the following protocols can you use?
 - A. IPX/SPX.
 - B. AppleTalk.
 - C. NetBEUI.
 - D. TCP/IP.
 - D. TCP/IP.**

2. The users in your network need to conduct business over the Internet. Which protocol will you install in the network to allow the users to communicate over the Internet?
 - A. IPX/SPX.
 - B. TCP/IP.
 - C. AppleTalk.
 - D. NetBEUI.
 - B. TCP/IP.**

-
3. You have a small workgroup that uses Windows 2000 and other Microsoft-based operating systems. You need to install a protocol that requires minimal configuration to enable communication within the workgroup. Which protocol will you install?
- A. IPX/SPX.
 - B. TCP/IP.
 - C. AppleTalk.
 - D. NetBEUI.
 - D. NetBEUI.**
4. You need to transfer large amounts of audio, video, and data files simultaneously over a network. Which of the following protocols enables the high-speed transmission of this data over the network?
- A. ATM.
 - B. TCP/IP.
 - C. IrDA.
 - D. NetBEUI.
 - A. ATM.**
5. You want to set up a Windows 2000-based server to enable remote clients to connect to the server by using SLIP or PPP. Can you do this? If so, does it require configuration?
- A. Yes. The setup configurations are automatic.
 - B. Yes, you can do it without any additional configurations.
 - C. No, because Windows 2000 cannot be used as a SLIP server.
 - D. No, because Windows 2000 cannot be used as a PPP server.
 - C. No, because Windows 2000 cannot be used as a SLIP server.**

Module 6: Examining TCP/IP

Contents

Overview	1
Introduction to TCP/IP	2
TCP/IP Protocol Suite	7
Lab A: Using TCP/IP Utilities	17
Name Resolution	20
Examining the Data Transfer Process	26
Routing Data	32
Lab B: Identifying Processes and Protocols in TCP/IP	37
Review	38



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
105 Minutes

Labs:
30 Minutes

This module provides students with an overview of TCP/IP concepts and how TCP/IP handles network communication. The first section of the module begins with an introduction to the communication process and is followed by an overview of the four layers in the protocol stack. The first section concludes with a discussion of the use of sockets in identifying the applications involved in a communication at any given time.

The next section describes the protocols in the TCP/IP protocol suite and the functions each performs in the communication process. This section concludes with information about some of the various utilities—Hostname, Arp, and Ping—included with the TCP/IP suite. In the lab that follows this section, the students will use the Hostname, Arp, and Ping utilities, as examples of TCP/IP utilities, to test connectivity.

The third section in the module focuses on the name resolution process. It begins with a description of host names and NetBIOS names and then explains static and dynamic mapping and the name resolution process.

The next section examines the TCP/IP data transfer process. This section explains the terminology used to refer to a packet and discusses the frame components and the route taken by the data to travel from the source computer to the destination computer. This continues the analogy introduced in the first section and identifies how the TCP/IP protocols interact to enable communication between computers.

The last section of the module describes the routing process. The types of packet delivery are explained and then the process by which data is routed across a network to its final destination is detailed. The analogy from the first section ends here with an explanation that describes how packets are routed from one router to another until the packet reaches its destination. The module concludes with a lab in which the students identify the processes involved with name resolution and the protocols involved in using the Ping utility across a router.

At the end of this module, students will be able to:

- Describe the TCP/IP communication process.
- Name the protocols in the TCP/IP protocol stack and describe the services they provide.
- Describe the process for resolving user-friendly computer names by mapping them to an IP address.
- Describe the process for sending data packets from one computer to another.
- Describe how the process of routing passes information between two segments so that computers can communicate on a larger scope.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2151A_06.ppt
- Module 6, “Examining TCP/IP”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Read the TCP/IP topic in Windows 2000 Help.
- Read the white papers, *Introduction to TCP/IP* and *TCP/IP Implementation Details for Windows 2000*, on the Trainer Materials compact disc.
- Complete the two labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- Introduction to TCP/IP
Provide an overview of the data communication process. Then briefly introduce the layers in the TCP/IP protocol stack and explain how sockets are used to differentiate one communication connection from another.
- TCP/IP Protocol Suite
Describe the features and functions of each protocol in the TCP/IP suite and the utilities included in it. Then demonstrate the usage of the Hostname, Arp, and Ping utilities.
- Name Resolution
Describe the two types of computer names, the concepts of static and dynamic mapping, and the name resolution process for host names as well as NetBIOS names.
- Examining the Data Transfer Process
Explain the different terms used to refer to the data packet at various stages of preparing it for transmission across the network. Describe the components of a data packet and the process used to prepare it at the source computer and to access the information in it at the destination computer.
- Routing Data
Describe the process of IP routing and the types of packet delivery. Then explain the process by which data is routed from one segment to another.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about communication in a Windows 2000 network by using the TCP/IP protocol suite.

- Introduction to TCP/IP
- TCP/IP Protocol Suite
- Name Resolution
- Examining the Data Transfer Process
- Routing Data

*****ILLEGAL FOR NON-TRAINER USE*****

Transmission Control Protocol/Internet Protocol (TCP/IP) for Microsoft® Windows® 2000 offers a standard, routable enterprise networking protocol that is the most complete and accepted protocol available. Most network operating systems in use today offer TCP/IP support, and large networks rely on TCP/IP for much of their network traffic.

TCP/IP provides a technology for connecting dissimilar systems. It also provides a robust, scaleable, cross-platform client/server framework and a foundation for gaining access to global Internet services, such as the World Wide Web and e-mail.

The various protocols in the TCP/IP stack function together to make network communication happen. This process involves multiple activities, including resolving user-friendly computer names to Internet Protocol (IP) addresses; determining the location of the destination computer; and packaging, addressing, and routing the data so that it reaches the destination successfully.

At the end of this module, you will be able to:

- Describe the TCP/IP communication process.
- Name the protocols in the TCP/IP protocol stack and describe the services they provide.
- Describe the process for resolving user-friendly computer names by mapping them to an IP address.
- Describe the process for sending data packets from one computer to another.
- Describe how the process of routing passes information between two segments so that computers can communicate on a larger scope.

◆ Introduction to TCP/IP

Topic Objective

To introduce the TCP/IP protocol suite.

Lead-in

Windows 2000 supports TCP/IP both as a protocol and as a set of services for connecting and managing networks.

- The Communication Process
- TCP/IP Layers
- Identifying Applications

*****ILLEGAL FOR NON-TRAINER USE*****

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard protocol stack that is used for communication between Windows 2000-based computers. TCP/IP is designed for communication across large-scale networks.

The tasks involved in using TCP/IP in the communication process are distributed between protocols that are organized into four distinct layers of the TCP/IP stack. Each protocol in the TCP/IP stack has a distinct role in the communication process.

During the communication process, many applications may be in communication at the same time. TCP/IP has the ability to differentiate one application from another. TCP/IP identifies an application on one computer and then moves the data from that application to an application on another computer.

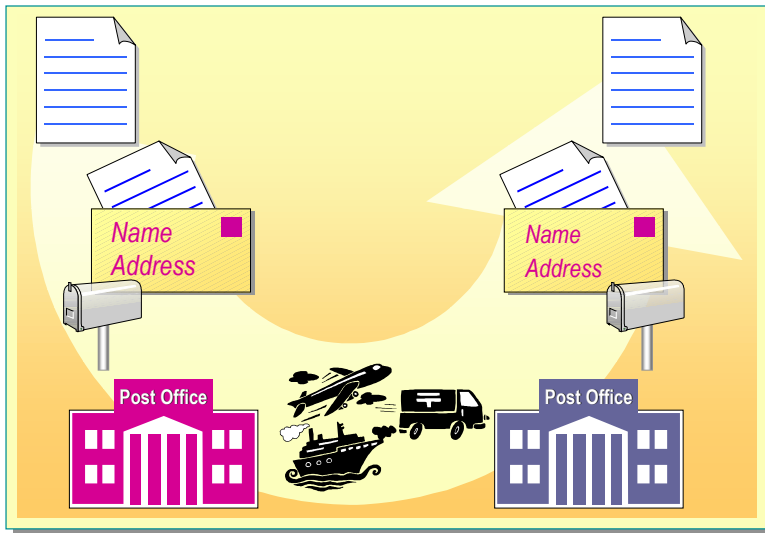
The Communication Process

Topic Objective

To illustrate the TCP/IP communication process.

Lead-in

TCP/IP enables connectivity on Windows 2000-based computers by using a communication model.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Explain how communication that uses TCP/IP relates to a common concept, such as the process of sending a letter. Use the animated slides to show the students that the process is parallel at each computer.

The process by which TCP/IP transmits data between two locations is analogous to the procedure used to send a letter from one city to another by postal mail.

TCP/IP Activities

The TCP/IP communication process is initiated using an application on the source computer that prepares the data to be transmitted in a format that an application on the destination computer can read. This is similar to writing a letter in a language that the recipient can understand. Then the data is associated with the destination application and computer, much like how you address a letter to a recipient and household. The address of the destination computer is then added to the data, just as the address of the recipient is specified on the letter.

After these activities are performed, the data and additional information, including a request for confirmation of its delivery, are sent over the network to the destination. The network medium used for transmitting the data is independent of the above activities, just as the means of transport that transfers the letter from one post office to another is independent of the letter's content or address.

TCP/IP Protocols and Layers

TCP/IP organizes the communication process outlined here by assigning these activities to various protocols in the TCP/IP stack. To increase the efficiency of the communication process, the protocols are arranged in layers. The addressing information is placed last, so that the computers on a network can quickly check whether the data is meant for them. Only the computer that is the destination computer opens and processes all of the data.

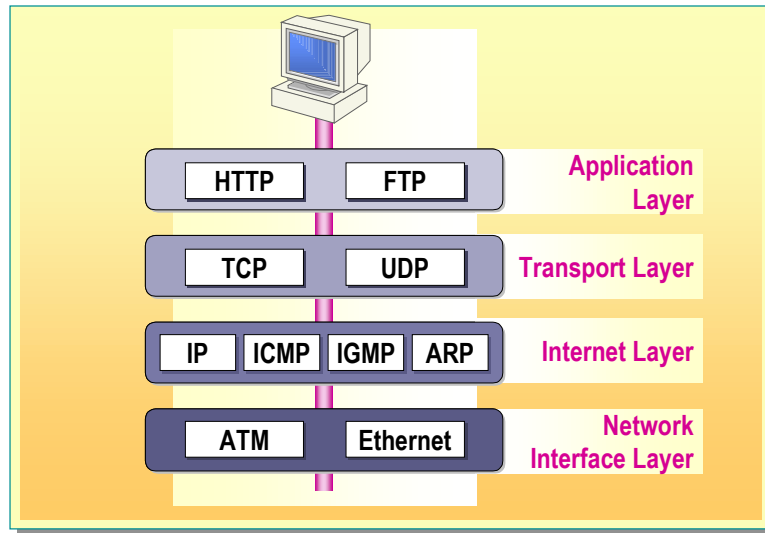
TCP/IP Layers

Topic Objective

To illustrate the TCP/IP layers.

Lead-in

TCP/IP uses a four-layer communication model.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Explain that the four layers of the TCP/IP protocol stack are a specific implementation of the seven layers of the OSI model. Relate the information in this module to the content on protocol stacks in module 5, "Examining Network Protocols," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*. Do not spend a large amount of time on the specific protocols, as these are discussed later. Instead, use this page to point out the division of tasks.

TCP/IP uses a four-layer communication model to transmit data from one location to another. The four layers in this model are application, transport, Internet, and network interface. All protocols that belong to the TCP/IP protocol stack are located in these layers of the model.

Application Layer

The application layer is the topmost layer in the TCP/IP stack. All applications and utilities are contained in this layer and use this layer to gain access to the network. The protocols in this layer are used for the formatting and exchange of user information. They include:

- Hypertext Transfer Protocol (HTTP)
HTTP is used to transfer files that make up the Web pages of the World Wide Web.
- File Transfer Protocol (FTP)
FTP is used for interactive file transfer.

Transport Layer

The transport layer provides the ability to order and guarantee communication between computers and passes the data up to the application layer or down to the Internet layer. The transport layer also specifies the unique identifier of the application to which data is to be delivered.

The transport layer has two core protocols that control the method by which data is delivered. They are:

- Transmission Control Protocol (TCP)
TCP guarantees the delivery of data through an acknowledgement.
- User Datagram Protocol (UDP)
UDP provides fast delivery of data but does not guarantee data delivery.

Internet Layer

The Internet layer is responsible for addressing, packaging, and routing the data that is to be transmitted. This layer contains four core protocols:

- Internet Protocol (IP)
IP is responsible for addressing the data to be transmitted and getting it to its destination.
- Address Resolution Protocol (ARP)
ARP is responsible for identifying the media access control (MAC) address of the network adapter on the destination computer.
- Internet Control Message Protocol (ICMP)
ICMP is responsible for providing diagnostic functions and reporting errors due to unsuccessful delivery of data.
- Internet Group Management Protocol (IGMP)
IGMP is responsible for the management of multicasting within TCP/IP.

Network Interface Layer

The network interface layer is responsible for placing data on the network medium and receiving data off the network medium. This layer contains such physical devices as network cables and network adapters. The network adapter has a unique 12-character hexadecimal number, such as B5-50-04-22-D4-65, which is known as the media access control (MAC) address. The network interface layer does not contain the type of software-based protocols that are included in the other three layers, but it does contain such protocols as Ethernet and asynchronous transfer mode (ATM), which define how data is transmitted on the network.

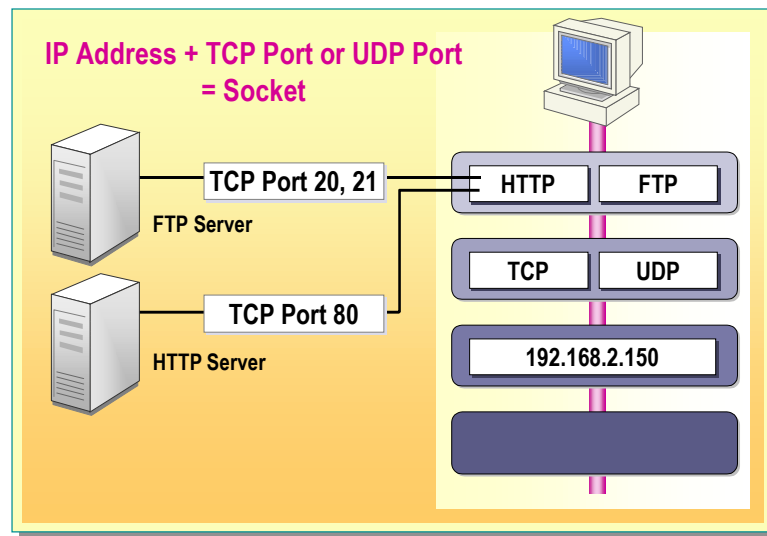
Identifying Applications

Topic Objective

To explain the role of sockets and ports in network communication.

Lead-in

How do multiple applications communicate simultaneously in a network?



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use this page to inform the students that they must identify both the computer to which they are sending the data as well as the specific application on that computer.

In a network, many applications are in communication at the same time. When multiple applications are active on a single computer, TCP/IP requires a method for differentiating one application from another. For this purpose, TCP/IP uses a socket, also known as an end point in network communication, to identify a specific application.

IP Address

To start a network communication, the location of the source and destination computers in the network must be known. The location is identified by a unique number, known as an IP address, which is assigned to each computer on the network. An example of an IP address is 192.168.2.200.

TCP/UDP Port

A *port* is an identifier for an application within a computer. A port is associated with either TCP or UDP transport layer protocols and is referred to as a TCP port or UDP port. A port can be any number between 0 and 65,535. Ports for common server-side TCP/IP applications, referred to as well-known port numbers, are reserved to numbers below 1,024 in order to avoid confusion with other applications. For example, the FTP Server application uses the TCP port numbers 20 and 21.

Socket

A *socket* is the combination of an IP address and the TCP port or UDP port. An application creates a socket by specifying the IP address of the computer, the type of service (TCP for guarantee of data delivery, otherwise UDP), and the port that the application monitors. The IP address component of the socket helps to identify and locate the destination computer, and the port determines the specific application to which the data is to be sent.

◆ TCP/IP Protocol Suite

Topic Objective

To introduce the core protocols in the Microsoft TCP/IP protocol suite.

Lead-in

The TCP/IP protocol suite consists of six core protocols and a set of utilities.

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Address Resolution Protocol (ARP)
- TCP/IP Utilities

*****ILLEGAL FOR NON-TRAINER USE*****

The Microsoft TCP/IP protocol *suite* enables enterprise networking and connectivity on Windows 2000-based computers. A suite is created by a vendor or organization to customize a protocol stack for its requirements. Therefore, a protocol suite is a set of protocols designed and built as complementary parts of a complete, smoothly functioning set.

The TCP/IP protocol suite includes six core protocols and a set of utilities. The six core protocols—TCP, UDP, IP, ICMP, IGMP, and ARP—provide a set of standards for communications between computers and for connections between networks. All applications and other protocols in the TCP/IP protocol suite rely on the basic services provided by these core protocols.

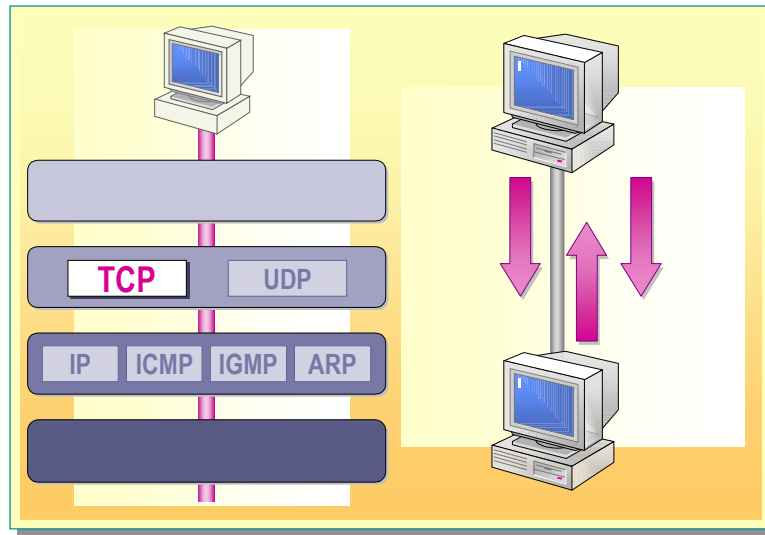
Transmission Control Protocol (TCP)

Topic Objective

To describe the features of TCP.

Lead-in

TCP is one of the two core protocols in the transport layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the slide to illustrate the three-way handshake process that initiates a TCP session. Also emphasize the unicast nature of TCP. You can mention that a credit card transaction is an example of how TCP is used.

Transmission Control Protocol (TCP) is a required TCP/IP standard protocol that provides a reliable, connection-oriented data delivery service between only two computers. Such a communication is known as a unicast. In connection-oriented communication, the connection must be established before data can be transmitted between the two computers.

After the connection is established, data is transmitted over this single connection only. Connection-oriented communication is also referred to as reliable communication because it guarantees the delivery of the data at the destination.

On the source computer, TCP organizes the data to be transmitted into packets. On the destination computer, TCP reorganizes the packets to recreate the original data.

Data Transmission Using TCP

TCP transmits packets in groups to increase efficiency. It assigns a sequence number to each packet and uses an acknowledgment to verify that the destination computer has received a group of packets. If the destination computer does not return an acknowledgment for each group of packets sent within a specified period of time, the source computer retransmits the data.

In addition to adding the sequencing and acknowledgement information to the packet, TCP also adds the port information for both the source and the destination applications. The source computer uses the destination port to direct the packet to the proper application at the destination computer, and the destination computer uses the source port to return information to the correct source application.

Three-Way Handshake

Because TCP is a reliable protocol, two computers using TCP for communication must establish a connection before exchanging data. This connection is a virtual connection and is known as a *session*. Two computers using TCP establish a connection, or TCP session, through a process known as a three-way handshake. This process synchronizes sequence numbers and provides other information needed to establish the session.

The three-way handshake is a three-step process:

1. The source computer initiates the connection by transmitting the session information, including the sequence number and size of the packet.
2. The destination computer responds with its session information.
3. The source computer agrees with and acknowledges the received information.

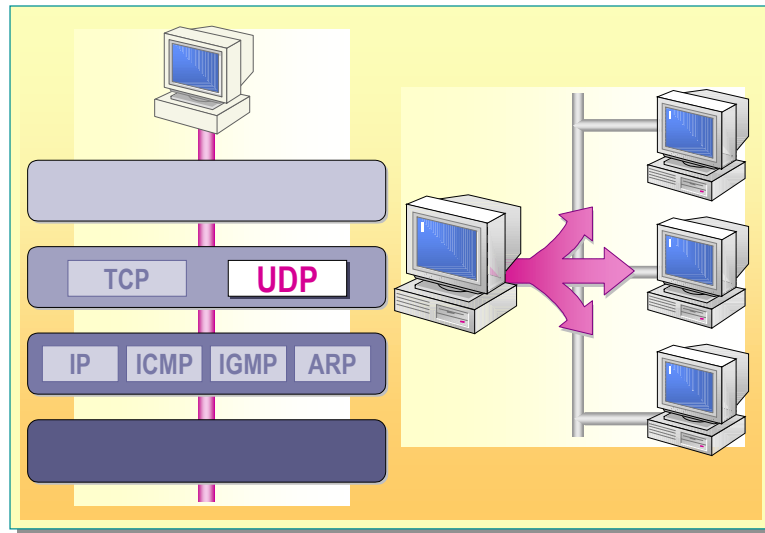
User Datagram Protocol (UDP)

Topic Objective

To describe the features of UDP.

Lead-in

Along with TCP, UDP is another core protocol in the transport layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Although UDP is capable of unicast transmissions, use the slide to emphasize its broadcast or multicast nature as well. Be sure to contrast it with TCP. Additional examples could include information about the need to communicate with more than one computer at a time or about small pieces of data that would not benefit from the overhead of TCP.

User Datagram Protocol (UDP) is a transport layer protocol that identifies the destination application in network communications. UDP provides a connectionless packet delivery service that offers fast but unreliable, best-effort delivery of the data. UDP does not require an acknowledgment for the data received and does not attempt to retransmit data that is lost or corrupted. This means that less data is sent, but neither the arrival of packets nor the correct sequencing of delivered packets is acknowledged or guaranteed.

UDP is used by applications that transmit data to multiple computers by using broadcast or multicast transmissions. It is also used for transmitting small amounts of data or data that is not of high importance. Example uses of UDP include multicasting streaming media, such as during a live videoconference, and broadcasting a list of computer names, which are maintained for local communication.

To use UDP, the source application must supply its UDP port number as well as that of the destination application. It is important to note that UDP ports are distinct and separate from TCP ports, even though some of them use the same numbers.

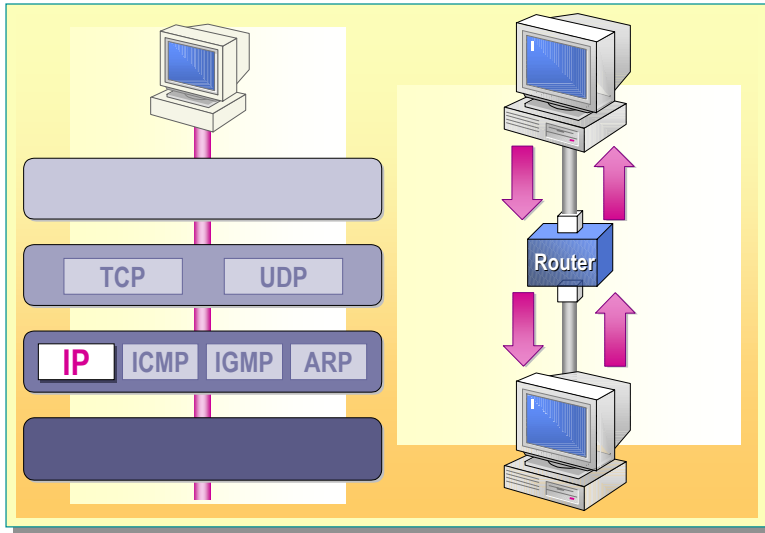
Internet Protocol (IP)

Topic Objective

To describe the features of IP.

Lead-in

IP is one of the three core protocols of the Internet layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the slide to illustrate the importance of IP in moving data across routers. Remind students that although the network adapters use the MAC address to identify a computer on the local segment, it is IP that moves the data to the local segment.

Internet Protocol (IP) helps to identify the location of the destination computer in a network communication. IP is a connectionless, unreliable protocol that is primarily responsible for addressing packets and routing them between networked computers. Although IP always attempts to deliver a packet, a packet may be lost, corrupted, delivered out of sequence, duplicated, or delayed. However, IP does not attempt to recover from these types of errors by requesting retransmission of the data. Acknowledging the delivery of packets and recovering lost packets is the responsibility of a higher-layer protocol, such as TCP, or of the application itself.

Activities Performed by IP

You can visualize IP as the mailroom of the TCP/IP stack, where packet sorting and delivery take place. The packets are passed down to IP by UDP or TCP from the transport layer or passed up from the network interface layer. The primary function of IP is to route the packets until they reach their destination.

Each packet includes the source IP address of the sender and the destination IP address of the intended recipient. These IP addresses in a packet remain the same throughout the packet's journey across a network.

If IP identifies a destination address as an address from the same segment, it transmits the packet directly to that computer. If the destination IP address is not on the same segment, IP must use a router to send the information.

IP is also responsible for ensuring that a packet does not remain on the network forever by limiting the number of networks across which the packet can travel. This is done by assigning a Time to Live (TTL) number to every packet. A TTL specifies the maximum length of time that the packet can travel on the network before being discarded.

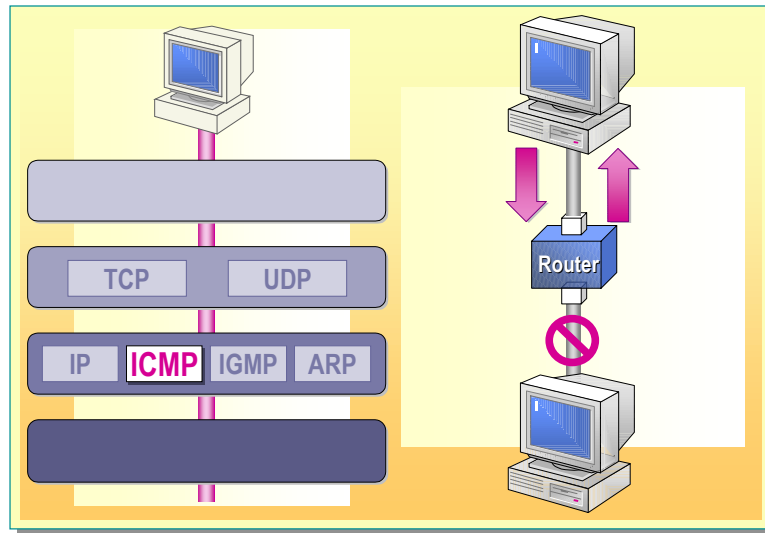
Internet Control Message Protocol (ICMP)

Topic Objective

To describe the features of ICMP.

Lead-in

ICMP is another core protocol in the IP layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Remind the students that unreliable (not guaranteed) delivery is not bad; it is just not needed in many cases. And the overhead involved to send a simple error message across the network is unnecessary. However, when a packet must reach a specific destination, TCP is used. The above graphic provides an example of an ICMP message being returned.

Internet Control Message Protocol (ICMP) provides troubleshooting facilities and error reporting for undeliverable packets. With ICMP, computers and routers that use IP communication can report errors and exchange limited control and status information. For example, if IP is unable to deliver a packet to a destination computer, ICMP sends a Destination Unreachable message to the source computer.

Although the IP protocol is used to move data across routers, ICMP reports errors and control messages on behalf of IP. ICMP does not attempt to make IP a reliable protocol, because ICMP messages are unacknowledged and therefore unreliable. It only attempts to report errors and provide feedback on specific conditions. Although this may not seem effective, it is much more efficient than using bandwidth to acknowledge each ICMP message.

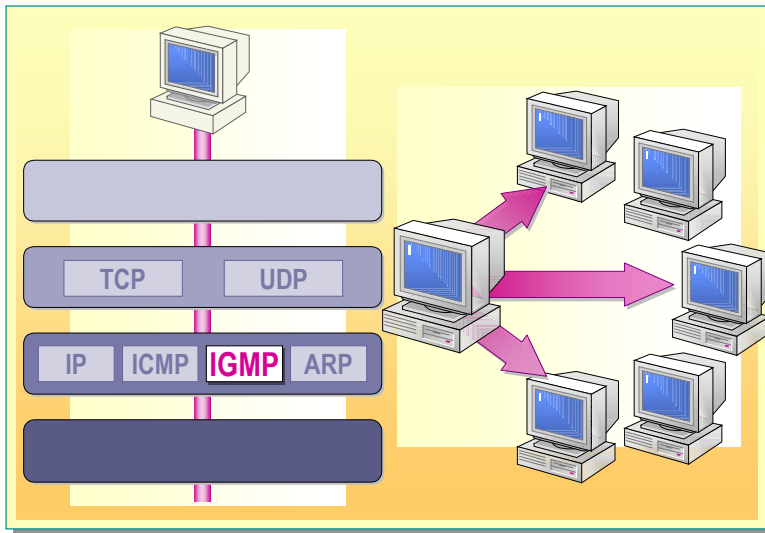
Internet Group Management Protocol (IGMP)

Topic Objective

To describe the features of IGMP.

Lead-in

IGMP is also one of the core protocols in the Internet layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Make sure that the students are not confused by the similarity between IGMP and ICMP. A good way to ensure this is to remind the students that G = group with IGMP.

Internet Group Management Protocol (IGMP) is a protocol that manages the membership lists for IP multicasting in a TCP/IP network. IP multicasting is a process by which a message is transmitted to a select group of recipients, known as a multicast group. IGMP maintains the list of members who subscribe to each multicast group.

Managing IP Multicasting

All of the members of a multicast group listen for IP traffic directed to a specific multicast IP address and receive the packets sent to that IP address. However, because multicasting involves multiple computers, the packets are sent using the unreliable UDP protocol, which does not guarantee the delivery of the packets to the multicast group.

When multiple computers need to access information, such as streaming media, an IP address reserved for multicasting is used. Routers that are configured to process multicast IP addresses pick up this information and forward it to all subscribers of the multicast group associated with the multicast IP address.

For multicast information to reach its recipients, it is important that each router in the path of communication supports multicasting. Windows 2000-based computers can both send and receive IP multicast traffic.

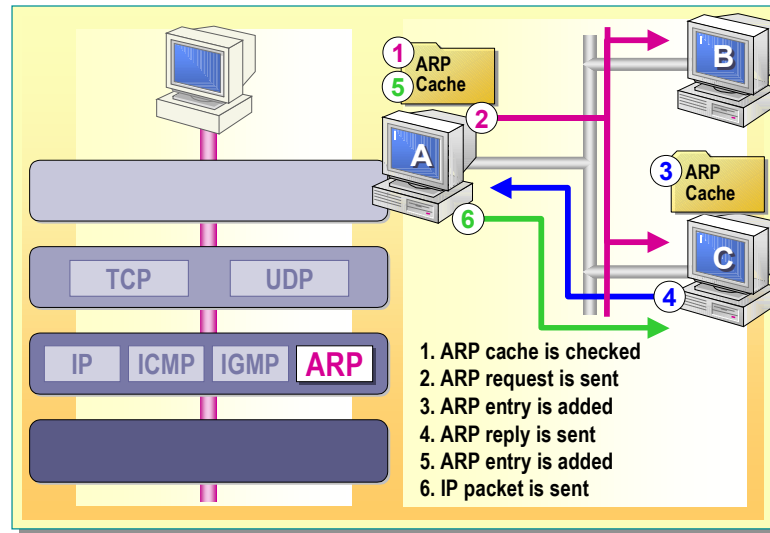
Address Resolution Protocol (ARP)

Topic Objective

To describe the features of ARP.

Lead-in

ARP is another of the three core protocols in the Internet layer.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Point out to the students that ARP can occur only between computers on the same network segment and that a router is needed if the destination computer is remote.

Delivery Tip

Test the students' understanding by asking questions about broadcast messages and whether they are routable.

Located in the Internet layer of the TCP/IP suite, Address Resolution Protocol (ARP) performs address resolution for outgoing packets. Address resolution is the process by which IP addresses are mapped to MAC addresses. The network adapters use the MAC address to determine if a packet is meant for that computer.

Without the MAC address, the network adapters do not know if they are to pass the data to a higher layer for further processing. As the outgoing packets in the IP layer are being readied for transmission on the network, the source and destination MAC addresses must be added.

ARP Cache

ARP stores a table containing IP addresses and their corresponding MAC addresses. The area of memory where this table is stored is referred to as the ARP cache. The ARP cache for any computer contains the mappings for only computers and routers that reside on the same segment.

Physical Address Resolution

ARP compares every outbound packet's destination IP address with the ARP cache to determine the MAC address to which the packet will be sent. If there is a matching entry, the MAC address is retrieved from the cache. If not, ARP broadcasts a request for the computer owning the IP address in question to reply with its MAC address. Next, the computer with the corresponding IP address adds the initial computer's MAC address to its cache and then replies with its own MAC address. When an ARP reply is received, the ARP cache is updated with the new information and the packet can then be sent.

If the packet is going to another segment, ARP resolves the MAC address for the router responsible for that segment, rather than resolving the address for the final destination computer. The router is then responsible for either finding the MAC address of the destination or forwarding the packet to another router.

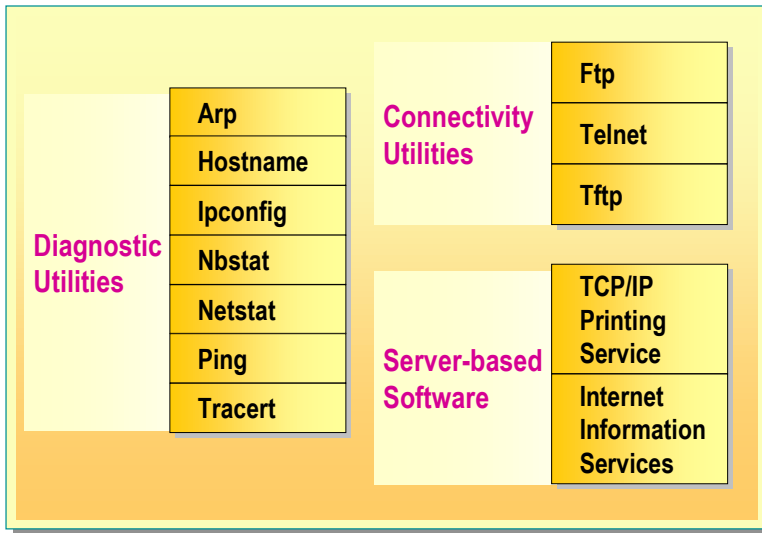
TCP/IP Utilities

Topic Objective

To introduce the types of TCP/IP utilities.

Lead-in

The TCP/IP protocol suite consists of a number of utilities that allow users to access information on the network.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This is not an inclusive list of utilities. It only illustrates the various types of utilities that are included with the TCP/IP suite. Remind the students that these utilities are all found on the application layer. Demonstrate the Hostname, Arp, and Ping utilities. Point out that Arp is both a utility and a protocol (ARP). Also point out that Ping uses another protocol, ICMP, to accomplish its work. Note that Ipconfig is discussed in module 7, "Examining IP Addressing," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials* and the above utilities are used in the following lab.

The Microsoft TCP/IP suite provides basic TCP/IP utilities that enable a computer running Windows 2000 to access a wide variety of information on the network. Their capabilities range from determining if a specific computer on the network is accessible to downloading multimedia documents from the Internet.

Windows 2000 includes three types of TCP/IP-based utilities: diagnostic utilities, connectivity utilities, and server-based software.

Diagnostic Utilities

Diagnostic utilities allow users to detect and resolve networking problems. Some of the common diagnostic utilities are:

- **Arp:** This utility displays and modifies the Address Resolution Protocol (ARP) cache.
- **Hostname:** This utility displays the host name of your computer.
- **Ipconfig:** This utility displays and updates the current TCP/IP configuration, including the IP address.
- **Nbstat:** This utility displays the local NetBIOS name table, which is a table of user-friendly computer names mapped to IP addresses.
- **Netstat:** This utility displays the TCP/IP protocol session information.
- **Ping:** This utility verifies configurations and tests IP connectivity between two computers. Ping sends an ICMP request from the source computer, and the destination computer responds with an ICMP reply.
- **Tracert:** This utility traces the route that a packet takes to a destination.

Connectivity Utilities

Connectivity utilities allow users to interact with and use resources on a variety of Microsoft and non-Microsoft hosts, such as UNIX systems. Some of the common connectivity utilities are:

- **Ftp:** This utility uses TCP to transfer files between Windows 2000 and computers running File Transfer Protocol (FTP) server software.
- **Telnet:** This utility remotely accesses network resources on computers running Telnet server software.
- **Tftp:** This utility uses UDP to transfer small files between Windows 2000 and computers running Trivial File Transfer Protocol (TFTP) server software.

Server-based Software

This software provides printing and publishing services to TCP/IP-based clients on Windows 2000.

- **TCP/IP Printing service:** This utility provides standard TCP/IP printing services. It allows computers running operating systems other than Windows 2000 to print to a printer attached to a Windows 2000-based computer.
- **Internet Information Services:** Internet Information Services (IIS) offers Web, news, e-mail, and file transfer server software for TCP/IP-based publishing services.

Examples of Common Utilities

Hostname, Arp, and Ping are three common TCP/IP utilities. Because they are frequently used, it is recommended that you know how to access them.

Hostname

The syntax to use this utility is *hostname*. To access this utility, type **hostname** at the command prompt. The system displays the host name of your computer.

Arp

The syntax to access information from the ARP cache is *arp -a*. Type **arp -a** at the command prompt to display the information in your ARP cache.

Ping

The syntax to test connectivity is *ping*. To test connectivity by using an IP address or computer name, type **ping** [*IP_address* or *computer_name*]

To test the TCP/IP configuration of your own computer, you use *local loopback*. Local loopback is the IP address 127.0.0.1. To test system configuration by using local loopback, type **ping 127.0.0.1**

Lab A: Using TCP/IP Utilities

Topic Objective

To introduce the lab.

Lead-in

In this lab, you use the Ping utility to test the TCP/IP configuration of your computer. You will also use Ping to test connectivity with other computers, the Hostname utility to identify your computer, and the Arp utility to identify your MAC address.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Use the Ping utility to test configuration and connectivity.
- Use the Hostname utility to obtain your computer name.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how to log on to Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Using TCP/IP Utilities

Scenario

You are an administrator of a small company and want to ensure that your server is properly configured with TCP/IP and to test that it can communicate with other computers on the network.

Goal

In this exercise, you will use the Ping utility to verify TCP/IP configuration and then use the Hostname utility to identify your computer name. You will then use Ping to test connectivity with your partner to ensure that you can communicate on the network.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password . Use the Hostname utility to verify your computer's host name and Ping to test the TCP/IP configuration.	- Log on to Windows 2000 as Administrator with a password of password. - Click Start, point to Programs, point to Accessories, and then click Command Prompt. - Type PING 127.0.0.1 in the Command Prompt window.
 How many packets were sent, received, and lost? Four packets were sent, four packets were received, and no packets were lost, unless there is a problem with your TCP/IP installation.	
 Is TCP/IP functioning properly? Yes, if all four packets were received.	

Tasks	Detailed Steps
2. Use the Hostname utility to obtain your host name, and then use the Ping utility with your host name to return your IP address.	a. In the Command Prompt window, type hostname b. In the Command Prompt window, type ping computer (where <i>computer</i> is the host name that was returned in step a).
 What is your computer's host name? Answers will vary; for the Instructor, it will be London.	
 What is your computer's IP address? 192.168.x.y (where x is the room number and y is between 1 and 199).	
3. Use the Ping utility with the instructor's computer name to verify that your computer can communicate on the network.	a. In the Command Prompt window, type ping London
 What is London's IP address? 192.168.1.200.	
 How do you know that you are able to communicate with London? Because no packets were lost.	
4. Close all windows and log off from Windows 2000.	b. Close all windows and log off from Windows 2000.

◆ Name Resolution

Topic Objective

To introduce the factors involved in name resolution.

Lead-in

All user-friendly names need to be mapped to their IP addresses to provide for communication.

- Types of Names
- Static IP Mapping
- Dynamic IP Mapping
- Name Resolution in Windows 2000

*****ILLEGAL FOR NON-TRAINER USE*****

TCP/IP identifies source and destination computers by their IP addresses. However, users are much better at remembering and using words (user-friendly names) than numbers (IP addresses). There are different types of user-friendly names by which a computer can be addressed.

The Windows 2000 operating system has different storage locations where it keeps a record of user-friendly names mapped to their corresponding IP addresses. This mapping of the IP address of a computer can be stored in either a static or a dynamic file, based on the type of name used.

Some applications, such as Microsoft Internet Explorer and the Ftp utility, can use either the IP address or a user-friendly name to establish communication. When a user-friendly name is specified, a Windows 2000-based computer uses a process called name resolution to identify the appropriate IP address before TCP/IP-based communication with the desired resource can begin. However, if the IP address is specified, communication can happen immediately.

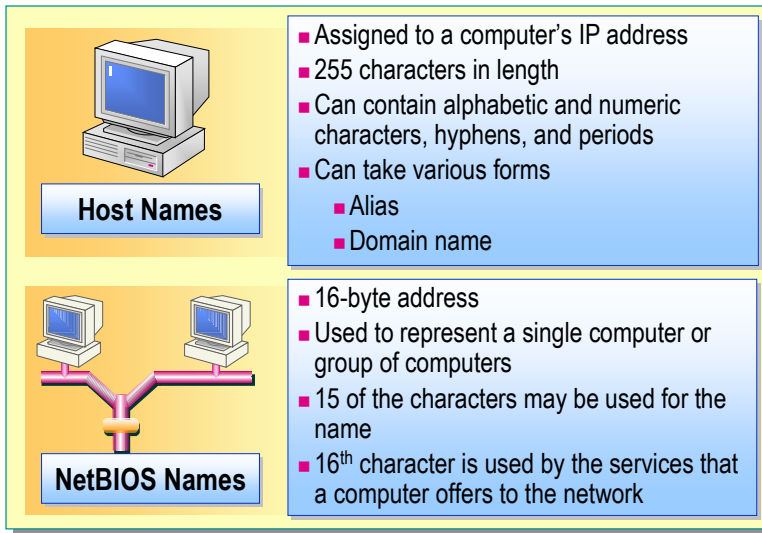
Types of Names

Topic Objective

To describe the characteristics of the two types of user-friendly names.

Lead-in

There are two types of popular user-friendly names.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Ask students what NetBIOS means. Use the definition of NetBIOS when explaining a NetBIOS name. Tell the students that some applications, including NetBIOS resources, identify themselves by using a NetBIOS name instead of the more common host name. Host names are used in such products as browsers and are standard in Windows 2000.

There are two types of user-friendly names: host names and NetBIOS names.

Host Names

A host name is a user-friendly name that is assigned to a computer's IP address to identify it as a TCP/IP host. The host name can be up to 255 characters in length and can contain alphabetic and numeric characters, hyphens, and periods.

Host names can take various forms. The two most common forms are alias and domain name. An alias is a single name associated with an IP address, such as London. A domain name is structured for use on the Internet and includes periods as separators. An example of a domain name is london.nwtraders.msft.

NetBIOS Names

A NetBIOS name is a 16-character name that is used to identify a NetBIOS resource on the network. A NetBIOS name can represent a single computer or a group of computers, but only the first 15 of the characters may be used for the name. The final character is used to identify the resource or service that is being referred to on the computer.

An example of a NetBIOS resource is the File and Printer Sharing for Microsoft Networks component on a computer running Windows 2000. When your computer starts, this component registers a unique NetBIOS name, based on the name of your computer and one character identifier that represents the component.

Important In Windows 2000, the NetBIOS name uses up to the first 15 characters of the host name and cannot be configured separately. Although Windows 2000 does not require NetBIOS names, previous versions of Windows require NetBIOS names to support networking capabilities.

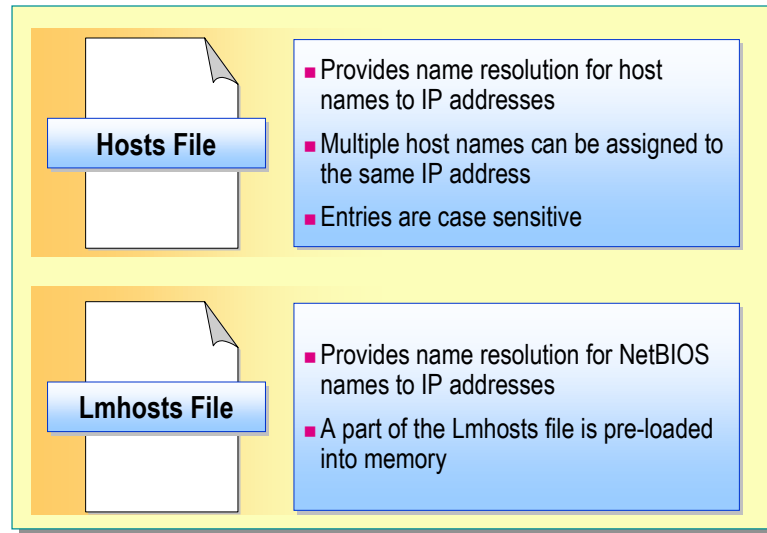
Static IP Mapping

Topic Objective

To describe the components of the static IP mapping method.

Lead-in

Static IP mapping is a method to store information about user-friendly names and their corresponding IP addresses.



*****ILLEGAL FOR NON-TRAINER USE*****

When users specify a user-friendly name to communicate with a destination computer, TCP/IP still requires an IP address for transmission to occur, so the computer name is mapped to an IP address. This mapping is then stored in either a static or dynamic table. In a static table, mappings are stored in one of two text files: the Hosts file or the Lmhosts file.

The advantage of using a static table is that, because it is a text file located on each computer, it is customizable. Each user can create any number of required entries, including easy-to-remember aliases for frequently accessed resources. However, it is difficult to maintain and update static tables if the tables contain a large number of IP address mappings or if the IP addresses change often.

Hosts File

The Hosts file is a text file that contains IP address-to-host name mappings. Within the Hosts file:

- Multiple host names can be assigned to the same IP address. A server at the IP address 167.91.45.121 can be referred to by its domain name (london.nwtraders.msft) or by an alias (London). This allows a user at this computer to refer to this server by using the alias London rather than by typing the entire domain name.
- Entries are case-sensitive, depending upon the platform. Hosts file entries for computers running Windows 2000 and Microsoft Windows NT® version 4.0 are not case-sensitive.

Lmhosts File

The Lmhosts file is a text file that contains the IP address-to-NetBIOS name mappings. A portion of the Lmhosts file is pre-loaded into memory and is referred to as the NetBIOS name cache.

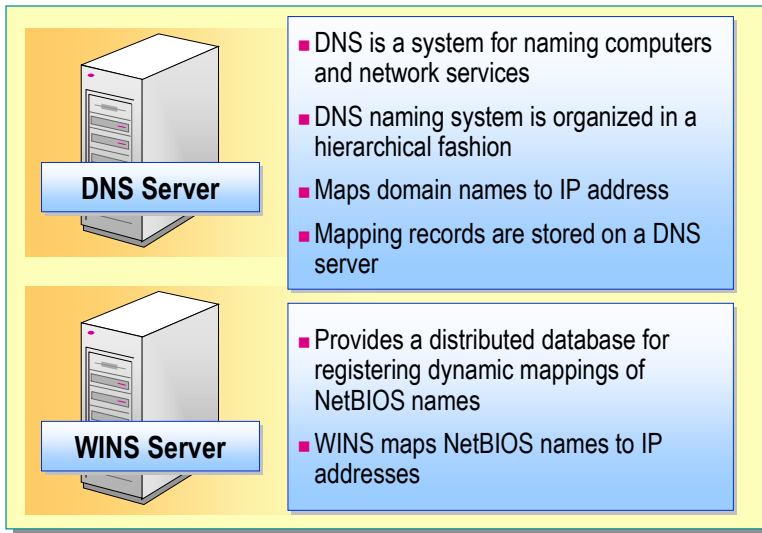
Dynamic IP Mapping

Topic Objective

To describe the features of dynamic routing.

Lead-in

Manually updating mapping entries is not efficient.



*****ILLEGAL FOR NON-TRAINER USE*****

The advantage of dynamic tables that store IP mappings is that they are updated automatically. To accomplish this, the dynamic tables use two services: Domain Name System (DNS) and Windows Internet Name Service (WINS). DNS and WINS perform the same functions as the Hosts and Lmhosts files, but without the need for manual configuration.

Domain Name System (DNS)

DNS is a method for naming computers and network services. TCP/IP networks use the DNS naming convention to locate computers and services through user-friendly domain names. When a user enters a domain name in an application, the DNS service maps the name to an IP address.

The DNS naming system is organized in a hierarchical fashion to allow scalability to large systems, such as the Internet. By using a hierarchical system to create domain names, the computers that store the domain name-to-IP address mapping records have mappings for only their area. These computers, known as DNS servers, only process queries for computers located in their respective areas. As the mappings in the area change, Windows 2000-based DNS servers are automatically updated with the new information.

Windows Internet Name Service (WINS)

WINS provides a distributed database for registering dynamic mappings of NetBIOS names used on a network. WINS maps NetBIOS names to IP addresses and allows NetBIOS names to be used across routers.

Note A WINS server is not required for a pure Windows 2000 network but is recommended for use in a mixed environment.

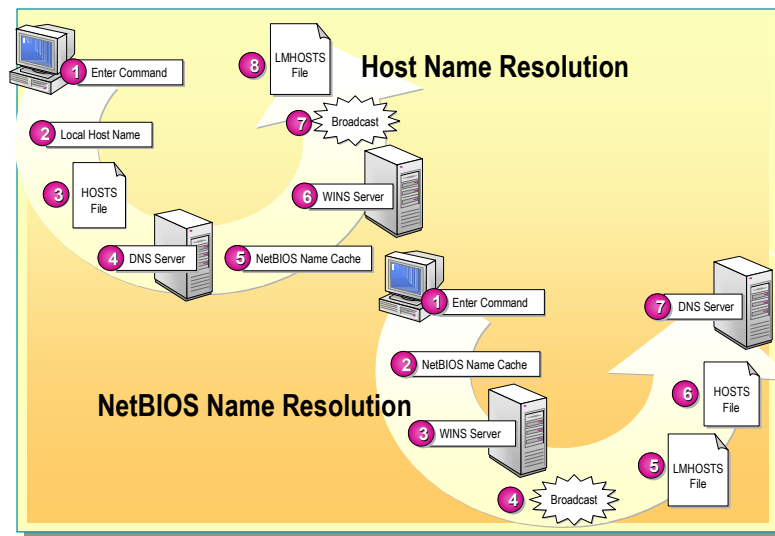
Name Resolution in Windows 2000

Topic Objective

To illustrate the name resolution process.

Lead-in

Windows 2000 resolves both host names and NetBIOS names.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Windows 2000 applications are designed to use host names, but both NetBIOS and host names can be resolved using either process if configured properly. It is the order of resolution and the time to resolve that differs.

Name resolution is the procedure by which a name is resolved, or mapped, to an IP address. When you enter a user-friendly name in an application, the application determines whether the name is a host or NetBIOS name. Current applications in Windows 2000 use the host name resolution process, but some older applications, such as those designed for Microsoft Windows NT, Windows 95, and Windows 98, still use NetBIOS names. If the name resolution process fails, then the application cannot communicate with the desired destination. If you use an IP address, name resolution is not needed.

Host Name Resolution Process

Host names can be resolved directly by the Hosts file or by a DNS server. The default name resolution procedure is as follows:

1. Computer A enters a command, such as **FTP**, by using the host name of Computer B.
2. Computer A checks to see if the specified name matches its local host name.
3. If not, then Computer A checks its Hosts file looking for Computer B's host name. If it finds the host name, it resolves it to an IP address.
4. If Computer A does not find Computer B's host name in the Hosts file, it sends a query to the DNS server. If the host name is found, it is resolved to an IP address.

5. If the host name is not found on the DNS server, Windows 2000 checks for the name in the NetBIOS name cache. It does this because Windows 2000 treats the NetBIOS name as the host name.
6. If the NetBIOS name cache does not have the host (NetBIOS) name, a query is sent to the WINS server.
7. If the WINS server cannot resolve the name, a broadcast message is sent out on the network.
8. If no host responds to the broadcast, the Lmhosts file is checked for the host (NetBIOS) name.

NetBIOS Name Resolution Process

By default, NetBIOS names do not function over a TCP/IP network. Windows 2000 enables NetBIOS clients to communicate over TCP/IP by providing the NetBT protocol. NetBT is an acronym for NetBIOS over TCP/IP. This protocol allows NetBIOS-based applications to communicate using TCP/IP by translating the NetBIOS name to an IP address. If WINS is configured for use, then the procedure for resolving NetBIOS names is as follows:

1. Computer A enters a command, such as **net use**, by using the NetBIOS name of Computer B.
2. Computer A checks to see if the specified name is in its NetBIOS name cache.
3. If not, then Computer A queries a WINS server.
4. If the WINS server cannot locate the name, then Computer A uses a broadcast on the network.
5. If a broadcast does not resolve the name, then Computer A checks its Lmhosts file.
6. If the above NetBIOS methods do not resolve the name, then Computer A checks the Hosts file.
7. Finally, Computer A queries a DNS server.

Caution The order in which Windows 2000 uses these mechanisms depends on how the Windows 2000-based computer is configured.

◆ Examining the Data Transfer Process

Topic Objective

To introduce the role of packets in data transfer.

Lead-in

Data transfer is a complex process that involves many activities.

- Packet Terminology
- Frame Components
- Data Flow

*****ILLEGAL FOR NON-TRAINER USE*****

TCP/IP transmits data on the network by dividing it into smaller portions called packets. Packets are often referred to by different terms based on the protocol with which they are associated. The division of data into packets is necessary because a large unit of data takes a long time to move on the network and can clog the network. While the large unit is being transmitted, no other computer can transmit data. Also, if an error occurs, the entire unit of data must be retransmitted.

In contrast, if small packets are sent on the network, they move quickly. Because small packets don't clog the network, other computers can also transmit data. If any packet becomes corrupted, only the corrupted packet needs to be retransmitted, instead of the entire data.

When a packet is transmitted in the network interface layer, it is referred to as a frame. A frame consists of different components that have specific functions in the flow of data in the network interface layer.

The data flow process involves a number of steps, including the organization of data into small packets at the source computer and their reassembly in the original form at the destination computer. Each layer of the TCP/IP protocol stack is involved in these activities at both the source and destination computers.

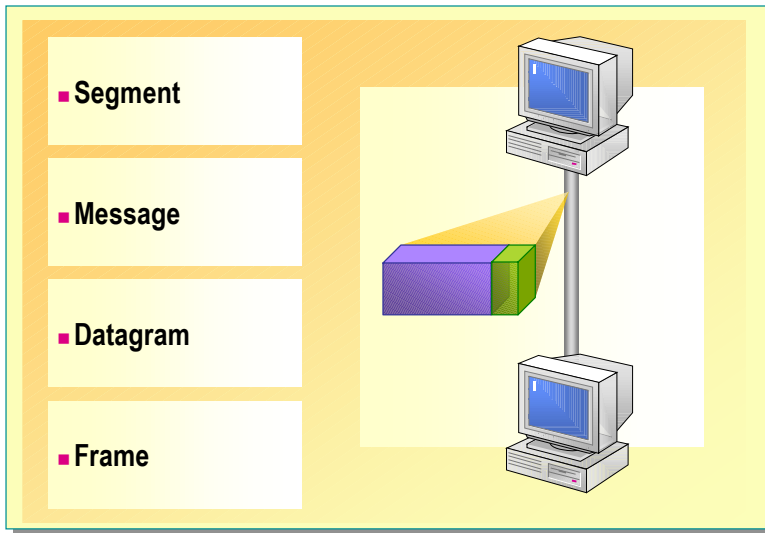
Packet Terminology

Topic Objective

To introduce terminology frequently associated with packets.

Lead-in

At each layer of the TCP/IP stack, the packet is referred to by a different name.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This page should be used to clarify the fact there is more than one term associated with a packet of data. Remind students of the meaning of segment as it applies to the network.

As a packet of data moves from one layer to another in the TCP/IP stack, each protocol adds its own header information. The packet, along with the information added to it, is referred to by a different technical name as it is identified with different protocols. These names are segment, message, datagram, and frame.

Segment

A segment is the unit of transmission in TCP. It contains a TCP header, accompanied by application data.

Message

A message is the unit of transmission in unreliable protocols, such as ICMP, UDP, IGMP, and ARP. It consists of a protocol header, accompanied by application or protocol data.

Datagram

A datagram is the unit of transmission in IP. It consists of an IP header, accompanied by transport layer data, and is also considered unreliable.

Frame

A frame is the unit of transmission in the network interface layer and consists of a header added at the network interface layer, accompanied by IP layer data.

Note As the name for UDP (user datagram protocol) suggests, it can also be referred to as a datagram. However, UDP message is the generally accepted term. The term segment is applied when a physical device is used to divide a network. In the context of a packet, the term segment is often referred to as a TCP segment.

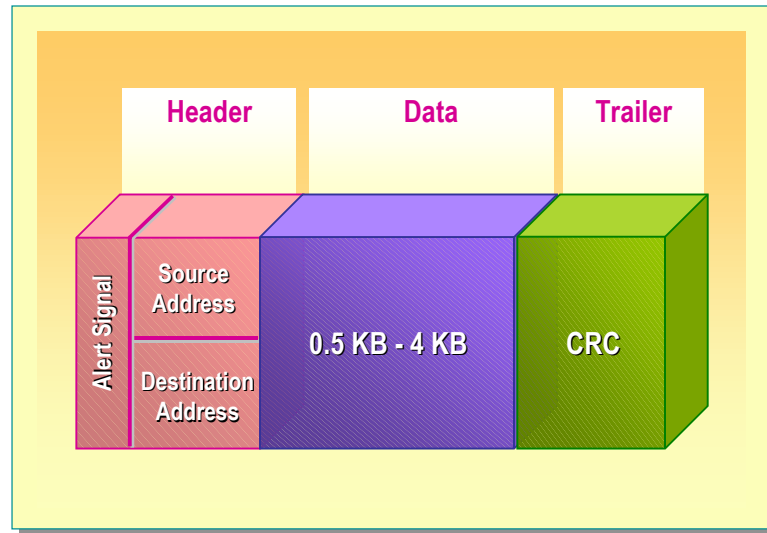
Frame Components

Topic Objective

To illustrate the three components of a data packet.

Lead-in

When data is broken up into packets, various types of information are added to it to enable it to reach its destination.



*****ILLEGAL FOR NON-TRAINER USE*****

A frame (the term for a data packet in the network interface layer) consists of three components: the header, the data, and the trailer.

Header

The header includes:

- An alert signal to indicate that the packet is being transmitted.
- The source address.
- The destination address.

Data

This is the actual information sent by the application. This component of the packet varies in size, depending on the size limits set by the network. The data section on most networks varies from 0.5 kilobytes (KB) to 4 KB. With Ethernet, the size of the data is approximately 1.5 KB.

Because most original data strings are much longer than 4 KB, data must be broken into pieces small enough to be put into packets. It takes many packets to complete the transmission of a large file.

Trailer

The exact content of the trailer varies depending on the network interface layer *protocol*. However, the trailer usually contains an error-checking component called a *cyclical redundancy check (CRC)*. The CRC is a number produced by a mathematical calculation on the packet at its source. When the packet arrives at its destination, the calculation is made again. If the results of both calculations are the same, this indicates that the data in the packet has remained stable. If the calculation at the destination differs from the calculation at the source, this means that the data has changed during transmission. In that case, the source computer retransmits the data.

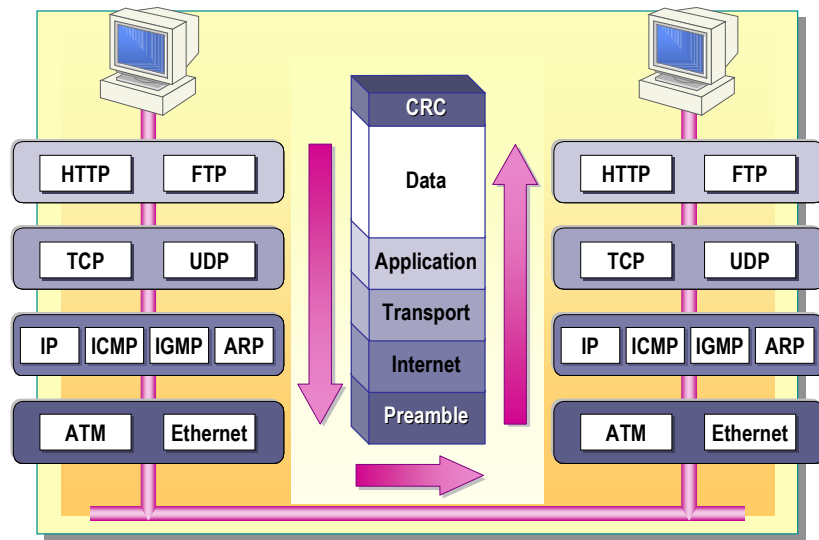
Data Flow

Topic Objective

To illustrate the process of data transfer.

Lead-in

Transferring packets from one computer to another involves the TCP/IP layers at both the source and destination computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide on this page furthers the analogy that was introduced in the first section. The students should now be familiar with the various tasks involved with TCP/IP, and this page integrates them by using a single segment approach. Also compare the CRC of the frame with the checksum added by the protocols at each layer. Remember that this is not a comprehensive list of items added by each protocol.

The packets of data being transmitted from one computer to another travel through the layers of the TCP/IP protocol stack. As the data packets pass through each layer, the protocols in that layer attach specific information to the header. The information added by every protocol includes error-checking information, known as the *checksum*. The checksum is used to verify whether the header information added by the protocol arrived intact at the destination protocol, compared with the CRC, which verifies the whole packet.

The information added by the protocols in one layer is encapsulated as data by the protocols in the layer below. When the packet is received at the destination, the corresponding layer strips off a header and treats the remaining packet as data. The packet is then passed up the protocol stack to the appropriate protocol.

Application Layer

The data transmission process begins at the application layer of the TCP/IP protocol stack. An application, such as the Ftp utility, initiates the process at the source computer by preparing the data in a format that the application at the destination computer recognizes. The application at the source computer controls the entire process.

Transport Layer

From the application layer, the data moves to the transport layer. This layer contains the TCP and UDP protocols. The application initiating the transmission request selects which protocol to use—TCP or UDP—and the checksum is added for both TCP and UDP.

If selected, TCP:

- Assigns a sequence number to each segment to be transmitted.
- Adds acknowledgement information for a connection-oriented transmission.
- Adds the TCP port number for the source and destination applications.

If selected, UDP:

- Adds the UDP port number for the source and destination applications.

Internet Layer

After the transport information is added, the data packet is passed to the Internet layer of the TCP/IP protocol stack. In this layer, IP adds the following header information:

- The source IP address
- The destination IP address
- The transport protocol
- The checksum value
- Time to Live (TTL) information

In addition to adding this information, the Internet layer is also responsible for resolving the destination IP addresses to a MAC address. The ARP performs this resolution. The MAC address is added to the packet header and the packet is handed down to the network interface layer.

Network Interface Layer

The network interface layer adds two types of information—a preamble and a cyclical redundancy check (CRC)—to the packet that it receives from IP. The preamble is a sequence of bytes that identifies the beginning of a frame. The CRC is a mathematical computation that is added to the end of the frame to verify that the frame has not been corrupted.

After the information is added to the frames at the network interface layer, they are merged onto the network. The frames are sent to all computers on the network.

Destination Computer

When the frames reach the destination computer, the network interface layer on this computer discards the preamble and recalculates the CRC. If this value matches the value calculated before transmission, then the destination MAC address on the frame is examined.

If the MAC address is a broadcast address or if the MAC address matches that of the destination computer, the frame is passed to the IP in the Internet layer above, otherwise the frame is discarded. At the IP layer, IP recalculates the checksum and compares it with the value calculated before transmission to determine if the packet arrived intact. Then IP passes the packet to the transport protocol identified in the IP header.

At the transport layer, if the packet is received by TCP, it checks the sequence number on the packet and sends an acknowledgement back to the TCP at the source computer. Then, it uses the TCP port information on the packet to send it onwards to the appropriate application in the application layer above.

If UDP receives the packet from the Internet layer, it uses the UDP port information on the packet to send it to the appropriate application in the application layer without sending an acknowledgement to the source computer. After the application receives the data, it processes it as required.

◆ Routing Data

Topic Objective

To introduce the role of routers in transmitting data.

Lead-in

On most large networks, data needs to be routed from one portion of the network to another.

- IP Routing
- Data Transfer Across Routers

*****ILLEGAL FOR NON-TRAINER USE*****

Data flow in a network that consists of a single segment is simple. Each computer that transmits data can broadcast a request over the network for the MAC address of the destination computer and send the data to it. However, in networks that have multiple segments, the data transmission process is more complex. In such environments, TCP/IP provides for multiple paths between computers and prevents unnecessary communication from crossing segment boundaries.

In an environment that has connected networks, the source and destination computers may not be on the same segment. IP determines whether the destination computer is local or remote in relation to the source computer. If the destination computer is remote, the data cannot be sent to it directly. Instead, IP sends it to a router, which then forwards the packet to its destination.

In this section, you will learn about the role of IP in the routing process and the process by which data is transmitted across routers.

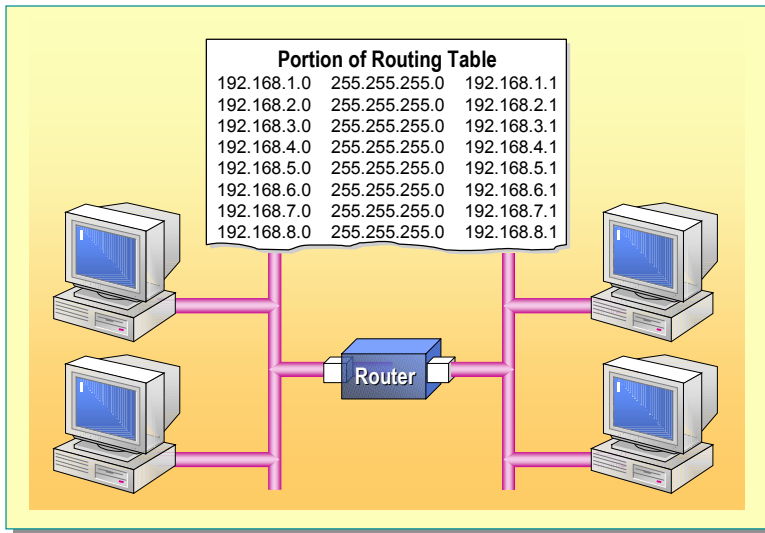
IP Routing

Topic Objective

To illustrate the role of IP in transferring data.

Lead-in

IP plays a very important role in transferring data across multiple network segments.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Introduce the term internetwork here because the primary function of the TCP/IP protocol stack is to enable communication over a large area. Point out that routers are the key to understanding how an internetwork functions. Make sure students understand the difference between direct and indirect delivery, as this is an important aspect of the IP protocol.

Large TCP/IP networks, referred to as internetworks, are broken up into smaller segments to reduce the amount of communication within the segment. An *internetwork* is a network consisting of multiple segments that are connected by routers. Routers are basically computers with two network adapters that provide the primary means of joining two or more physically separated segments.

Routers pass IP packets from one network segment to another. This process of forwarding IP packets is known as routing. Routers are attached to two or more IP network segments, enabling packets to be forwarded from one segment to another.

Packet Delivery

Forwarded IP packets use at least one of two types of delivery, based on whether the IP packet is forwarded to the final destination or whether it is forwarded to a router. These two types of delivery are known as direct and indirect delivery.

- Direct delivery occurs when a computer forwards a packet to a final destination on the same segment. The computer encapsulates the IP packet in a frame format for the network interface layer and addresses the packet to the destination's MAC address.
- Indirect delivery occurs when a computer forwards a packet to a router because the final destination is not on the same segment. The computer encapsulates the IP packet in a frame format for the network interface layer addressed to the IP router's MAC address.

Routing Table

To determine where a packet is to be forwarded, routers use routing tables to send data between network segments. A routing table is stored in memory and maintains information about other IP networks and hosts. In addition, a routing table provides information to each local host about how to communicate with remote networks and hosts.

For each computer on an IP network, you can maintain a routing table that contains an entry for every other computer or network in communication with the local computer. However, this is not practical for large networks and a default router is used to maintain the routing table.

Routing tables can be either static or dynamic, depending upon the way they are updated. You update a static routing table manually. Because updating cannot be done often, the information in the routing table may not be current. On the other hand, a dynamic routing table is automatically updated as new information becomes available.

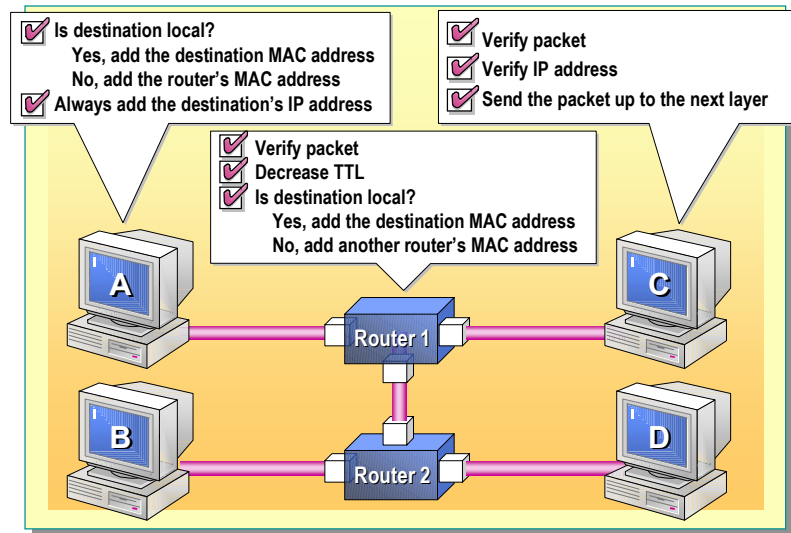
Data Transfer Across Routers

Topic Objective

To illustrate the process of data transfer across routers.

Lead-in

Data is transmitted across interconnected networks through routers.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use this slide as a conclusion to the analogy begun in the first section. Use the slide to first explain the process of transmitting data from computer A over router 1 to computer C. Then question the students about the process of transmitting data from computer A to computer B or D. Make sure to emphasize the placement of the second MAC address in the second example.

IP plays an important role in transmitting data across internetworks. Packets are exchanged and processed on each computer by using IP at the Internet layer on the source computer, at routers along the path to the destination, and at the destination computer.

To send data between two computers that are on different network segments, IP consults a local routing table for a route to the remote computer. If it finds a route, it sends the packet using that route. Otherwise, it forwards the data packets to its default router.

IP at the Source Computer

In addition to adding such information as the TTL, IP always adds the IP address of the destination computer to the packet. In the case of a direct delivery, ARP is used to add the MAC address of the destination computer. In the case of indirect delivery, ARP is used to add the MAC address of the router to which the packet will be forwarded.

IP at the Router

After the packet reaches a router, IP on the router determines where the packet is to be sent next. For this purpose, IP performs the following steps:

1. IP verifies the checksum and destination IP address.
If the IP address is the router's IP address, the router processes the packet as the destination computer (IP at the destination).
2. IP then decreases the TTL and checks its routing table for the best route to the destination IP address.
3. In the case of a direct delivery, ARP is used to add the MAC address of the destination computer. In the case of indirect delivery, ARP is used to add the MAC address of the router to which the packet will be forwarded.

This entire process is repeated at each router in the path between the source and destination computer until the packet reaches a router on the same segment as the destination computer.

Fragmentation and Reassembly

When a packet that is too large to be transmitted on the network arrives at a router, IP breaks up the packet into smaller packets before transmitting it onward. This process is known as fragmentation.

All of the small packets are then routed to the remote network. Even if they travel through multiple routers, the fragments are reassembled only when all of the small packets that make up the entire data transmission reach the destination computer. This process is known as reassembly.

IP at the Destination

When a packet is received at the destination computer, it is passed up to IP. IP on the destination computer verifies the checksum and destination IP address. IP then passes the packet to either TCP or UDP. Finally, the packet is passed to the destination application, based on the port number, for final processing.

Note If at any time the TTL drops below zero or a step fails, such as if the destination application is not found, the packet is dropped and an ICMP packet may be returned. Although the delivery of an ICMP packet is not guaranteed, if TCP is used, then the original packet will be retransmitted.

Lab B: Identifying Processes and Protocols in TCP/IP

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the processes that are involved in name resolution and the protocols involved in using the Ping utility across a router.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify the processes involved with name resolution.
- Identify the protocols involved in using the Ping utility across a router.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- Microsoft Internet Explorer 5 or later.
- A minimum display resolution of 800 x 600 with 256 colors (16-bit recommended).

► To start the lab

1. Log on as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Processes and Protocols in TCP/IP**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 15 minutes

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to TCP/IP
- TCP/IP Protocol Suite
- Name Resolution
- Examining the Data Transfer Process
- Routing Data

*****ILLEGAL FOR NON-TRAINER USE*****

1. TCP/IP uses a four-layer communication model to transmit data from one location to another. What are the layers in the four-layer model used by TCP/IP?

Internet layer, application layer, transport layer, and network interface layer.

2. When one application needs to communicate with an application on another computer, what does TCP/IP use to differentiate applications from one another, as well as to identify which computer they belong to?

It uses a socket.

3. What three elements make up a socket?

An IP address, port, and the transport layer protocol.

4. What are the six core protocols provided in the Microsoft TCP/IP suite?

TCP, UDP, ICMP, IGMP, IP, and ARP.

5. Which of the six core protocols would you want to use if you need to have an application that accepts credit cards across the network and want to guarantee that the data arrives?

TCP.

6. Which of the six core protocols is responsible for addressing and routing the data to its final destination?

IP.

7. As the administrator of a network, you want to verify that the TCP/IP suite is installed properly and to test communications on the network. Which TCP/IP utility would you use?

Ping.

8. If you wanted to use a user-friendly computer name versus an IP address to identify a computer, what are some of the storage locations that could map the computer names to IP addresses?

Hosts file, Lmhosts file, DNS, and WINS.

9. When using indirect delivery to send a packet from a source computer to a destination computer, the source computer must first determine the MAC address belonging to _____.

A router.

Module 7: Examining IP Addressing

Contents

Overview	1
Classful IP Addressing	2
Subnetting a Network	6
Lab A: Determining Class Addresses and Subnet Masks	11
Planning IP Addressing	15
Lab B: Identifying Valid IP Addresses	19
Assigning TCP/IP Addresses	20
Lab C: Examining the Configuration of TCP/IP	25
Review	32
Course Evaluation	34



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
60 Minutes

Labs:
60 Minutes

This module provides students with an overview of classful IP addressing, subnetting, assigning IP addresses, and viewing the TCP/IP configuration. The first section defines the components of an IP address and describes the IP address classes. The second section then explains the process of subnetting with subnets and subnet masks. In the lab that follows these sections, the students identify the class of an IP address, its components, and default subnet mask. The third section describes the addressing guidelines and valid ranges of network IDs and host IDs. In the lab that follows this section, students allocate IP addresses and identify valid IP configurations.

The last section in the module discusses static and dynamic addressing and the methods for viewing TCP/IP information. The key function of the section is to identify the different reasons for using each tool. In the lab that follows, the students use two methods—the Ipconfig utility and the **Internet Protocol (TCP/IP) Properties** dialog box—to view the TCP/IP information on their computers. They also identify the appropriate use of both methods.

At the end of this module, students will be able to:

- Define IP address classes and describe the features of each class.
- Define subnetting and describe the components used to subnet a network.
- Describe the issues involved in planning the IP addresses to be used in a network.
- Describe the methods used to assign an IP address by using the tools provided by Microsoft® Windows® 2000.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_07.ppt
- Module 7, “Examining IP Addressing”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Read the white papers, *Introduction to TCP/IP* and *TCP/IP Implementation Details for Windows 2000*, on the Trainer Materials compact disc.
- Read the IP Addressing topic in Windows 2000 Help.
- Complete the three labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Classful IP Addressing**

Begin the module with a review of the concept of an IP address that was introduced in module 6, “Examining TCP/IP,” in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*. Describe the components of an IP address. Next, give an overview of classful addressing, and then explain the types of address classes and their function in identifying the components of an IP address.

- **Subnetting a Network**

Describe the reason for creating subnets in a network. Continue by explaining the concepts of subnetting and subnet masks and the reason why custom subnet masks are useful for dividing an existing network ID. Then describe the procedure for determining whether two hosts are local or remote with respect to each other.

- **Planning IP Addressing**

Explain the restrictions on the values of the network ID and host ID that must be considered before assigning an IP address. Then describe the valid ranges of network IDs and host IDs that can be assigned.

- **Assigning TCP/IP Addresses**

Differentiate between static and automatic IP addressing. Demonstrate how to assign an IP address to a host, and then explain the two methods for viewing TCP/IP information. Demonstrate how to use the Ipconfig utility, and then describe the situations in which the use of each of these methods is most appropriate.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how IP addresses are used to determine the address class of a computer, how networks are subnetted, how IP addresses are planned, and how they are assigned in a network.

- **Classful IP Addressing**
- **Subnetting a Network**
- **Planning IP Addressing**
- **Assigning TCP/IP Addresses**

*****ILLEGAL FOR NON-TRAINER USE*****

The primary function of Internet Protocol (IP) is to add address information to data packets and to route them across the network to the correct destination. To understand how IP accomplishes this, it is necessary to be familiar with the concepts that determine the intermediate and final destination addresses of the data packet.

To determine the location of a destination host with respect to the source computer, IP addresses are organized into classes. This is called classful IP addressing. You must assign IP addresses to all computers that are connected on the network. Network segments connected by a router are called subnets. Breaking down the network into subnets for the purpose of assigning IP addresses is called *subnetting*.

Based on the rules that govern classful IP addressing, you plan and assign the IP addresses for each computer by using the tools provided by Microsoft® Windows® 2000.

Note The word *host* is often used to describe any device on a network that sends and receives information by using an IP address. All of the computers, printers, and routers in a TCP/IP network are hosts and require at least one IP address to communicate.

At the end of this module, you will be able to:

- Describe classful IP addressing and describe the features of each class.
- Describe the procedure for subnetting a network.
- Describe the issues involved in planning the IP addresses for a network.
- Describe the procedure used to assign an IP address using the tools provided by Windows 2000.

◆ Classful IP Addressing

Topic Objective

To introduce the concept of IP address classes.

Lead-in

A computer needs to determine the location of another computer before it can send data to it.

- IP Addresses
- IP Address Classes

*****ILLEGAL FOR NON-TRAINER USE*****

To be able to communicate on a network, each computer must have a unique IP address. In classful IP addressing, there are three address classes used to assign IP addresses to computers. The size and type of a network determines the IP address class that you apply when you provide IP addresses for the computers and other hosts on your network.

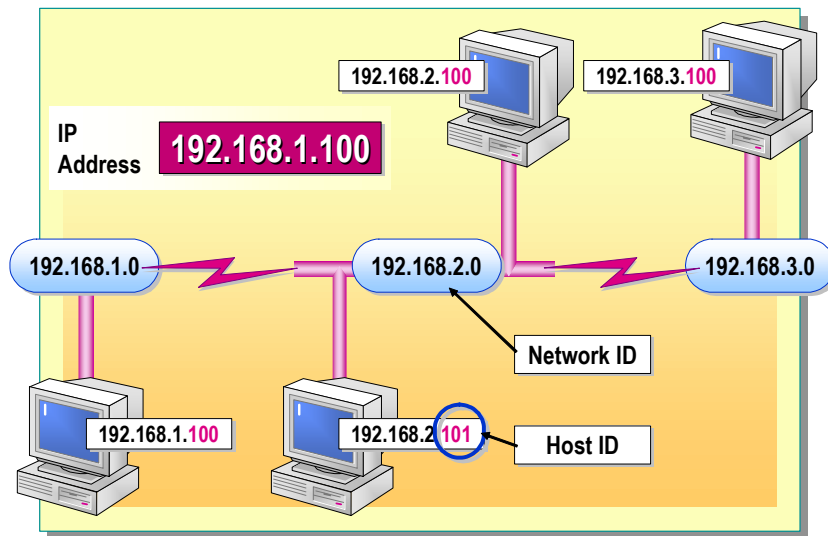
IP Addresses

Topic Objective

To illustrate an IP address.

Lead-in

IP addresses form the backbone of the TCP/IP communication process.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide shows four computers with IP addresses, located on three different networks. The slide shows how the IP addresses could represent the same host ID or network ID, but that the entire IP address must be unique to communicate with another computer.

Key Point

An IP address is not just an identifier; it is also a way to locate a computer on the network. This is why we introduce network ID and host ID on this page. At this point, the students need to know that the IP addresses themselves are unique and that the first portion is used for the network ID and the second is used for the host ID. The exact formatting of the host ID and the network ID is discussed on the following page.

The IP address is the unique identifier that differentiates one computer from another in a network and helps to locate where that computer resides in the network. An IP address is required for each computer and network component, such as a router, that communicates using TCP/IP.

The IP address identifies a computer's location on the network; similar to the way a numerical address identifies a house in a city. Just as the address for a specific house must be unique but follow certain addressing conventions, an IP address should be unique but conform to a standard format. An IP address consists of a set of four numbers, each of which can range from 0 to 255.

Components of an IP Address

In the same way that a house address has two parts—a street address and a postal delivery area code (ZIP code)—an IP address also has two parts—the host ID and the network ID.

Network ID

The first part of the IP address is the network ID, which identifies the network segment on which the computer is located. All computers on the same segment must have the same network ID, just as all houses in a specific area must have the same postal delivery area code.

Host ID

The second part of the IP address is the host ID, which identifies a computer, router, or other device within a segment. The host ID for each host must be unique within the network ID, in the same way that the street address for a house must be unique within the postal delivery area code.

It is important to note that just as two different postal delivery areas can have the same street address within them, two computers with different network IDs can have the same host ID. However, the combination of the network ID and the host ID must be unique to all computers in communication with each other.

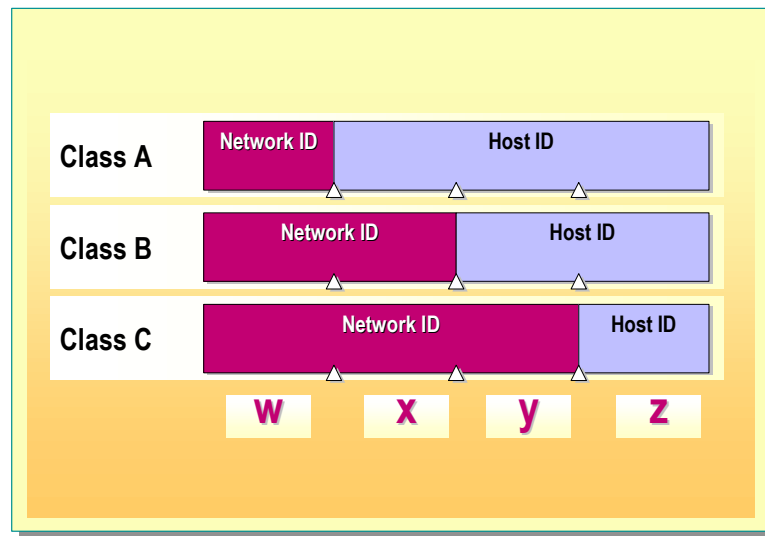
IP Address Classes

Topic Objective

To illustrate the IP address classification system.

Lead-in

IP addresses are divided into five categories for ease of management, three of which are used to assign IP addresses to computers.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Ensure that the students understand that only class A, B, and C addresses are assigned to hosts. Also point out that besides separating host IDs and network IDs, classes are used to allocate IP addresses to allow communication on the Internet.

Address classes are used to assign network IDs to organizations so that the computers on their networks can communicate on the Internet. Address classes are also used to define the dividing point between the network ID and host ID. An organization is assigned a block of IP addresses, which are referred to by the addressees' network ID and which are based on the organization's size. For example, an organization with 200 hosts is assigned a class C network ID; whereas an organization with 20,000 hosts is assigned a class B network ID.

Class A

Class A addresses are assigned to networks with a very large number of hosts. This class allows for 126 networks, by using the first number for the network ID. The remaining three numbers are used for the host ID, allowing for 16,777,214 hosts per network.

Class B

Class B addresses are assigned to networks that range from medium to large in size. This class allows for 16,384 networks, by using the first two numbers for the network ID. The remaining two numbers are used for the host ID, allowing for 65,534 hosts per network.

Class C

Class C addresses are used for small, local area networks (LANs). This class allows for approximately 2,097,152 networks, by using the first three numbers for the network ID. The remaining number is used for the host ID, allowing for 254 hosts per network.

Classes D and E

Classes D and E are not allocated to hosts. Class D addresses are used for multicasting, and the class E addresses are reserved for future use.

Determining the Address Class

Classful IP addressing is based on the structure of the IP address and provides a systematic way to differentiate network IDs from host IDs. There are four numerical segments of an IP address. An IP address can be represented as $w.x.y.z$, where w , x , y , and z are numbers with values ranging from 0 to 255. Based on the value of the first number, w in the numerical representation, IP addresses are categorized into five address classes as illustrated in the following table.

IP address class	IP address	Network ID	Range of values of w
A	$w.x.y.z$	$w.0.0.0$	1 - 126*
B	$w.x.y.z$	$w.x.0.0$	128 – 191
C	$w.x.y.z$	$w.x.y.0$	192 – 223
D	$w.x.y.z$	Not available	224 – 239
E	$w.x.y.z$	Not available	240 - 255

*The network ID 127.0.0.0 is reserved for testing connectivity.

Determining the Network and Host ID

For the IP addresses in class A, the network ID is the first number in the IP address. For class B, the network ID is the first two numbers; and for class C, the network ID is the first three numbers in the IP address. The remaining numbers identify the host ID.

The network ID has a four-number structure like the IP address. Therefore, if the first number, w , in an IP address represents the network ID, the structure of the network ID is $w.0.0.0$, with the three remaining numbers being 0. The structure of the host ID is $x.y.z$. Note that the host is not preceded by a 0.

For example, the IP address 172.16.53.46 would be a class B address because $w=172$ and is between 128 and 191. That makes the network ID 172.16.0.0 and the host ID 53.46 (without a period at the end).

◆ Subnetting a Network

Topic Objective

To introduce the concept of subnetting.

Lead-in

Subnets enable a large number of computers to effectively communicate in a network. To accomplish this, the computers must be able to differentiate between a computer on the same subnet and one on a different subnet.

- Subnets
- Subnet Masks
- Determining Local and Remote Hosts

*****ILLEGAL FOR NON-TRAINER USE*****

You can expand a network by using physical devices, such as routers and bridges, to add network segments. You can also use physical devices to divide a network into smaller segments in order to increase the network's efficiency. Network segments separated by routers are called *subnets*.

When you create subnets, you must break up the network ID for the hosts on the subnets. Dividing the network ID used to communicate on the Internet into smaller (based on the number of IP addresses identified) network IDs for a subnet is called *subnetting* a network. To then identify the new network ID for each subnet, you must use a subnet mask to specify which portion of the IP address is to be used for the new network ID of the subnet.

You can locate a host on a network by analyzing the host's network ID. Matching network IDs show which hosts are on the same subnet. If the network IDs are not the same, you know that they are on different subnets and that you need a router to establish communication between them.

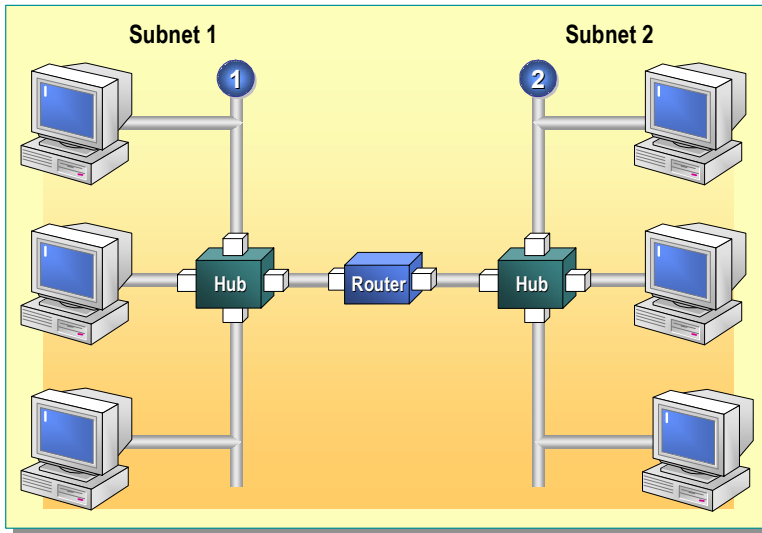
Subnets

Topic Objective

To illustrate the structure of a subnet.

Lead-in

This topic explains why networks are subdivided into smaller network segments.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Make sure to point out that in creating a subnet, each subnet receives its own network ID. Also stress the important function of a router as the boundary between subnets. This arrangement between subnets and routers leads to the term internetwork, which describes a network divided into subnets.

Most Windows 2000 networks are based on Ethernet technology, in which computers use broadcasts to transmit information. As the number of computers and the volume of traffic on an Ethernet network increase, there is a corresponding increase in data collision and a decrease in network performance. To solve this problem, computers in an Ethernet network are grouped together into physical divisions, called segments, which are separated by a physical device, such as a router or bridge.

In a TCP/IP environment, segments that are separated by routers are known as subnets. All of the computers that belong to one subnet have the same network ID in their IP addresses. Every subnet must have a different network ID to communicate with other subnets. Based on the network ID, subnets define the logical divisions of a network. Computers that are on different subnets need to pass their communication through routers.

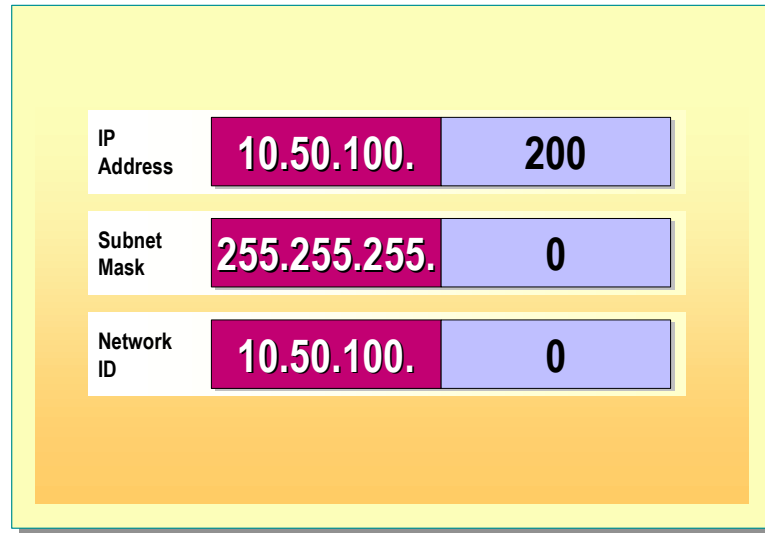
Subnet Masks

Topic Objective

To illustrate the division of an IP address into the network and host ID by using a subnet mask.

Lead-in

This topic explains the process by which the computer differentiates the network ID from the host ID by using a subnet mask.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Although it is possible to use subnet masks other than the ones mentioned here, the goal is to introduce the topic of subnet masks in a fashion that allows the student to configure a subnet mask without using classful boundaries. A second goal is to recognize how a subnet mask can identify the network ID in an IP address. Because the focus is on the network ID, the slide is animated and shows that the 10.50.100.200 IP address could have different subnet masks.

In the classful method, the number of networks and hosts available for a specific address class is pre-determined. As a result, an organization that is allocated a network ID has a single, fixed network ID and a specific number of hosts as determined by the address class to which the IP address belongs.

With the single network ID, the organization can have only one network connecting its allocated number of hosts. If the number of hosts is large, the single network will not be able to perform efficiently. To solve this problem, the concept of subnetting was introduced.

Subnetting allows a single classful network ID to be divided into smaller (as defined by the number of IP addresses identified) network IDs. Using these multiple smaller network IDs, the single network can be segmented into subnets, each with a different network ID, also known as a subnet ID.

Structure of Subnet Masks

To divide a network ID, you use a subnet mask. A subnet mask is a screen that differentiates the network ID from a host ID in an IP address but is not restricted by the same rules used in the classful method. A subnet mask consists of a set of four numbers, similar to an IP address. These numbers can range in value from 0 to 255.

In the classful method, each of the four numbers can assume only the maximum value 255 or the minimum value 0. The four numbers are then arranged as contiguous maximum values followed by contiguous minimum values. The maximum values represent the network ID and the minimum values represent the host ID. For example, 255.255.0.0 is a valid subnet mask, whereas 255.0.255.0 is not. The subnet mask 255.255.0.0 identifies the network ID as the first two numbers in the IP address.

Default Subnet Masks

In the classful method, every address class has a default subnet mask. The following table lists the default subnet masks for each address class.

IP address class	IP address	Subnet mask	Network ID	Host ID
A	<i>w.x.y.z</i>	255.0.0.0	<i>w.0.0.0</i>	<i>x.y.z</i>
B	<i>w.x.y.z</i>	255.255.0.0	<i>w.x.0.0</i>	<i>x.y</i>
C	<i>w.x.y.z</i>	255.255.255.0	<i>w.x.y.0</i>	<i>z</i>

Custom Subnet Masks

When subnetting an existing network ID to create additional subnets, you can use any of the above subnet masks with any IP address or network ID. So the IP address 172.16.2.200 could have the subnet mask 255.255.255.0 and network ID 172.16.2.0, as opposed to the default subnet mask 255.255.0.0 with the network ID 172.16.0.0. This allows an organization to subnet an existing class B network ID of 172.16.0.0 into smaller network IDs to match the actual configuration of their network.

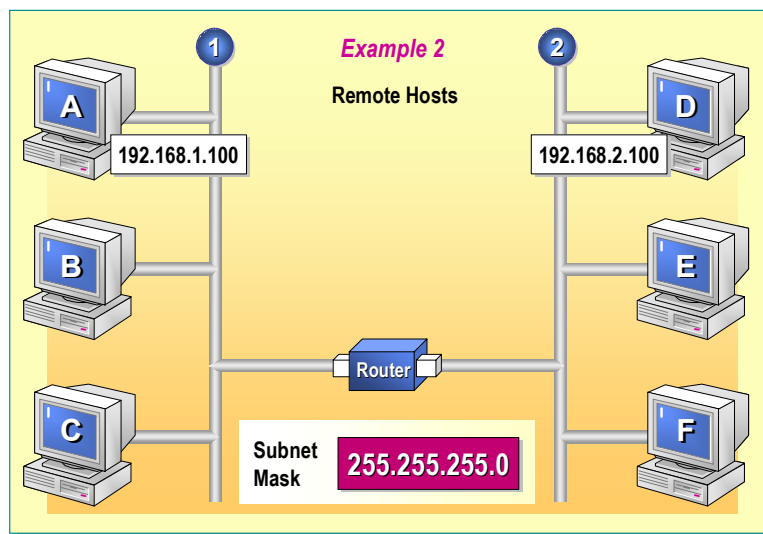
Determining Local and Remote Hosts

Topic Objective

To illustrate local and remote hosts.

Lead-in

After the network IDs of IP addresses are identified, determine whether two hosts are local or remote with respect to each other.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Remind the students that if a network is not divided into subnets, then all communication must be local. And if the network IDs do not match, communication does not occur. Again, reinforce the idea that IP is responsible for getting a packet to its destination. The focus here is how IP determines if a router is needed for communication. Note that the IP addresses in the examples are the same, but the subnet mask varies. This shows the importance of a properly configured subnet mask.

After the network ID of a host is identified, it is easy to determine whether another host is local or remote with respect to it. To do so, you compare the network IDs of both hosts. If the network IDs match, the two hosts are on the same subnet. If the network IDs do not match, then the hosts are on different subnets and a router is required to transmit data between them.

Example 1

Consider the two computers A and B with the IP addresses 192.168.1.100 and 192.168.2.100 and a subnet mask of 255.255.0.0. As illustrated in the following table, the network IDs of their IP addresses match. Therefore, computers A and B are local.

	Computer A	Computer B
IP Address	192.168.1.100	192.168.2.100
Subnet Mask	255.255.0.0	255.255.0.0
Network ID	192.168.0.0	192.168.0.0

Example 2

As another example, consider the computers A and D with the IP addresses 192.168.1.100 and 192.168.2.100 and a subnet mask of 255.255.255.0. The network IDs of these IP addresses do not match as illustrated by the following table. Therefore, computer A is remote with respect to computer D.

	Computer A	Computer D
IP Address	192.168.1.100	192.168.2.100
Subnet Mask	255.255.255.0	255.255.255.0
Network ID	192.168.1.0	192.168.2.0

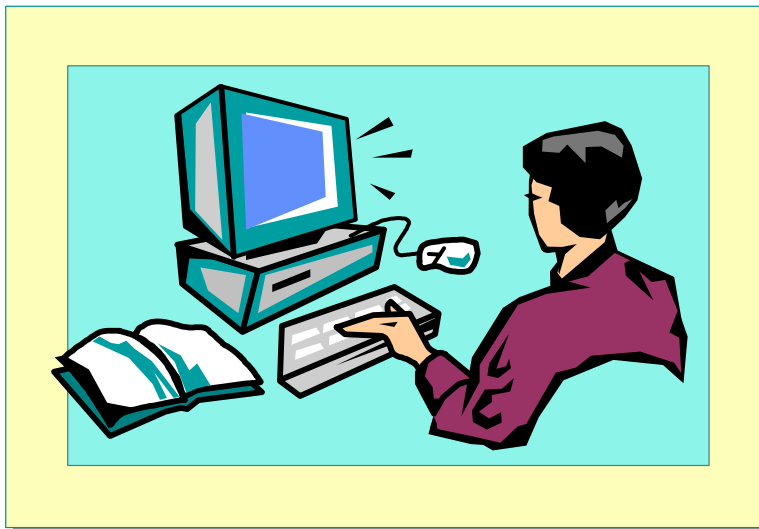
Lab A: Determining Class Addresses and Subnet Masks

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the correct address class and subnet mask for a given IP address and then determine the host ID and network ID of the IP address.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify the class of an IP address.
- Identify the default subnet mask of an IP address.
- Identify the network ID of an IP address.
- Identify the host ID of an IP address.

Estimated time to complete this lab: 15 minutes

Exercise 1

Using IP Address Classes to Determine Network and Host IDs

Scenario

You are an administrator and need to identify the network and host ID for a given IP address, so that you can determine if a router is needed to communicate between the two computers.

Goal

In this exercise, you will identify the class of IP address and the default subnet. You will then separate the network ID from the host ID.

Tasks	Detailed Steps
1. Identify the class, subnet mask, network ID, and host ID for the IP address 131.107.2.1	- Use the first number of the IP address to identify the default class and associated subnet mask for the address. - Calculate the network ID by using the numeric values in the IP address that correspond to 255 in the subnet mask, and then fill in the remaining portion with zeros (0s). - Calculate the host ID by using the numeric values in the IP address that correspond to 0 in the subnet mask.
 Note: Repeat for each IP address in the table below. The first IP address is filled in as an example.	

IP address	Class/Subnet mask	Network ID	Host ID
129.102.197.23	B/255.255.0.0	129.102.0.0	197.23
131.107.2.1			
199.32.123.54			
32.12.54.23			
1.1.1.1			
221.22.64.7			
93.44.127.235			
23.46.92.184			
152.79.234.12			
192.168.2.200			
168.192.3.26			
224.224.224.224			
200.100.50.25			
172.71.243.2			
163.37.212.32			
76.35.61.23			

(continued)

Tasks	Detailed Steps
	What does calculating the network ID allow you to determine? You calculate the network ID so that you can compare it with the network ID of the destination computer. If the two network IDs are equal, then the two computers are on the same segment. If the two network IDs are not equal, then you must use a router to communicate.
	Although the host ID can be used to identify a computer on a specific segment, what address does the TCP/IP suite use to determine if it is communicating with the correct computer? Although the host ID is a user-friendly way to identify a computer, the MAC address is always the most basic identifier used for communication between computers. The host ID is still important because it must be unique on a given segment so that the IP address can be resolved to a MAC address.
	What type of communication transmission is used to identify the MAC address and limit the identification of a MAC address to only those computers on the same segment? The TCP/IP suite uses ARP, which in turn uses a broadcast message to resolve a MAC address from an IP address. Since ARP queries all of the computers on the same segment, it is important that each of the computers on that segment have a unique IP address.

(continued)

Tasks	Detailed Steps
 Why is it important to use routers to physically segment a network? Physically segmenting a network allows more computers to communicate by avoiding the need for each computer to listen to every packet that is sent. This way, only the limited number of computers that exist on the same segment will see all the packets that are sent. The specific packets that are destined for other segments are the only packets seen by more than one segment.	

◆ Planning IP Addressing

Topic Objective

To introduce the guidelines for assigning network and host IDs.

Lead-in

After a network is established, IP addresses are required for all of the computers in it. This section explains how to plan the assignment of IP addresses so that there are no conflicts.

- Addressing Guidelines
- Assigning Network IDs
- Assigning Host IDs

*****ILLEGAL FOR NON-TRAINER USE*****

After a network is established, each computer in it needs an IP address; in much the way houses on a city block need addresses assigned to them. Without an IP address, a computer does not receive data directed to it. And like house addresses, the format of the IP address must follow certain guidelines to ensure that the data is transmitted to the correct computer.

This section explains the guidelines for assigning network and host IDs.

Addressing Guidelines

Topic Objective

To highlight the important addressing guidelines.

Lead-in

Not all possible IP addresses can be assigned to host computers.



The First Number in the Network ID Cannot Be 127



The Host ID Cannot Be All 255s



The Host ID Cannot Be All Zeros



The Host ID Must Be Unique to the Local Network ID

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Although these guidelines are defined further when considering binary IP addresses and subnets, they also work well for classful and simple IP address assignments (those that use only 255s in the subnet mask). The goal here is to add no additional content that is not related to the module.

You must consider some guidelines on the numbers used for the network ID and the host ID when you assign an IP address by using classes. These guidelines are:

- The first number in the network ID cannot be 127. This ID number is reserved for testing connections, such as the local loopback.
- The numbers in the host ID cannot all be 255, as this address is used as an IP broadcast address.
- The host ID cannot be all zeros (0s) because this address is used to denote a network ID.
- The host ID must be unique to the local network ID.

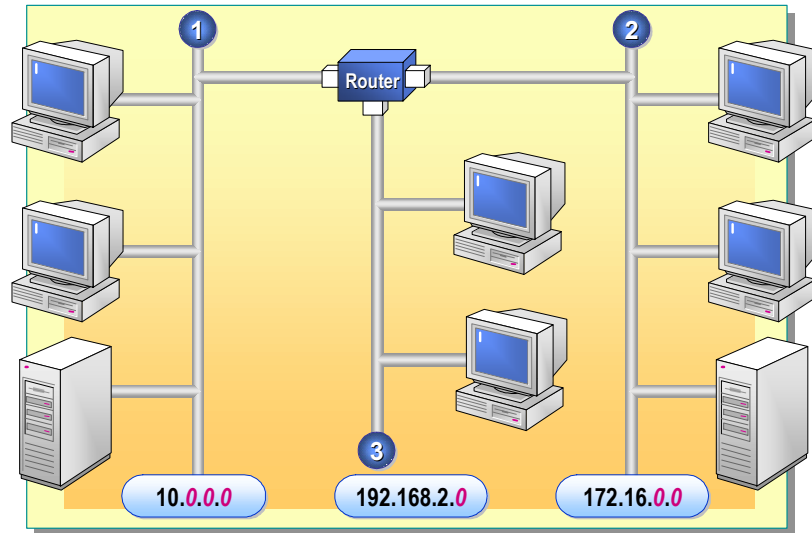
Assigning Network IDs

Topic Objective

To illustrate the valid ranges of network IDs.

Lead-in

Each subnet must be identified by a network ID.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Remind the students that classes are an effective method for dividing the IP addresses for organizations on the Internet. This is why each organization that communicates on the Internet must have a unique network ID.

The network ID identifies the TCP/IP hosts that are located on the same physical subnet. All hosts on the same subnet must be assigned the same network ID to enable them to communicate with each other.

Each subnet must have a unique network ID. For example, subnet A could have the network ID 10.0.0.0, subnet B could have the network ID 192.168.2.0, and subnet C could have the network ID 172.16.0.0.

The following table lists the valid ranges of network IDs for a network.

Address class	Beginning range	Ending range
Class A	1.0.0.0	126.0.0.0
Class B	128.0.0.0	191.255.0.0
Class C	192.0.0.0	223.255.255.0

Note If you plan to connect your network to the Internet, you must ensure that the network ID portion of the IP address is unique among all of the other networks on the Internet. To obtain a valid IP network number assignment, you can contact your Internet service provider. You can then subnet your network by using subnet masks to further divide your individual network.

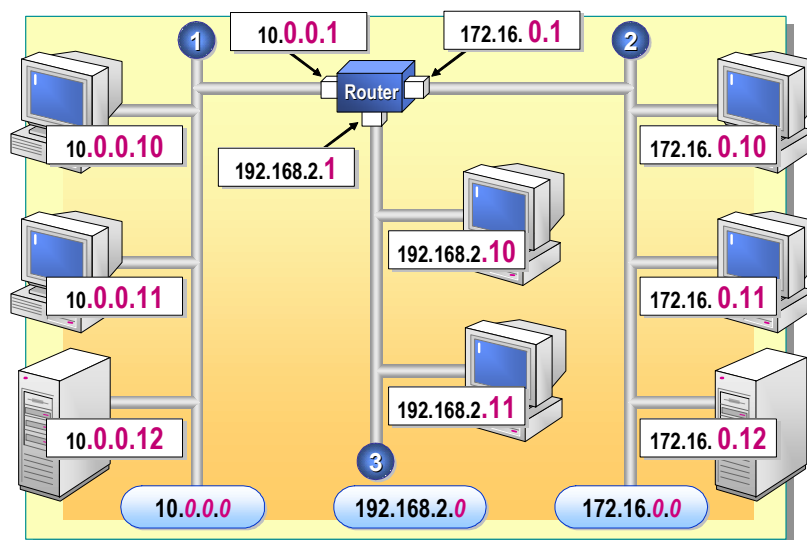
Assigning Host IDs

Topic Objective

To illustrate the valid ranges of host IDs.

Lead-in

Consider the following issues before assigning host IDs.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Although calculating the host ID helps in assigning IP addresses in a subnet, the host ID by itself is not useful. You need a complete IP address to identify a host.

The host ID identifies a TCP/IP host within a network and must be unique to the network ID. All TCP/IP hosts, including routers, require unique host IDs. There are no rules for assigning host IDs in a subnet. For example, you can number all TCP/IP hosts consecutively, or you can number them so that they can be easily identified, such as by assigning the router on each subnet the number 1 for the last number of the host ID.

Valid Host IDs

The following table lists the valid ranges of host IDs for each class of network.

Address class	Beginning range	Ending range
Class A	w.0.0.1	w.255.255.254
Class B	w.x.0.1	w.x.255.254
Class C	w.x.y.1	w.x.y.254

Default Gateway

For a specific host, the IP address of the router that is on the same segment as the host is known as the host's default gateway. All information that the host needs to send to segments other than its own is routed through the default gateway.

Because a host and its default gateway are on the same segment, they have the same network ID but different host IDs. For example, for the host with the IP address 192.168.2.11, the IP address of the default gateway is 192.168.2.1.

Lab B: Identifying Valid IP Addresses

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will allocate IP addresses and then give reasons why various IP addresses are valid for different sizes of networks.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Allocate IP addresses in a single-segment environment.
- Allocate IP addresses in a multiple-segment environment.
- Identify invalid IP configurations.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- Microsoft Internet Explorer 5 or later.
- A minimum display resolution of 800 x 600 with 256 colors. Recommended display resolution of 800 x 600 with high color (16-bit).

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Valid IP Addresses**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 30 minutes

◆ Assigning TCP/IP Addresses

Topic Objective

To introduce the processes for assigning TCP/IP addresses.

Lead-in

After the network and host IDs are formulated, the next step is to configure the computers accordingly.

- Static IP Addressing
- Automatic IP Addressing
- Viewing TCP/IP Configuration
- Viewing TCP/IP Configuration Using Ipconfig

*****ILLEGAL FOR NON-TRAINER USE*****

You can set IP addresses using either of two methods—static or automatic. If you choose to set the IP address statically, then you must manually configure the address at each computer in the network. If you choose to set the IP address automatically, then you can configure the IP addresses for an entire network from a single location and then dynamically assign them to each computer.

After you set the IP address, you can view its TCP/IP configuration by using either the **Internet Protocol (TCP/IP) Properties** dialog box or the Ipconfig utility.

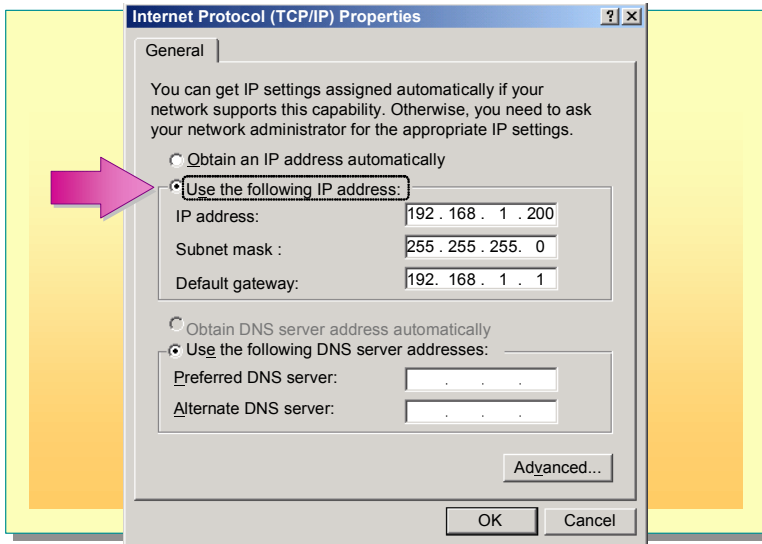
Static IP Addressing

Topic Objective

To illustrate static IP addressing.

Lead-in

You can assign IP addresses manually using the **Internet Protocol (TCP/IP) Properties** dialog box.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to use the **Internet Protocol (TCP/IP) Properties** dialog box and explain how to choose the option to set addresses statically. You can then use that as an introduction to the next page by having the students access the **Internet Protocol (TCP/IP) Properties** dialog box on their computers. Students asking why they cannot see their IP address will provide a lead-in to the next page. Note that your IP address is static, but theirs are automatic, if the standard class setup is used.

Static IP addressing refers to configuring IP addresses manually. In this method, you use a utility provided by Windows 2000 to assign an IP address. Windows 2000 provides the **Internet Protocol (TCP/IP) Properties** dialog box to manually assign an IP address to a TCP/IP host or device.

To open the TCP/IP Properties dialog box

1. From the **Start** menu, point to **Settings**, and click **Network and Dial-up Connections**.
2. In the Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties** to display the **Internet Protocol (TCP/IP) Properties** dialog box.

In this dialog box, click **Use the following IP address** to enter values for the IP address, subnet mask, and default gateway.

Note In general, most computers have only one network adapter installed and therefore require only a single IP address. If a device, such as a router, has multiple network adapters installed, each adapter needs its own IP address.

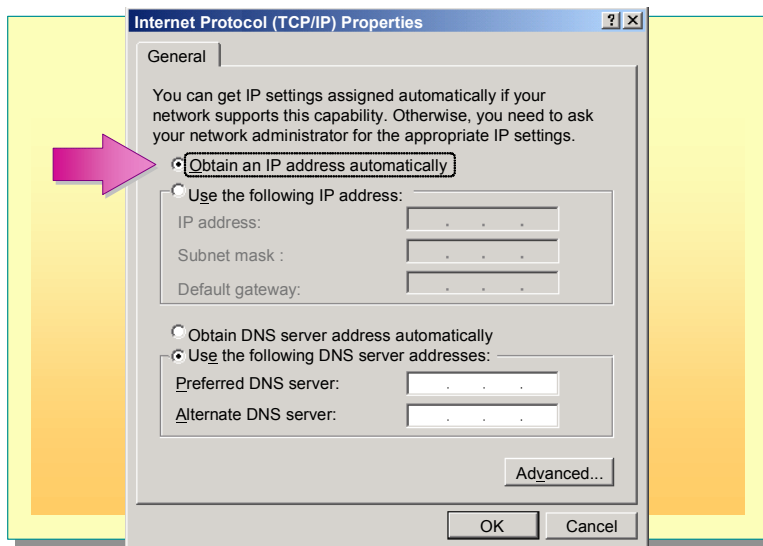
Automatic IP Addressing

Topic Objective

To illustrate automatic IP addressing.

Lead-in

Windows 2000 facilitates assigning IP addresses automatically.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the **Internet Protocol (TCP/IP) Properties** dialog box and point out the automatic options. The students' computers should be set to automatic if the standard classroom setup is used.

By default, Windows 2000 is configured to obtain an IP address automatically by using Dynamic Host Configuration Protocol (DHCP).

DHCP

DHCP is a TCP/IP standard for simplifying the management of IP configuration and assignment in an internetwork. DHCP uses a DHCP server to manage the dynamic allocation of IP addresses. DHCP servers contain a database of IP addresses that can be given out to hosts on the network.

To use DHCP in a network, hosts in the network must be DHCP-enabled. To enable DHCP, you must click **Obtain an IP address automatically**, which is selected by default in Windows 2000.

DHCP reduces the complexity and amount of administrative work involved in reconfiguring computers in TCP/IP-based networks. When you move a computer from one subnet to another, you must change its IP address to reflect the new network ID. DHCP allows you to automatically assign an IP address to a host, also called a DHCP client, from a database of addresses assigned to a subnet. Also, when a computer is offline for a specific amount of time, DHCP can reassign its IP address.

Automatic Private IP Addressing (APIPA)

If a DHCP server cannot be reached to assign an IP address automatically, Windows 2000 determines an address in the Microsoft-reserved, IP-addressing class that ranges from 169.254.0.1 through 169.254.255.254. This address is used until a DHCP server is located. This method of obtaining an IP address is termed automatic IP addressing. In this method, DNS, WINS, or a default gateway are not assigned because the method is designed only for a small network that consists of a single segment.

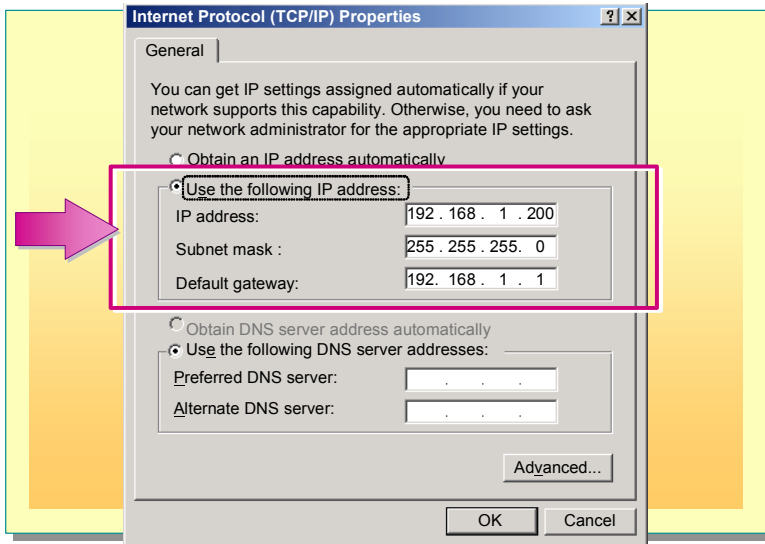
Viewing TCP/IP Configuration

Topic Objective

To illustrate the **Internet Protocol TCP/IP Properties** dialog box for viewing TCP/IP information.

Lead-in

After you set a TCP/IP configuration on a computer, you can view the configuration at any time, provided the IP address is static.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

If students ask how they can view their IP address, use their question as an introduction to the next page. Remember: you can see your IP address but they cannot see theirs. The **Internet Protocol (TCP/IP) Properties** dialog box is important because it is used to set TCP/IP to be configured statically or automatically. The students will view the dialog box in the lab.

You may encounter situations where you need to view the IP address information for a specific computer. For example, your computer may not communicate with other computers on the network, or other computers may not be able to communicate with your computer. In such situations, you need to know the IP address of the other computers in order to determine the problem.

You can use the **Internet Protocol (TCP/IP) Properties** dialog box to view static TCP/IP information.

Internet Protocol (TCP/IP) Properties Dialog Box

Using the **Internet Protocol (TCP/IP) Properties** dialog box, you can determine whether the IP address configuration has been performed dynamically or statically. However, if the IP address has been configured dynamically using DHCP or configured automatically by Windows 2000, you cannot determine the values of the TCP/IP configuration options. These options include the IP address, subnet mask, and default gateway. You can determine these values only if the configuration has been done statically.

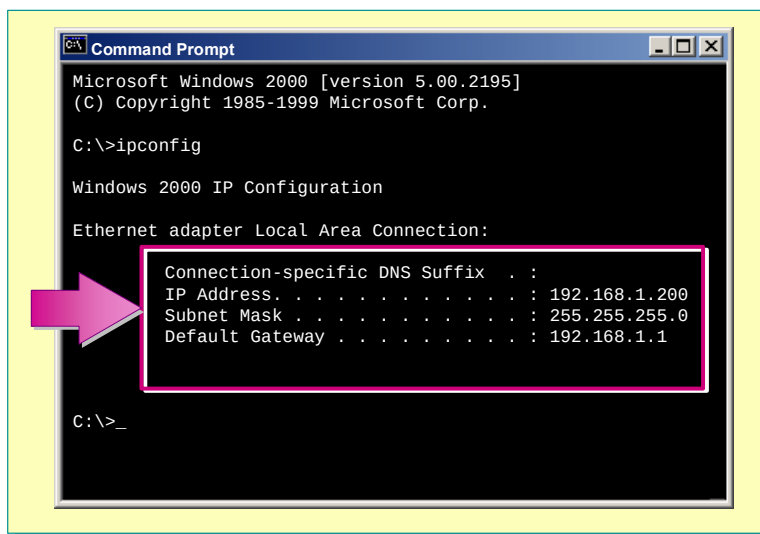
Viewing TCP/IP Configuration Using Ipconfig

Topic Objective

To illustrate the syntax of the Ipconfig utility for viewing TCP/IP information.

Lead-in

After you set a TCP/IP configuration on a computer, you can view the configuration at any time.



```

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.200
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1
  
```

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the procedure to access the Ipconfig utility. Emphasize to the students that the Ipconfig utility cannot be used to set the TCP/IP configuration. Question the students about the differences between the information displayed using Ipconfig and the **Internet Protocol (TCP/IP) Properties** dialog box. This will be the focus of the following lab.

Windows 2000 provides a command-line utility known as Ipconfig to view TCP/IP information.

Ipconfig

The Ipconfig utility is used to verify, but not set, the TCP/IP configuration options on a host, including the IP address, subnet mask, and default gateway. The command syntax for this utility is *ipconfig*.

To start the Ipconfig utility, type **ipconfig** at the command prompt. The values of the three primary configuration parameters are displayed. However, if you use this utility, you cannot determine whether the static or dynamic method has been used to assign the IP address.

Ipconfig /all

You can obtain more detailed information using the Ipconfig utility by specifying the switch, **all**, with it. To use the Ipconfig utility with this switch, type **ipconfig /all** at the command prompt.

The screen displays the information about all TCP/IP configuration options. You can now determine whether DHCP is enabled. If the value of the DHCP Enabled parameter is Yes and a DHCP server IP address is displayed, then it implies that the IP address has been obtained using DHCP.

A DHCP server leases an IP address to a client for a specific length of time. The Lease Obtained and Lease Expires labels display information on when the lease was obtained and when it will expire, respectively.

If a DHCP server was unavailable to assign an IP address and the IP address was assigned automatically, the term autoconfiguration would precede the label for the IP address of the computer. The Autoconfiguration Enabled label would be Yes. Also, the DHCP server IP address would not be displayed.

Lab C: Examining the Configuration of TCP/IP

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will evaluate a scenario and identify errors in IP address allocation.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- View the configuration of TCP/IP by using the Ipconfig utility.
- View the configuration of TCP/IP by using the **Internet Protocol (TCP/IP) Properties** dialog box.
- Identify the appropriate use of both the Ipconfig utility and the **Internet Protocol (TCP/IP) Properties** dialog box.

Prerequisites

Before working on this lab, you must have:

- Knowledge of the Microsoft Windows 2000 TCP/IP suite.
- Knowledge of IP addresses.
- Knowledge of how to log on to Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Examining the Configuration of TCP/IP

Scenario

You are the administrator of a small network and want to view the configuration of the computers on your network.

Goal

In this exercise, you will use and compare the **Internet Protocol (TCP/IP) Properties** dialog box and Ipconfig utility to identify the current IP configuration of your computer.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password , and then open the Internet Protocol (TCP/IP) Properties dialog box.	a. Log on to Windows 2000 as Administrator with a password of password. b. Click Start, point to Settings, and then click Network and Dial-up Connections.  <i>The Network and Dial-up Connections window appears.</i> c. Right-click the Local Area Connection icon. d. Click Properties. e. Click Internet Protocol (TCP/IP). f. Click Properties.
 Can you tell if your IP address is assigned? If yes, then how is it assigned? The computer is configured to obtain the IP address automatically.	
 Can you view your IP address? If so, what is it? No.	

Tasks	Detailed Steps
? Can you configure TCP/IP to use a static IP address? If so, how? Yes, by clicking Use the following IP address. _____ _____ _____ _____	
1. (continued)	g. Close all open windows. (Click Cancel when available.)
2. Use the Ipconfig utility to view your computer's IP address.	a. Click Start, point to Programs, point to Accessories, and then click Command Prompt. b. Type ipconfig in the Command Prompt window.
? Can you tell how your IP address was assigned? If yes, how? No. _____ _____ _____ _____	
? Can you view your IP address? If so, what is it? Yes, 192.168.1.x (where x is between 100 and 199). _____ _____ _____ _____	
? What additional configuration information is displayed? Also, what is your computer's additional configuration? Subnet mask and default gateway. 255.255.255.0 and w.x.y.z (instructor's IP address). _____ _____ _____ _____	

Tasks	Detailed Steps
? Can you use Ipconfig to manually set your IP address? How? No. _____ _____ _____ _____	
3. Use a switch with ipconfig to view your computer's detailed IP configuration.	a. Type ipconfig /all in the Command Prompt window.
? Can you tell how your IP address was assigned? If yes, how? Yes, DHCP. _____ _____ _____ _____	
? Can you still view your IP address and IP configuration options from earlier? Yes. _____ _____ _____ _____	
? What is the IP address of the server that provided your IP address? w.x.y.z (instructor's computer). _____ _____ _____ _____	

Tasks	Detailed Steps
	When does your IP address expire? Answers will vary, but the expiration date will be seven days after the last lease.
	If you were to type ipconfig /all in the Command Prompt window, what results would appear if your computer is configured to obtain an IP address automatically, but a DHCP server is not available? What would not appear? The word autoconfiguration would appear before the IP address label, and there would not be a DHCP server address.
	What are the benefits of using the Internet Protocol (TCP/IP) Properties dialog box instead of the Ipconfig utility? The Internet Protocol (TCP/IP) Properties dialog box allows an administrator to set a static IP address and switch between static and automatic IP addressing methods.
	What are the benefits of using the Ipconfig utility instead of the Internet Protocol (TCP/IP) Properties dialog box? The Ipconfig utility allows an administrator to view an IP address regardless of the method used to assign it. You can also use the Ipconfig utility to determine if autoconfiguration or the DHCP method was used.

Tasks	Detailed Steps
? What class of IP address do you have? Class C.	
? Is your subnet mask the same as the default subnet mask for a class C IP address? Yes, both are 255.255.255.0.	
? What is your network ID? 192.168.1.0.	
? What is the IP address of the default gateway? 192.168.1.200.	
? Does the default gateway have the same network ID as your computer? Yes.	

Tasks	Detailed Steps
 Is the default gateway located on your segment? Yes. _____ _____ _____ _____	
 What is another term for default gateway? Router. _____ _____ _____ _____	
 How many IP addresses with the same network ID could be assigned to computers on your segment? 254 _____ _____ _____ _____	
4. Close all windows and log off from Windows 2000.	a. Close all windows and log off from Windows 2000.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Classful IP Addressing**
- **Subnetting a Network**
- **Planning IP Addressing**
- **Assigning TCP/IP Addresses**

*****ILLEGAL FOR NON-TRAINER USE*****

1. What does an IP address do?

An IP address differentiates one computer from another as a separate entity in a network and helps locate a computer on an internetwork.

2. In each of the three classes (A, B, and C), which numbers (w , x , y , z) in the IP address represent the network ID and which represent the host ID?

Class A: The network ID is the first number in the IP address. The last three numbers make up the host ID.

Class B: The network ID consists of the first two numbers in the IP address. The last two numbers make up the host ID.

Class C: The network ID consists of the first three numbers. The host ID is the last number.

3. As an administrator, you need to make sure that the computers in your network communicate effectively. As your network grows, what can you do to reduce the number of computers on each portion of your network?

Break up the network into subnets.

4. You are in the process of assigning IP addresses to computers in your network. What do you need to remember when assigning IP addresses?

Such addressing guidelines as: the network ID cannot start with 127, the host ID cannot be all zeros or 255s, and the host ID must be unique to each network ID. Also, when assigning the network ID, make sure that there is one network ID for each subnet.

5. As an administrator of a large network, you want to facilitate the assignment of IP addresses in your network. What could you use to automatically assign IP addresses to computers in your network?

DHCP. Although IP addresses are automatically assigned by default without it, DHCP is effective only with a single subnet and does not allow communication to the Internet.

6. While working in a network, your computer is unable to communicate with other computers on the network. You want to view the IP address of the other computers to determine the problem. What are the two utilities provided by Windows 2000 to view the IP address configuration? What are the benefits and disadvantages of each of these tools?

The Internet Protocol (TCP/IP) Properties dialog box and the command-line utility Ipconfig. The Internet Protocol (TCP/IP) Properties dialog box is useful for switching between the automatic and static IP address options as well as for assigning a static IP address. Ipconfig is useful for viewing TCP/IP configuration options, including automatic IP address and DHCP lease information.

Course Evaluation

Topic Objective

To direct students to a Web site to complete a course evaluation.

Lead-in

Go to the Web site listed on this page to complete a course evaluation.



*******ILLEGAL FOR NON-TRAINER USE*******

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time between now and the end of the course, please complete a course evaluation, which is available at <http://www.metricsthatmatter.com/survey>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.

Module 8: Optimizing IP Address Allocation

Contents

Overview	1
Classless Inter-Domain Routing (CIDR)	2
Binary IP Addresses	5
Lab A: Using Windows Calculator to Convert Decimal and Binary Numbers	10
Binary Subnet Masks	18
Lab B: Determining Local and Remote Destinations	27
IP Address Allocation Using CIDR	28
Lab C: Allocating IP Addresses	33
Review	37



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
120 Minutes

Labs:
60 Minutes

This module provides students with the knowledge and skills required to assign IP addresses optimally. The module begins with a discussion of the limitations of classful IP addressing and introduces the benefits of Classless Inter-Domain Routing (CIDR). The next section describes the procedures to convert numbers from decimal to binary notation and vice versa. The students test the skills they learn in this section in the lab that follows it.

The third section of the module introduces the use of CIDR notation to represent IP addresses and explains the procedure for calculating a network ID in binary notation. This section is followed by a lab in which the students calculate the network ID when given an IP address and subnet mask and determine whether a destination computer is local or remote. The last section of the module provides an overview of the range of host IDs available and the concepts of supernetting and subnetting. In the lab that follows this section, the students determine the size of the network ID required based on the number of computers on the network.

At the end of this module, students will be able to:

- Describe the features of Classless Inter-Domain Routing (CIDR).
- Convert IP addresses from decimal format to binary format.
- Convert subnet masks to binary format to calculate the network ID and to determine if the destination computer is local or remote in relation to the source computer.
- Describe IP address allocation by using CIDR.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2151A_08.ppt
- Module 8, “Optimizing IP Address Allocation”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Read the white papers, *Introduction to TCP/IP* and *TCP/IP Implementation Details for Windows 2000*, on the Trainer Materials compact disc.
- Complete the three labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Classless Inter-Domain Routing (CIDR)**
Discuss the limitations of classful IP addressing and explain the underlying philosophy of CIDR.
- **Binary IP Addresses**
Explain the concept of binary notation and describe the procedure to convert decimal notation to binary notation and vice versa.
- **Binary Subnet Masks**
Explain the advantage of using subnet mask bits. Define CIDR notation and describe the procedure to calculate the network ID in binary notation. Finally, explain how to determine whether a destination host is local or remote.
- **IP Address Allocation Using CIDR**
Describe the procedure to calculate the number of hosts specified by an address block and explain the guidelines for binary IP addresses. Then discuss the concepts of supernetting and subnetting.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about the binary representation and the effective allocation of IP addresses.

- **Classless Inter-Domain Routing (CIDR)**
- **Binary IP Addresses**
- **Binary Subnet Masks**
- **IP Address Allocation Using CIDR**

*****ILLEGAL FOR NON-TRAINER USE*****

The designers of the Internet did not foresee the popularity it enjoys today. Unaware of the long-term consequences of their actions, they assigned large numbers of IP addresses without considering the effect on IP address availability. As the Internet increased in size, the number of available IP addresses declined at a rapid rate.

This shortage of available IP addresses was a result of using IP address classes to organize IP addresses. Classful IP addressing proved inefficient because it allows for only three fixed sizes for networks on the Internet—one size for each of the address classes: A, B, and C. These sizes are a result of the natural division of an IP address in decimal notation.

The depleted supply of IP addresses led to the creation of a new addressing system called Classless Inter-Domain Routing (CIDR). CIDR represents IP addresses and subnet masks in binary notation to divide the traditional fixed network sizes. This makes CIDR a more efficient choice for the allocation of IP addresses than does the classful method.

At the end of this module, you will be able to:

- Describe the features of Classless Inter-Domain Routing.
- Convert IP addresses from decimal format to binary format.
- Convert subnet masks to binary format and calculate the network ID to determine local and remote hosts.
- Describe IP address allocation by using CIDR.

◆ Classless Inter-Domain Routing (CIDR)

Topic Objective

To introduce the concept of Classless Inter-Domain Routing (CIDR).

Lead-in

The classful method of categorizing IP addresses presents certain problems.

- **Limitations of Classful IP Addressing**
- **Defining CIDR**

*****ILLEGAL FOR NON-TRAINER USE*****

IP address classes provide a simple method for differentiating local hosts from remote hosts and for locating the route to a remote host. However, this method permits very few variations in network sizes, which has led to such problems as inappropriately assigning IP addresses to networks. To overcome these limitations, a method known as Classless Inter-Domain Routing (CIDR) was developed for breaking up networks into a larger variety of sizes.

In this section, you will learn about the limitations of classful IP addressing and the advantages of using CIDR.

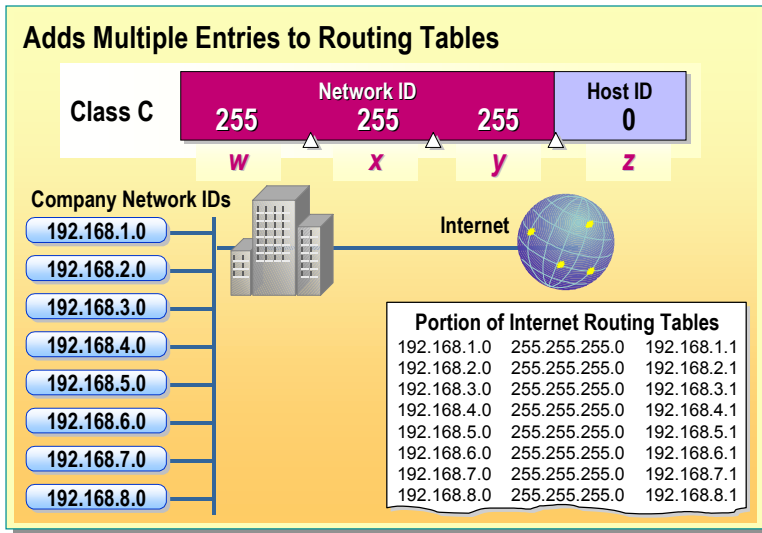
Limitations of Classful IP Addressing

Topic Objective

To illustrate the limitations of classful IP addressing.

Lead-in

As their usage grew, the IP address classes could not accommodate the demand for medium-sized networks.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the animated slides to demonstrate the unused IP addresses of a class B network. Then show how a solution to the problem of unused addresses produced another problem: overloaded routers on the Internet. The third limitation of the classful addressing system is partially addressed by simply not wasting IP addresses. An additional solution (using NAT or a proxy server) to the problem of the third limitation is addressed in module 9, "Examining Web Services," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*. These solutions are summarized in the final section.

As a result of its dramatic growth, the Internet began to experience problems with scalability. These problems resulted from using address classes to allocate IP addresses to networks that needed to connect to the Internet.

Classful IP addressing involved three major limitations:

- The number of available addresses in the class B address space was near depletion.
- The Internet routing tables were nearly full.
- All available IP addresses would be eventually assigned.

Depletion of Class B Addresses

The disparate network sizes offered by the classful method caused the depletion of class B addresses. In this system, an organization with a medium-sized network of 2,000 computers belongs to the class B category and is assigned 65,534 IP addresses although it may require only 2,000. Therefore, 63,534 IP addresses are not used because of this allocation.

Filling Up of Internet Routing Tables

To overcome the problem of unused IP addresses, an organization with a medium-sized network of 2,000 computers can divide its network into eight smaller class C networks with 254 computers each. This solution results in the generation of eight routes, or paths, to the organization's eight smaller networks. Consequently, each router on the Internet needs to maintain eight routes to forward a packet to this single organization, thus increasing the amount of information in the Internet's routing tables.

Depletion of All IP Addresses

Because of the wastefulness of the classful method and the finite number of IP addresses available, the entire pool of IP addresses would be depleted if the classful method were still in use.

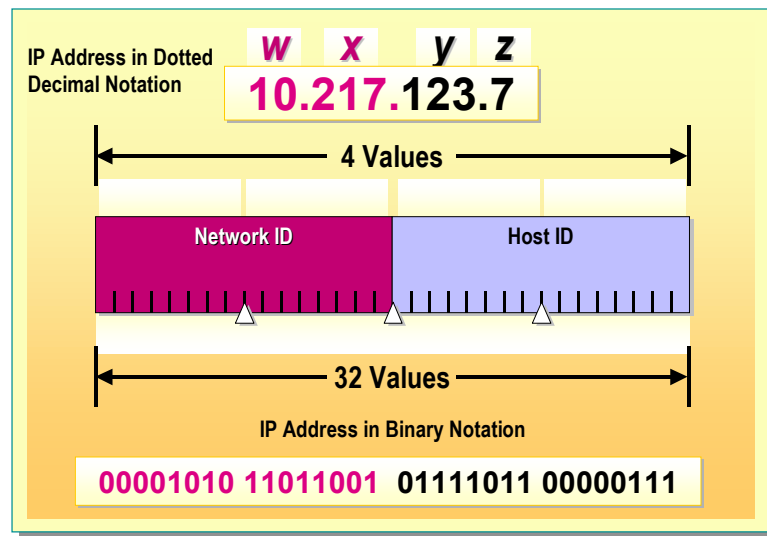
Defining CIDR

Topic Objective

To illustrate the binary representation of an IP address.

Lead-in

In response to the need to optimize the available IP address space, the CIDR method was developed.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the slide to show how the binary representation of an IP address has 32 separate values. Compare the 32 separate values available for host and network IDs with the four values visible in the decimal format.

Classless Inter-Domain Routing (CIDR) uses binary notation, whereas the classful method used decimal notation.

Use of Binary Notation

Computers use binary notation for their internal processing because they communicate using signals that have only two states: on or off. Because the binary system also has only two values: 0 or 1, computers operate using binary notation.

Increased Choice of Network Sizes

CIDR translates all IP address and subnet masks to binary notation. CIDR divides an IP address into a set of 32 values, in place of the four values used in the classful system. This division allows for more variations in network size and optimizes the allocation of IP addresses. By using CIDR, not many IP addresses go unused because it is now possible for companies to obtain IP addresses in numbers that are much closer to what they require.

CIDR does not define a default subnet mask based on the IP address. Instead, each host is configured with a custom subnet mask, and each router is sent the IP address as part of the data packet. The router then uses a subnet mask from its routing table to determine the network ID of the computer to which the packet must be forwarded.

◆ Binary IP Addresses

Topic Objective

To introduce the concept of binary notation.

Lead-in

This section describes the basics of the binary notation system.

- Converting to Binary Format
- Converting to Binary Format Using a Calculator

*****ILLEGAL FOR NON-TRAINER USE*****

To avoid the limitations of classful IP addressing, CIDR presents IP addressing in binary notation. Binary notation consists of two values: 0 and 1, whereas decimal notation has 10 values: 0 to 9. In decimal notation, a number is expressed in terms of powers of 10, in binary notation in terms of powers of 2.

This section covers the procedure used to convert binary IP addresses to decimal notation and vice versa, both manually and by using the calculator in Microsoft® Windows® 2000.

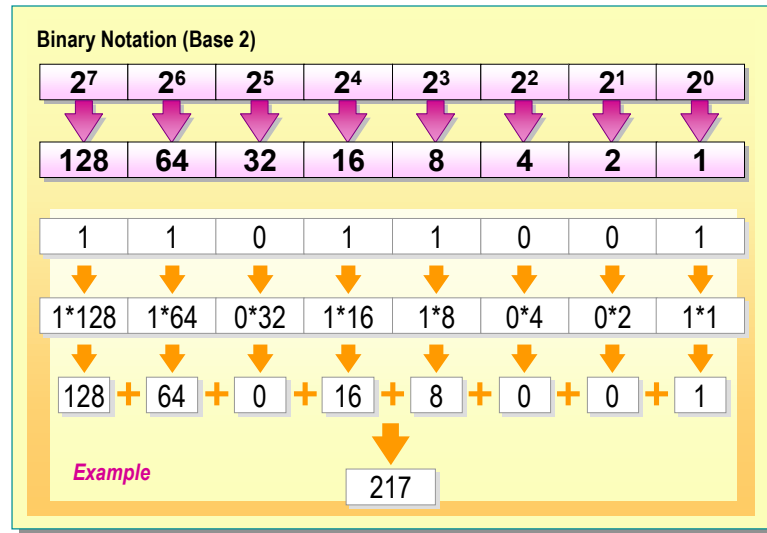
Converting to Binary Format

Topic Objective

To illustrate how to work with the binary system.

Lead-in

Computation in the binary system is similar to that in the decimal system.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The students need to know the basis of the binary system. So explain the mathematics behind binary notation before teaching them how to use a calculator to convert between decimal and binary. Depending on the specific class, you will focus on either converting manually or on using the calculator. Use the slide to show the values of each position of a binary number. Point out to the students that an IP address consists of four distinct numbers, each of which must be converted, not just one large binary number. Then use the second and third slides as examples of how both the decimal and binary number systems work.

In the binary system, an IP address is represented as a string of 32 numbers. This string can be divided into four fields; each field is called an octet, or byte. Each octet consists of eight bits. A bit has a value of either 0 or 1. Therefore, an IP address consists of 4 bytes, for a total of 32 bits.

An example of an octet in binary notation is 11011001, and an example of an IP address in binary notation is 00001010 11011001 01111011 00000111. The decimal representations of this octet and IP address are 217 and 10.217.123.7, respectively.

Decimal Notation

In decimal, or base 10 representation, you calculate the value of a number as follows: Starting with the rightmost digit, multiply each digit by increasing powers of 10, beginning with 10^0 . Then add these values to obtain the number. For example, the computation for the number 217 is:

$$7 \times 10^0 = 7 \times 1 = 7$$

$$1 \times 10^1 = 1 \times 10 = 10$$

$$2 \times 10^2 = 2 \times 100 = 200$$

$$200 + 10 + 7 = 217$$

Binary Notation

You use a similar procedure to calculate the decimal value of a binary representation. In this case, base 10 is replaced by base 2. Multiply each number in the representation by powers of 2 in place of powers of 10. For example, for the number 11011001, starting with the rightmost digit:

$$1 * 2^0 = 1 * 1 = 1$$

$$0 * 2^1 = 0 * 2 = 0$$

$$0 * 2^2 = 0 * 4 = 0$$

$$1 * 2^3 = 1 * 8 = 8$$

$$1 * 2^4 = 1 * 16 = 16$$

$$0 * 2^5 = 0 * 32 = 0$$

$$1 * 2^6 = 1 * 64 = 64$$

$$1 * 2^7 = 1 * 128 = 128$$

$$128 + 64 + 0 + 16 + 8 + 0 + 0 + 1 = 217$$

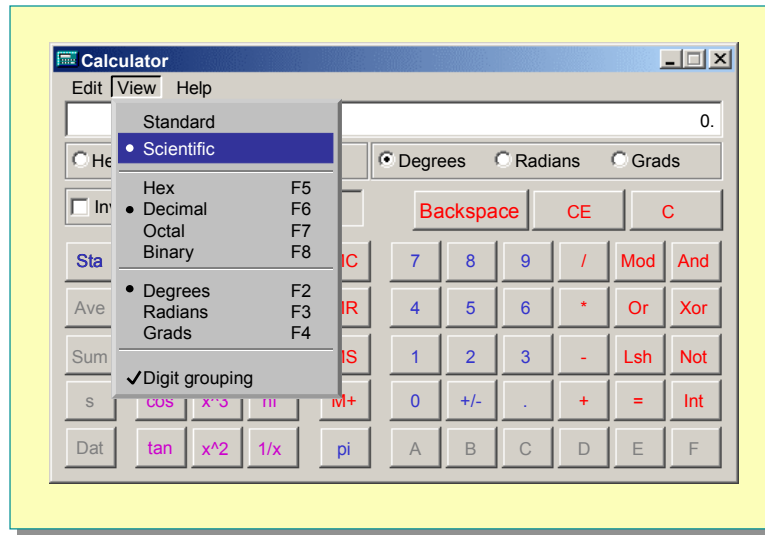
Converting to Binary Format Using a Calculator

Topic Objective

To display the scientific mode of the Windows Calculator.

Lead-in

Windows 2000 provides a calculator that simplifies the conversion of decimal numbers to binary and vice versa.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to convert from decimal format to binary format and back by using Windows Calculator in scientific mode. Remind students that they do not need to memorize the binary system because they can use the calculator to convert the numbers.

Multiplying each number in the binary representation by powers of 2 is a tedious method for obtaining its decimal equivalent. The process is simplified if you use the calculator provided by the Windows 2000 operating system.

By default, the calculator appears in standard mode. To perform calculations that include binary values, you must switch to scientific mode.

To switch to scientific mode

- On the **View** menu, click **Scientific**.

The calculator expands to display many choices for performing mathematical functions.

Using Windows Calculator to convert from decimal to binary format

- With the calculator set to scientific mode, click **Dec**.
- Type a decimal value, for example **29** and then click **Bin**.

The binary value, 11101, is displayed.

Using Windows Calculator to convert from binary to decimal format

1. With the calculator set to scientific mode, click **Bin**.
2. Type a binary value, for example **10010** and then click **Dec**.

The decimal value, 18, is displayed.

Note Windows Calculator does not accept the leftmost zeros (0s) in the binary notation of a number. Enter the binary values beginning with the first 1 in the notation. Therefore, in the above example, in place of 00010010, you type only 10010. Similarly, the calculator does not display the leftmost zeros (0s) in an octet that begins with 0. To obtain the 8-bit octet, you must prefix the displayed number with the required number of 0s. For example, the octet value of 11101 is 00011101.

Lab A: Using Windows Calculator to Convert Decimal and Binary Numbers

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will use the Windows Calculator in scientific mode to convert numbers from decimal to binary and back to decimal.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Convert decimal numbers to binary format.
- Convert binary numbers to decimal format.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how to log on to Windows 2000.

Estimated time to complete this lab: 15 minutes

Exercise 1

Converting Decimal Numbers to Binary

Scenario

You are an administrator and must convert your computers' IP addresses to binary formats before you can efficiently allocate their addresses.

Goal

In this exercise, you will convert multiple IP addresses to binary format by first converting their individual decimal numbers.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password , and then open Windows Calculator in scientific mode.	- Log on to Windows 2000 as Administrator with a password of password. - Click Start, point to Programs, point to Accessories, and then click Calculator. - On the View menu, click Scientific.  <i>Notice that the calculator expands and four option buttons appear to allow you to convert decimal numbers to binary and back again.</i> - Click Dec to ensure that the calculator is in decimal mode.
2. Convert the IP address 131.107.2.200 to binary.	In the calculator window, type 131 and then click Bin.
 What is the binary result of 131? 10000011	
 How many digits are in the binary number for 131? 8	
2. (continued)	Click Dec, type 107 and then click Bin.

Tasks	Detailed Steps
? What is the binary result of 107? 1101011 _____ _____ _____	
? How many digits are in the binary number for 107? 7 _____ _____ _____	
2. (continued)	c. Click Dec, type 2 and then click Bin.
? What is the binary result of 2? 10 _____ _____ _____	
? How many digits are in the binary number for 2? 2 _____ _____ _____	
2. (continued)	d. Click Dec, type 200 and then click Bin.
? What is the binary result of 200? 11001000 _____ _____	

Tasks	Detailed Steps
? How many digits are in the binary number for 200? 8 _____ _____	
? All octets in a binary IP address have eight digits. For any decimal numbers that are converted to binary that have fewer than eight digits, leading zeros precede the binary numbers. What will be the binary numbers for 107 and 2 with the addition of leading zeros? For 107, the binary number 1101011 becomes 01101011. For 2, the binary number 10 becomes 00000010. _____ _____ _____ _____	
? An IP address is represented by four octets separated by decimal points. What is the full binary version of the 131.107.2.200 IP address? 10000011.01101011.00000010.11001000 _____ _____ _____ _____	
3. Convert the IP addresses in the following table to binary. The first one is provided as an example.	a. Convert the first decimal number to binary. b. Convert the second decimal number to binary. c. Convert the third decimal number to binary. d. Convert the fourth decimal number to binary. e. Add leading zeros to all binary results to complete the octet. f. Separate the four binary octets with decimal points. g. Repeat until the table on the next page is completed.

Decimal IP address	Binary portions	Binary IP address
122.131.25.64	1111010, 10000011, 11001, 1000000	01111010. 10000011.00011001.01000000
215.34.211.9		
97.49.153.122		
64.144.25.100		
176.34.68.78		
42.89.215.61		
71.73.65.166		
47.245.235.84		
156.213.67.23		
124.87.235.87		
7.23.87.2		

Exercise 2

Converting Binary Numbers to Decimal

Scenario

You are an administrator and must convert your computer's IP addresses from binary formats to decimal formats so that they can be configured in Windows 2000.

Goal

In this exercise, you will convert multiple IP addresses from binary to decimal format by first converting the individual octets to decimal format.

Tasks	Detailed Steps
1. Convert the IP address 00110101.11100101.11101010.00001011 to decimal format.	a. Using Windows Calculator, make sure you are in scientific mode. b. Click Bin , type 110101 and then click Dec .
 What is the decimal result of the binary value 00110101? 53 _____ _____ _____ _____	
1. (continued)	c. Click Bin , type 11100101 and then click Dec .
 What is the decimal result of the binary value 11100101? 229 _____ _____ _____ _____	
1. (continued)	d. Click Bin , type 11101010 and then click Dec .

Tasks	Detailed Steps
? What is the decimal result of the binary value 11101010? 234	
1. (continued)	e. Click Bin, type 1011 and then click Dec.
? What is the decimal result of the binary value 00001011? 11	
? What is the decimal result of the binary IP address 00110101.11100101.11101010.00001011? 53.229.234.11	
2. Convert the IP addresses in the following table to decimal format. The first one is provided as an example.	a. Convert the binary numbers to decimals, one at a time. b. Separate the four decimal numbers with a decimal point. c. Repeat until the table on the next page is completed.

(continued)

Binary IP address	Decimal portions	Decimal IP address
01110110.00011010.10101111.01011101	118, 26, 175, 93	118.26.175.93
10101001.01010101.10101010.11011000		
00011011.11011000.10110101.01010111		
01111111.11100000.00000101.00101011		
11000100.10101100.01100001.11101111		
01110111.00111100.10111000.10101001		
10100011.11101101.10100010.10101110		
01010101.01100100.11110111.10101000		
00111100.00111010.10101000.10101111		
01010111.10111100.11101101.1010101		

Tasks	Detailed Steps
3. Close all windows and log off from Windows 2000.	a. Close all windows and log off from Windows 2000.

◆ Binary Subnet Masks

Topic Objective

To introduce the concept of binary subnet masks.

Lead-in

After converting the IP address, the subnet mask and network ID need to be converted to binary notation as well.

- Subnet Mask Bits
- CIDR Notation
- Calculating the Network ID
- Determining Local and Remote Hosts

*****ILLEGAL FOR NON-TRAINER USE*****

To be compatible with IP addresses in binary notation, subnet mask bits also must be converted to binary notation. Following the conversion of both IP addresses and subnet masks to binary notation, an IP address can be represented in CIDR notation. CIDR notation is an addressing method that associates a subnet mask with the IP address.

Regardless of whether the IP address and subnet mask are specified in CIDR notation or in decimal notation, you can calculate the network ID of the IP address by converting all values to binary notation. After you calculate the network ID, you can determine whether a destination host is local or remote.

Subnet Mask Bits

Topic Objective

To illustrate the binary values of subnet masks expressed in decimal notation.

Lead-in

Subnet masks can be converted to binary notation by using the same procedure as for IP addresses.

Binary Representation	Decimal Representation
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
11100000	224
11000000	192
10000000	128
00000000	0

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the animated slide to show the students an example of a subnet mask in binary format. Then show all of the possible decimal and binary values of a subnet mask. Emphasize the concept of contiguous maximums, in this case binary 1s, versus the maximum of 255 when viewed in decimal.

In binary notation, a subnet mask is represented by four octets, just as the IP address is. The following table shows the binary notation for the default subnet masks used in the classful method.

Decimal representation	Binary representation
255.0.0.0	11111111 00000000 00000000 00000000
255.255.0.0	11111111 11111111 00000000 00000000
255.255.255.0	11111111 11111111 11111111 00000000

Using the binary representation of a subnet mask, you can manipulate 32 numbers in place of the four numbers in the decimal representation. This increased capability provides a greater selection of network sizes compared with the three fixed sizes in the classful method.

Binary Versus Decimal Subnet Masks

Subnet masks are always composed of contiguous maximum values followed by contiguous minimum values. In binary notation, this translates to a series of contiguous 1s followed by contiguous 0s. The contiguous 1s determine the network ID and the contiguous 0s determine the host ID. Because a binary subnet mask consists of a series of contiguous 1s followed by contiguous 0s, each octet in the subnet mask represents only a limited number of decimal values, as illustrated in the following table.

Binary representation	Decimal representation
11111111	255
11111110	254
...	...
10000000	128
00000000	0

CIDR Notation

Topic Objective

To illustrate CIDR notation.

Lead-in

CIDR notation provides a simple method for identifying the subnet mask associated with an IP address.

IP Address	10 . 217 . 123 . 7
	00001010 11011001 01111011 00000111
Subnet Mask	255 . 255 . 240 . 0
	11111111 11111111 11110000 00000000
Number of Subnet Mask Bits (ones)	8 + 8 + 4 + 0 = 20
IP Address in CIDR Notation	10.217.123.7/20

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

IP addresses are divided into groups represented by a network ID. By using CIDR, the number of groups available is greater than in the classful method. The chart on the following page illustrates the relationship between classful and CIDR addresses. Remind students again that the popularity of communicating on the Internet is the reason for this increase in the number of groups.

CIDR notation involves specifying a dotted decimal notation with a bit mask. The bit mask specifies the number of contiguous 1s in the binary notation of the subnet mask associated with the IP address. The contiguous 1s are the leftmost bits in the subnet mask.

For example, the IP address represented in CIDR notation as 10.217.123.7/20 specifies that its subnet mask has 20 contiguous 1s. Consequently, the 12 bits remaining from the original 32 must be 0s.

The IP addresses in CIDR notation are known by the number of bits from the IP address that make up the network ID and are represented as /x. For example, a 10-bit network ID is represented as /10.

Note CIDR notation is also known as network prefix notation.

CIDR and IP Address Classes

In CIDR notation, the IP address represented with the /20 bit mask could be a former class A, class B, or class C IP address. The routers that support CIDR do not use the first three bits of the address to determine whether the destination host on the packet is local or remote, as they did in the classful method. Instead, they rely on the bit mask information provided with the route to make a determination.

The following table lists the practical bit masks, the associated subnet masks, and the number of classful networks possible for each.

CIDR notation	Subnet mask	Number of classful networks
/8	255.0.0.0	256 class Bs
/9	255.128.0.0	128 class Bs
/10	255.192.0.0	64 class Bs
/11	255.224.0.0	32 class Bs
/12	255.240.0.0	16 class Bs
/13	255.248.0.0	8 class Bs
/14	255.252.0.0	4 class Bs
/15	255.254.0.0	2 class Bs
/16	255.255.0.0	1 class B or 256 class Cs
/17	255.255.128.0	128 class Cs
/18	255.255.192.0	64 class Cs
/19	255.255.224.0	32 class Cs
/20	255.255.240.0	16 class Cs
/21	255.255.248.0	8 class Cs
/22	255.255.252.0	4 class Cs
/23	255.255.254.0	2 class Cs
/24	255.255.255.0	1 class C
/25	255.255.255.128	½ class C
/26	255.255.255.192	1/4 class C
/27	255.255.255.224	1/8 class C
/28	255.255.255.240	1/16 class C

Calculating the Network ID

Topic Objective

To illustrate the procedure for calculating the network ID.

Lead-in

The network ID needs to be calculated in binary notation to determine whether one host is local or remote with respect to another.

IP Address in CIDR Notation: 10.217.123.7/20			
IP Address	10 . 217 . 123 . 7		
	00001010 11011001 01111011 00000111		
Subnet Mask	255 . 255 . 240 . 0		
	11111111 11111111 11110000 00000000		
Network ID	00001010 11011001 01110000 00000000		
Network ID in CIDR Notation	10.217.112.0/20		

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Although it is possible to use Windows Calculator to AND two decimal numbers together, the students will benefit by learning the principle behind the calculation. Also remind students that this process is very similar to the process of dividing network IDs by using simple decimal subnet masks. Calculating the network ID prepares the students for identifying local and remote computers, which is described in the following section.

When you configure IP addresses in Windows 2000, you must type the IP address and subnet mask information in dotted decimal notation. Windows 2000 does not accept input in CIDR notation. However, whether the IP address and subnet mask are specified in dotted decimal notation or CIDR notation, the network ID is best calculated in binary notation.

To calculate the network ID when the IP address is specified in CIDR notation

1. Convert the IP address to binary format.
2. Use the bit mask to determine the number of bits in the IP address that make up the network ID.
3. Add 0s to the network ID to obtain its four-octet structure.

Example 1

For example, consider the IP address 10.217.123.7/20. Because this address shows that the subnet mask consists of 20 contiguous 1s, the network ID consists of the first 20 bits in the IP address followed by 0s. The following table illustrates the calculation of the network ID in binary notation.

Binary notation	
IP address	00001010 11011001 01111011 00000111
Subnet mask	11111111 11111111 11110000 00000000
Network ID	00001010 11011001 01110000 00000000

To calculate the network ID when the IP address and subnet mask are specified in decimal notation

1. Convert the IP address to binary format.
2. Convert the subnet mask to binary format.
3. Use the number of contiguous 1s in the subnet mask to determine the number of bits in the IP address that make up the network ID.

Example 2

For example, consider the IP address 10.217.123.7 and its associated subnet mask 255.248.0.0. The following table illustrates the calculation of the network ID in binary notation and the conversion of both the IP address and subnet mask to binary notation.

	Binary notation
IP address	00001010 11011001 01111011 00000111
Subnet mask	11111111 11111000 00000000 00000000
Network ID	00001010 11011000 00000000 00000000

Because the binary notation of the subnet mask consists of 13 contiguous 1s, the network ID consists of the first 13 bits in the IP address followed by 0s.

Note The process of combining the IP address with its subnet mask is known as binary ANDing.

To convert the network ID from binary notation to decimal notation

After you calculate the network ID in binary notation, you should convert it back to the dotted decimal system for users to work with it. The following table illustrates the dotted decimal notations for the network IDs calculated in the two examples above.

	Binary notation	CIDR notation
Network ID, Ex 1	00001010 11011001 01111000 00000000	10.217.56.0/20
Network ID, Ex 2	00001010 11011000 00000000 00000000	10.216.0.0/13

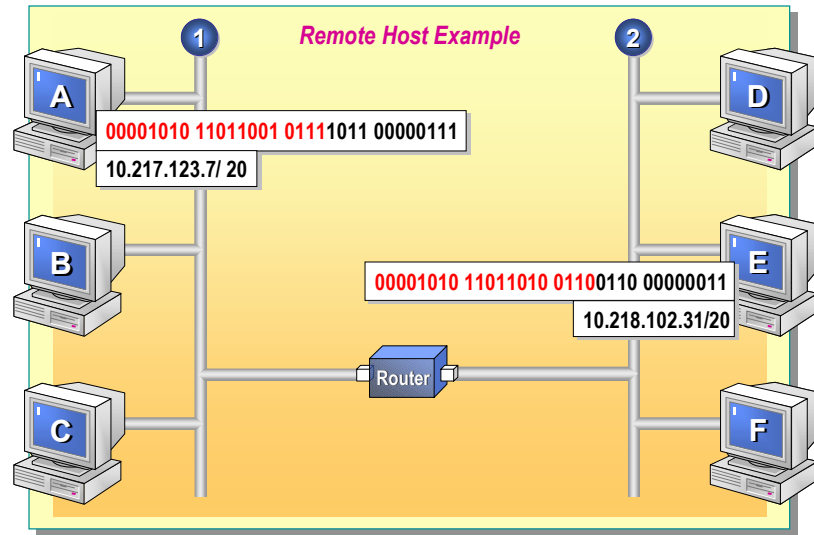
Determining Local and Remote Hosts

Topic Objective

To illustrate the procedure for determining whether a host is local or remote with respect to another.

Lead-in

After you convert the network ID of an IP address to binary notation, it is possible to determine if another host is local or remote with respect to it.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Remind the students that this process is identical to the one used with classful IP addresses: If the network IDs are different, then the computers are remote; if they are the same, the computers are local. Also ask the students if they remember what physical device is used to communicate if the computers are remote. The animated slide shows an example of both local and remote hosts that use the same IP addresses with different subnet masks.

After the network ID is identified, a computer can distinguish whether a destination host is local or remote by comparing its own network ID with that of the destination host. This determines whether a router is required as an intermediate host.

Local Host Example

Consider the pair of IP addresses 10.217.123.7/10 and 10.218.102.31/10 belonging to Computer A and Computer B. The following tables detail how the two network IDs are calculated to determine whether they are local or remote in relation to each other.

Computer A

IP addresses	00001010 11011001 01111011 00000111
Subnet masks	11111111 11000000 00000000 00000000
Network ID (binary)	00001010 11000000 00000000 00000000
Network ID (decimal)	10.192.0.0

Computer B

IP addresses	00001010 11011010 01100110 00000011
Subnet masks	11111111 11000000 00000000 00000000
Network ID (binary)	00001010 11000000 00000000 00000000
Network ID (decimal)	10.192.0.0

As the tables show, the network IDs of the two IP addresses match. Therefore, Computer A is local in relation to Computer B.

Remote Host Example

As another example, consider the pair of IP addresses 10.217.123.7/20 and 10.218.102.31/20 belonging to Computer A and Computer E. The following tables detail how the two network IDs are calculated to determine whether they are local or remote in relation to each other.

Computer A	
IP addresses	00001010 11011001 01111011 00000111
Subnet masks	11111111 11111111 11110000 00000000
Network ID (binary)	00001010 11011001 01110000 00000000
Network ID (decimal)	10.217.112.0

Computer E	
IP addresses	00001010 11011010 01100110 00000011
Subnet masks	11111111 11111111 11110000 00000000
Network ID (binary)	00001010 11011010 01100000 00000000
Network ID (decimal)	10.218.96.0

As these tables show, the network IDs of the two IP addresses do not match. Therefore, Computer A is remote in relation to Computer E.

Lab B: Determining Local and Remote Destinations

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will use Windows Calculator to create a subnet mask when given a number of hosts and report the number of hosts for a given subnet mask. You will also evaluate a subnet mask to determine if it is valid.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Calculate a network ID given a decimal IP address and subnet mask.
- Calculate whether the destination computer is local or remote.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- Microsoft Internet Explorer 5 or later.
- A minimum display resolution of 800 x 600 with 256 colors. Recommended display resolution of 800 x 600 with high color (16-bit).

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Determining Local and Remote Destinations**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 30 minutes

◆ IP Address Allocation Using CIDR

Topic Objective

To introduce the process of allocating IP addresses by using CIDR.

Lead-in

CIDR streamlines the process of allocating IP addresses.

- Available Host IDs
- Optimizing the Allocation of IP Addresses

*****ILLEGAL FOR NON-TRAINER USE*****

CIDR provides a simple method for calculating the number of available host IDs based on the subnet mask associated with a block of IP addresses.

CIDR optimizes the allocation of IP addresses through the use of *supernetting* and *subnetting*. Supernetting is a procedure that combines multiple addresses to form a single network ID. Subnetting divides a large network into multiple subnets.

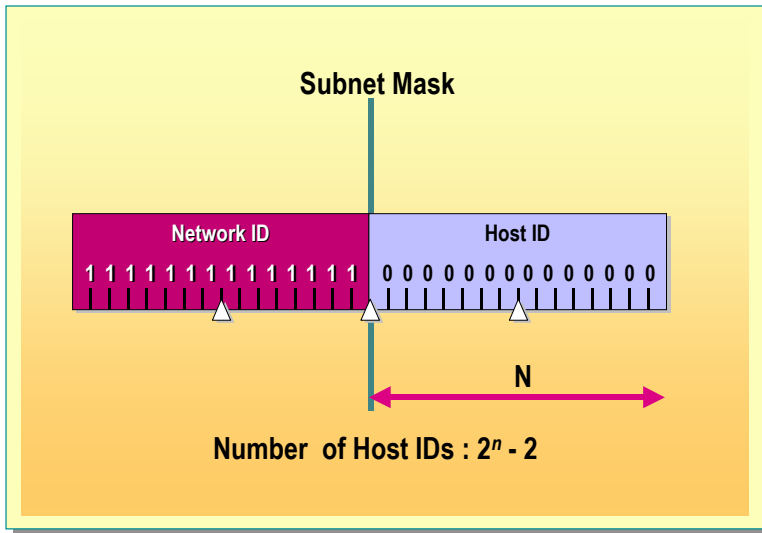
Available Host IDs

Topic Objective

To illustrate the calculation of the number of available host IDs in an address block.

Lead-in

The number of host IDs available per IP address block can be determined by using the subnet mask associated with the IP address block.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Review the addressing guidelines described in module 7, "Examining IP Addressing," in course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*. The first two guidelines in that topic also apply to this topic. Use the examples to point out the importance of viewing the IP address and subnet mask in binary format as a means of identifying valid and invalid host IDs. Use the chart on the following page to identify which subnet mask is needed to configure a specific size of network. Ask the students what the CIDR notation and subnet mask would be for several networks of different sizes.

The number of hosts supported by a network ID is calculated by using the number of 0s in the associated subnet mask. If the number of 0s is denoted by n , the number of hosts is calculated as $2^n - 2$. The two addresses that are subtracted from the expression are the reserved IP addresses that cannot be allocated to any host.

Reserved Host IDs

The values of the bits in a host ID cannot be all 0s or 1s. The host ID with the value 0 is used to denote a network ID. The host ID consisting of all 1s is used as an IP broadcast address. The following tables show an example of a valid host ID and a reserved host ID.

Valid Host ID

	Binary notation	Decimal notation
IP address	11000000 10101000 11000001.00000000	192.168.193.0
Subnet mask	11111111 11111111 11110000 00000000	255.255.240.0
Host ID	0001 00000000	1.0

Reserved Host ID

	Binary notation	Decimal notation
IP address	11000000 10101000 11000000.00000000	192.168.192.0
Subnet mask	11111111 11111111 11110000 00000000	255.255.240.0
Host ID	0000.00000000	0.0

The following table shows the possible host values for a specific number of non-zero bits in the CIDR notation of an IP address.

CIDR notation	Subnet mask	Number of 0s	Number of hosts (2^n-2)
w.x.y.z/1	128.0.0.0	31	2,147,483,646
w.x.y.z/2	192.0.0.0	30	1,073,741,822
w.x.y.z/3	224.0.0.0	29	536,870,910
w.x.y.z/4	240.0.0.0	28	268,435,454
w.x.y.z/5	248.0.0.0	27	134,217,726
w.x.y.z/6	252.0.0.0	26	67,108,862
w.x.y.z/7	254.0.0.0	25	33,554,430
w.x.y.z/8	255.0.0.0	24	16,777,214
w.x.y.z/9	255.128.0.0	23	8,388,606
w.x.y.z/10	255.192.0.0	22	4,194,302
w.x.y.z/11	255.224.0.0	21	2,097,150
w.x.y.z/12	255.240.0.0	20	1,048,574
w.x.y.z/13	255.248.0.0	19	524,286
w.x.y.z/14	255.252.0.0	18	262,142
w.x.y.z/15	255.254.0.0	17	131,070
w.x.y.z/16	255.255.0.0	16	65,534
w.x.y.z/17	255.255.128.0	15	32,766
w.x.y.z/18	255.255.192.0	14	16,382
w.x.y.z/19	255.255.224.0	13	8,190
w.x.y.z/20	255.255.240.0	12	4,094
w.x.y.z/21	255.255.248.0	11	2,046
w.x.y.z/22	255.255.252.0	10	1,022
w.x.y.z/23	255.255.254.0	9	510
w.x.y.z/24	255.255.255.0	8	254
w.x.y.z/25	255.255.255.128	7	126
w.x.y.z/26	255.255.255.192	6	62
w.x.y.z/27	255.255.255.224	5	30
w.x.y.z/28	255.255.255.240	4	14
w.x.y.z/29	255.255.255.248	3	6
w.x.y.z/30	255.255.255.252	2	2
w.x.y.z/31	255.255.255.254	1	Not available
w.x.y.z/32	255.255.255.255	0	Not available

Note Some individuals and small businesses are assigned the subnet mask 255.255.255.255 by their Internet provider. Although many of the network IDs in this chart are not practical, such as 2 or 2 billion, it is a useful reference for determining the subnet mask needed for subnets of particular sizes.

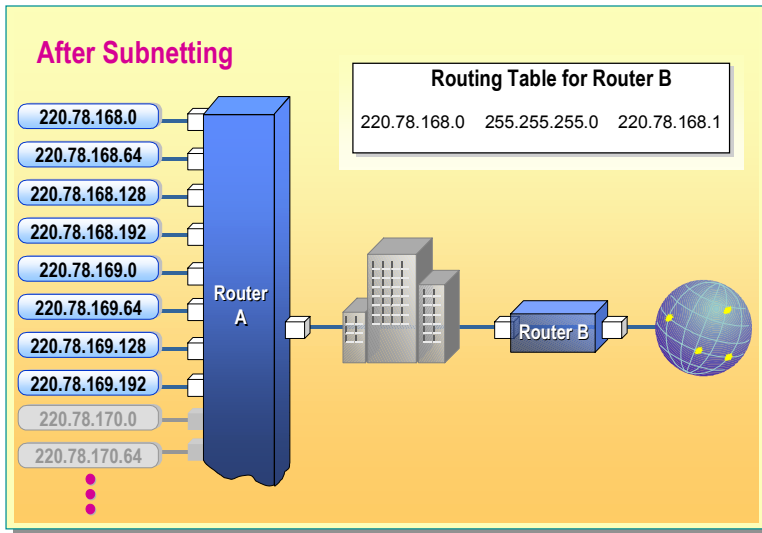
Optimizing the Allocation of IP Addresses

Topic Objective

To illustrate the concepts of supernetting and subnetting.

Lead-in

You can use two procedures to optimally allocate IP addresses.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This page introduces the topic of supernetting and reviews the topic of subnetting. This page does not provide the students with the skills to subnet and supernet an existing network. The slides illustrate router A inside an organization and router B on the Internet. Use the slides to illustrate how supernetting reduces the problems described at the beginning of the module, whereas subnetting enables an organization to maintain an internal structure that effectively separates their overall network.

In addition to providing a new method for differentiating between local and remote hosts, CIDR also provides solutions to the problems associated with classful IP addressing. These problems include the assignment of an incorrect number of IP addresses or the addition of multiple entries to Internet routing tables.

Adding Multiple IP Addresses

Consider an organization that must connect 800 computers to the Internet. It can do this by choosing either one class B network ID that provides 65,534 IP addresses or four class C addresses that provide 1,016 addresses. The first choice results in 64,734 unused IP addresses. With the second choice, only 216 IP addresses go unused, but each router on the Internet is required to add four routes to the organization in its routing table.

Supernetting

To avoid such inappropriate address allocations, CIDR uses the concept of *supernetting*. Supernetting is a strategy that combines multiple addresses from the classful environment into a single network ID in the classless environment. Using supernetting, CIDR combines multiple class C network IDs into a single CIDR network ID. In CIDR notation, a network ID is represented by the number of bits in a subnet mask, similar to an IP address, for example, 192.168.0.0/22.

In the example above, the organization can purchase a single 22-bit network ID (/22), which allows a maximum of 1,022 valid hosts, thereby providing the current 800-computer network with the ability to expand. This solution neither wastes numerous IP addresses nor adds multiple entries to the Internet routing tables.

Subnetting

Using supernetting, each organization is assigned a single CIDR network ID, which represents a single network. However, it is not efficient to work with a single large network because such factors as high network noise make the network inefficient.

To reduce the noise on its internal network, an organization can physically segment the network into subnets by using routers. As each subnet requires its own network ID, the single CIDR network ID obtained for the organization can be divided into smaller network IDs for each subnet. The process of dividing a network ID into smaller network IDs is known as subnetting. The smaller network IDs are also known as subnet IDs.

In the example considered earlier, after the organization is assigned a single network ID, it can choose to subdivide its network into smaller segments, depending upon its requirements. The organization does this by using an appropriate subnet mask. After segmenting the network physically, it is important to ensure that the network is divided logically into subnets and that a subnet is created for every segment in the network.

Then the organization assigns an internal network ID, the subnet ID, to each of the subnets, based on the number of computers that exist on each subnet. However, because subnetting is an internal process that is specific to a network, any router outside of the organization's network cannot view the separate subnets and their subnet IDs.

In the example, if the organization wanted to have no more than 62 computers on each subnet, it could use the subnet mask 255.255.255.192.

Lab C: Allocating IP Addresses

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the size of the network ID needed based on the number of computers on a network and the number of computers per subnet.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Identify the size of network ID needed based on the number of computers on a network.
- Identify the size of network ID needed based on the number of computers per subnet.

Prerequisites

Before working on this lab, you must have:

- Knowledge of classful IP addresses.
- Knowledge of converting binary numbers using a calculator.

Estimated time to complete this lab: 15 minutes

Exercise 1

Allocating IP Addresses

Scenario

You are an administrator and need to configure the network ID needed to ensure that there are enough IP addresses available for all of the computers in your network. You also need to consider using a network ID to divide your network to avoid excess broadcast traffic.

Goal

In this exercise, you will identify the network ID needed, given a specific number of hosts.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password , and calculate the number of available IP addresses given a subnet mask.	- Log on to Windows 2000 as Administrator with a password of password. - Open Windows 2000 Calculator in scientific mode. - Convert the CIDR notation to a binary subnet mask. - Write down the binary subnet mask in the table below. - Count the number of zeros in the subnet mask. - Write down the number of zeros in the table below. - In the calculator, type 2 - In the calculator, click x^y. - In the calculator, type 18 (This is the first calculation.) - In the calculator, click – (the minus button). - In the calculator, type 2 - In the calculator, click = (the equal button). - Write down the value returned from the calculator in the chart below.
 Note: Repeat the above steps for each IP address in the table below. The first calculation is provided as an example.	

CIDR notation	Subnet mask	Number of 0s	Number of hosts ($2^n - 2$)
w.x.y.z/18	11111111.11111111.11000000.00000000	18	16,382
w.x.y.z/19			
w.x.y.z/20			
w.x.y.z/21			
w.x.y.z/22			
w.x.y.z/23			
w.x.y.z/24			
w.x.y.z/25			
w.x.y.z/26			
w.x.y.z/27			

(continued)

Tasks	Detailed Steps
? Using the previous table, what is the CIDR notation for a network that needs 2,000 IP addresses? How many IP addresses are available and how many will be unused? Hint: do not forget that the number of unusable IP addresses also includes the network ID and broadcast address. w.x.y.z/21 is the CIDR notation. With 2,046 IP addresses available, 2,000 IP addresses will be used, resulting in a total of 48 unused IP addresses (46 plus the two unusable IP address for a total of 48).	
? What IP address class is required to provide 2,000 IP addresses? How many IP addresses will be provided and how many will be unused? A class B, which provides 65,534 IP addresses with 63,534 plus two for a total of 63,536 unused addresses.	
? What is the minimum number of class C address blocks that is needed to provide 2,000 IP addresses? How many IP addresses will be available for use? How many IP addresses will be unused? There are 254 available IP addresses per class C address, which requires at least eight class C address blocks, for a total of 2,032 addresses. Needing only 2,000 addresses would give 32 unused available addresses plus 16 (8 times 2) for a total of 48 unused IP addresses.	

(continued)

Tasks	Detailed Steps
	Although the number of addresses unused in the class C question is the same as the number unused in the CIDR notation, in which additional way are the multiple class C addresses inefficient? Using multiple class C addresses would also cause seven additional (eight total) routes to be added to every router on the Internet.
	If your organization decided to reduce broadcast traffic by subnetting a 21-bit network ID (2,048 IP addresses) to allow for a maximum of 126 computers per subnet, what will be the CIDR notation and decimal subnet mask for each subnet? Subnetting a CIDR notation of $w.x.y.z/21$ into 126 computers per subnet allows for a CDIR notation of $w.x.y.z/25$ and a decimal subnet mask of 255.255.255.128.
2. Close all windows and log off from Windows 2000.	a. Close all windows and log off from Windows 2000.

Review

Topic Objective

To reinforce module objectives by reviewing key points

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Classless Inter-Domain Routing (CIDR)**
- **Binary IP Addresses**
- **Binary Subnet Masks**
- **IP Address Allocation Using CIDR**

*****ILLEGAL FOR NON-TRAINER USE*****

1. What are the three major problems that developed as a result of using classful IP addressing?

The class B address space was near depletion.

The routing tables of the Internet were nearly full.

All IP addresses would be eventually assigned.

2. What is CIDR?

CIDR is a new method for organizing IP addresses. In this method, all IP addresses are represented using binary notation in place of decimal notation.

3. In the binary notation system, each IP address is represented as a string of 32 numbers. This string can be broken up into four fields, each called ____ or ____.

an octet; a byte.

4. In a subnet mask, the network ID is determined by the number of contiguous ___, and the host ID is determined by the number of contiguous ____.

1s; 0s.

5. Which notation must you use to type the IP address and subnet mask information when configuring IP addresses in Windows 2000?

Decimal notation.

6. What is supernetting?

Supernetting is a strategy that combines multiple IP addresses from the classful environment into a single address in the classless environment.

Module 9: Examining Web Services

Contents

Overview	1
Identifying Internet Concepts	2
Using Client Technologies	9
Lab A: Accessing an FTP Site by Using Internet Explorer	17
Connecting to the Internet	19
Identifying Web Server Concepts	25
Lab B: Identifying Web Concepts	29
Review	30
Course Evaluation	32



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows NT, Active Directory, BackOffice, FrontPage, Outlook, PowerPoint, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Project Lead: Red Johnston

Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)

Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.), Jay Johnson (The Write Stuff), Sonia Pande (NIIT (USA) Inc.)

Lead Program Manager: Jim Cochran (Volt)

Program Manager: Jamie Mikami (Volt)

Technical Contributors: Rodney Miller, Gregory Weber (Volt)

Testing Leads: Sid Benavente, Keith Cotton

Testing Developer: Greg Stemp (S&T OnSite)

Simulation Developer: Wai Chan (Meridian Partners Ltd.)

Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)

Graphic Artist: Julie Stone (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Patricia Rytkenon (The Write Stuff)

Copy Editor: Kaarin Dolliver (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: Eric Brandt (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Testing: Data Dimensions, Inc.

Production Support: Ed Casper (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes**Labs:**
30 Minutes

This module provides students with information about the Internet and how to securely access it from a Microsoft® Windows® 2000 network. The module begins with an introduction to the Internet, Internet services, intranets, and domain naming.

The module then describes common client technologies, such as newsreaders and Web browsers, and discusses Internet protocols and Uniform Resource Locators (URLs). At the end of this section, students will perform a lab to access an FTP site by using Microsoft Internet Explorer.

The module continues with a description of the methods for securely connecting to the Internet from a Windows 2000 network. The module concludes with a discussion of Web server concepts and the Microsoft Internet Information Services (IIS) software that is a part of the Windows 2000 operating system.

A lab in which students identify Web concepts follows the last section of the module.

At the end of this module, students will be able to:

- Describe the Internet, an intranet, the domain namespace, and a URL.
- Describe the different client technologies available for accessing information on the Internet.
- Describe the methods for securely connecting to the Internet from a Windows 2000 network by using network address translators (NATs), proxy servers, and firewalls.
- Explain how Web server technologies, such as IIS, can be used to host services on the Internet.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_09.ppt
- Module 9, “Examining Web Services”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- **Identifying Internet Concepts**
Introduce the structure of the Internet and mention that TCP/IP is used for communication over the Internet. Briefly describe the commonly used Internet services. Explain the concept of intranets and how they can be extended to form an extranet. Describe the need for domain names by using a suitable example.
- **Using Client Technologies**
Discuss common end-user tools, such as newsreaders and Web browsers, which are used to access information on the Internet. Explain the significance of Internet protocols for connecting to the Internet and introduce the concept of a Uniform Resource Locator (URL).
- **Connecting to the Internet**
Describe the methods for securely connecting to the Internet from a Windows 2000 network by using NATs, proxy servers, and firewalls. Emphasize that the Microsoft Proxy Server software can function as both a proxy server and a firewall. Mention to the students that Proxy Server is not a part of Windows 2000 but can be obtained separately.
- **Identifying Web Server Concepts**
Discuss Web server concepts and describe the features of IIS. Mention to the students that IIS is included with the Windows 2000 operating system.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

This module includes only computer-based interactive lab exercises, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about Internet concepts, end-user tools to access Internet information, and methods for securely connecting to the Internet and providing Web server content.

- Identifying Internet Concepts
- Using Client Technologies
- Connecting to the Internet
- Identifying Web Server Concepts

*****ILLEGAL FOR NON-TRAINER USE*****

Transmission Control Protocol/Internet Protocol (TCP/IP) enables communication between computers running Microsoft® Windows® 2000 and other operating systems, and in different network environments, including large internetworks. The largest of these internetworks is the Internet, which provides several services, called Web services. Web services use TCP/IP across large internetworks around the world. By accessing these Web services from a Windows 2000 network, you can search for information, share ideas and opinions, or communicate with other users who are connected to the Internet.

If you want to connect a Windows 2000 network to the Internet, you must first familiarize yourself with some of the basic concepts and terminologies related to Web services. You must also know which client technologies and end-user tools you can use to access the Web services. To access the Internet from a Windows 2000 network, you must also be familiar with the methods of connecting and securing access to the Internet. Finally, to host your own Web services, you must be aware of the server technologies available for providing information on the Internet.

At the end of this module, you will be able to:

- Describe the Internet, an intranet, the domain namespace, and a Uniform Resource Locator (URL).
- Describe the different client technologies available for accessing information on the Internet.
- Describe the methods for securely connecting to the Internet from a Windows 2000 network by using network address translators (NATs), proxy servers, and firewalls.
- Explain how Web server technologies, such as Microsoft Internet Information Services (IIS), can be used to host services on the Internet.

◆ Identifying Internet Concepts

Topic Objective

To introduce concepts, such as the Internet, intranet, domain namespace, and URL.

Lead-in

You must be able to understand such concepts as the Internet, intranets, domain namespaces, and URLs to access information on the Internet.

- The Internet
- Internet Services
- Intranets
- Domain Naming

*****ILLEGAL FOR NON-TRAINER USE*****

To understand the terminology and concepts involved with Web services, you should first become familiar with the structure of the Internet and the technologies deployed on it.

The technologies developed to host Internet services can also be deployed internally in an organization. You can do this by creating an intranet to maximize the advantages of Internet services within an organizational network.

You must also know how computers find, or address, other computers connected to the Internet to send information to them. Addressing of computers on the Internet is accomplished by using a user-friendly naming system called domain naming.

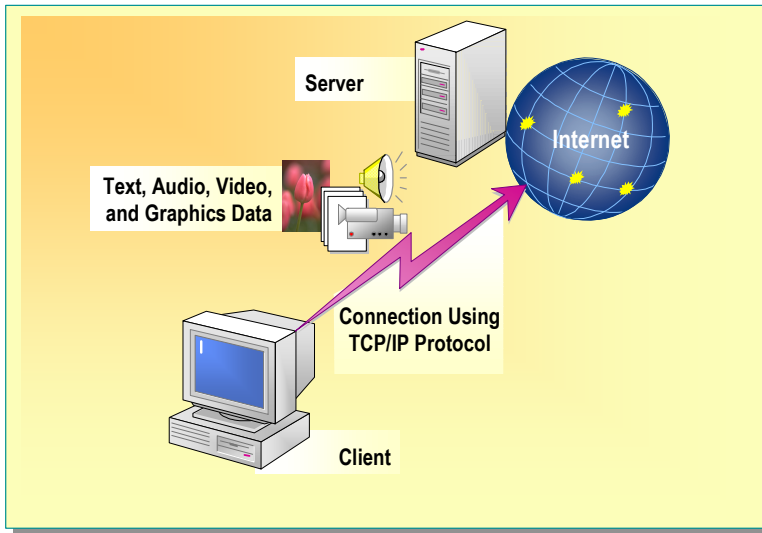
The Internet

Topic Objective

To illustrate the structure of the Internet, the protocol stack used for Internet communications, and private and public addresses.

Lead-in

The Internet is a global collection of networks that connects computer users around the world.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Do not spend much time discussing the Internet. Instead, emphasize to the students TCP's function as the underlying protocol stack, and the need for private IP addresses.

Many major companies, universities, and government agencies, as well as millions of individuals, place information on the Internet in order to share it with the public.

Structure of the Internet

Using the Internet, people all over the world can exchange information—text, word-processor documents, pictures, video, audio, and computer programs—over computers. Although specific organizations may develop tools or programs for the Internet, no individual or single organization controls or governs the Internet. However, private companies do own the Internet *backbone* (the physical media through which the Internet traffic flows).

Computers on the Internet use a client/server architecture. This means that a remote server provides files and services to the user's local client computer. The speed at which the client can access the services provided by the server depends upon the technology available. With continuous technological advancements, the access speeds and mechanisms are improving to allow large amounts of information to be quickly downloaded, or retrieved, from the server.

TCP/IP

TCP/IP is the standard protocol stack used for communication over the Internet. The TCP/IP protocol stack consists of the lower-level protocols TCP and IP and such higher-level protocols as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). TCP and IP provide the low-level functionality needed for many applications, whereas HTTP, FTP and SMTP give you access to higher-level services, such as transferring files between computers, sending e-mail, or identifying who is logged on at another computer. Therefore, because of its broad range of functions, you must install and configure TCP/IP on all computers accessing the Internet.

Public and Private Addresses

In addition to understanding how TCP/IP functions, you must also know how computers are assigned IP addresses for accessing the Internet. The Internet Assigned Numbers Authority (IANA) allocates IP addresses. The addresses allocated by IANA can receive traffic from Internet locations and are known as public addresses. For a typical small business or home office, public addresses are allocated by an *Internet service provider (ISP)*, which is a company that maintains a range of public addresses and offers access to the Internet.

For multiple computers in a small office or home office to communicate on the Internet, each computer must have its own public address. The demand for public addresses is greater than can be met by the limited supply of available public addresses. To overcome this shortfall in the supply of public addresses, IANA provides an address reuse system that reserves groups of IP addresses, called private addresses, for private networks connected to the Internet. Private addresses cannot directly receive traffic from Internet locations.

Internet Services

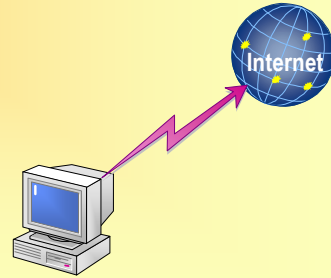
Topic Objective

To introduce the commonly used Internet services.

Lead-in

All Internet applications function by taking advantage of one or more of the basic Internet services.

- **Electronic Mail (e-mail)**
- **World Wide Web (WWW)**
- **Chat**
- **Internet News**
- **File Transfer Protocol (FTP)**
- **Telnet**



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Make sure that all students are familiar with the basic Internet services. The actual client applications will be mentioned later in this module.

Some of the most popular Internet services include electronic mail (e-mail), the World Wide Web (WWW), Chat, Internet News, File Transfer Protocol (FTP), and Telnet.

- **Electronic mail (e-mail)**

E-mail is the most popular service on the Internet. You can use it to send messages to any user connected to the Internet.

- **World Wide Web (WWW)**

The World Wide Web, or the Web, is a term used to describe the interlinked collection of hypertext documents and multimedia content available on the Internet. Hypertext documents are files that have been formatted for use on the Internet. You use a Web browser, such as Microsoft Internet Explorer, to search for, locate, view, and download information from the Internet.

- **Chat**

Chat programs allow you to participate in a real-time conversation with two or more people on the Internet.

- **Internet News**

Internet News is a service that hosts electronic discussion groups through which participants can share information and opinions. A news client, such as Microsoft Outlook® Express, can then be used to access these groups.

- **File Transfer Protocol (FTP)**

FTP is a service that includes a server for transferring files from the server to a client computer. Users can download files from the FTP server by using an FTP client utility.

- **Telnet**

Telnet offers a way to remotely log on to a computer and work on that computer. By logging on to this computer remotely, users can access services or resources that they may not have on their own workstation.

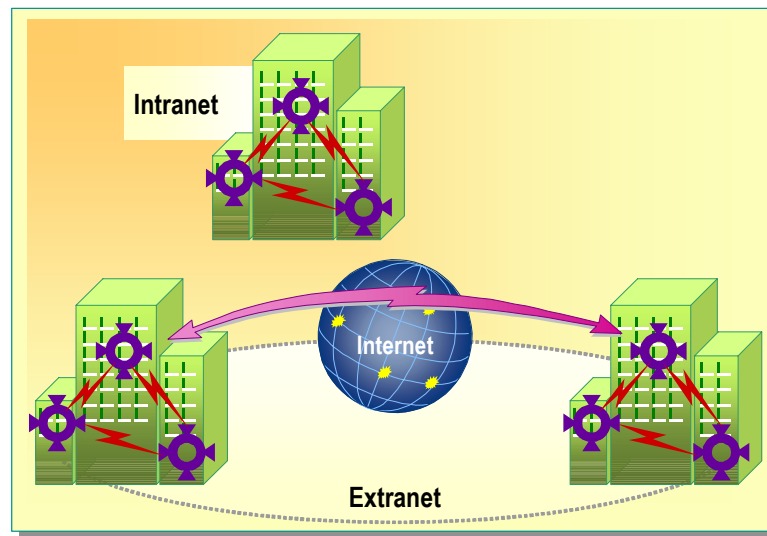
Intranets

Topic Objective

To illustrate an intranet and compare it with an extranet.

Lead-in

You can create an intranet site by installing Internet server software on any server on a LAN.



*****ILLEGAL FOR NON-TRAINER USE*****

You can deploy the technologies developed for the Internet on a local area network (LAN) to disseminate information, such as updates to a catalog or information from a database within the LAN. To do this, you must install Internet server software on one of the servers on the LAN.

What Is an Intranet?

An *intranet* is a network, internal to an organization, which uses Internet technology to improve internal communications, publish information, or develop applications. To use the free or relatively inexpensive Internet applications on an intranet, each of the computers on the intranet must support TCP/IP. An intranet may be private, in which case it is not connected to the Internet, or public, in which case it is connected to the Internet.

Extending Intranets to an Extranet

You may want to grant access to your intranet to authorized users from your customers, vendors, suppliers, or other partners. For example, a company may want to share business information with its vendors and customers by granting limited access to its intranet. You can use the Internet to extend intranet access to authorized users. Such an intranet that is partially accessible to only authorized users through the Internet, or through other means, is called an extranet. Setting up an extranet through the Internet is easier and more economical than setting up a dedicated communication link between two companies. However, an extranet is less secure than a private intranet because it allows possible access by unauthorized users.

Domain Naming

Topic Objective

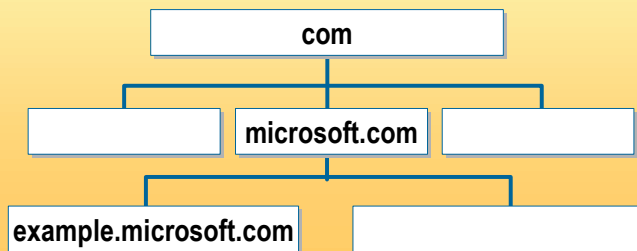
To introduce the concept of domain naming.

Lead-in

A domain name specifies an easy-to-remember name for Internet addresses.

■ Domain Name (example.microsoft.com)

- Top-level domain (com)
- Second-level domain (microsoft.com)
- Subdomain (example.microsoft.com)



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

This page is not intended to show students the DNS query process but to introduce the concept of DNS and specifically the format used by DNS. Remind the students that the IP address is what is actually used to locate a specific computer on the Internet.

With millions of computers on the Internet, there is an obvious need for an addressing system that provides an easy-to-remember method for locating computers. A domain name, which uses user-friendly names instead of long numbers, meets this need.

Domain Names

The address that is used at the computer level to uniquely identify a specific computer on the Internet is called the Internet Protocol (IP) address. An IP address consists of four sets of numbers, separated by periods, for example: 131.107.1.7 or 131.107.1.240.

Although a computer application has no difficulty with this numerical addressing system, people find it easier to remember user-friendly domain names, such as example.microsoft.com. However, before a computer can connect to the Internet, its domain name must be mapped, or resolved, to a unique IP address. A classification system called the Domain Name System (DNS) maps domain names to IP addresses. When you use a domain name to connect to a computer on the Internet, a DNS server resolves the name to an IP address. The server uses the mapping to locate the target computer's IP address and substitute it for the user-friendly name to connect to the computer on the Internet.

DNS uniquely identifies computers connected to the Internet based on a hierarchy that includes a top-level domain, a second-level domain, and often one or more subdomains. The top-level domain is based either on generic codes or country codes. Generic top-level domains indicate the type of organization. This table lists the generic top-level domains and their corresponding organizations.

Generic code	Description
com	Commercial organizations
edu	Educational institutions
gov	Government agencies
int	International associations
mil	Military organizations
net	Major network support centers
org	Other organizations

Country code top-level domains are two-letter codes, such as US for the United States and CA for Canada. This table provides examples of some country code domains and their corresponding countries.

Country code	Country
ar	Argentina
au	Australia
be	Belgium
br	Brazil
fr	France
de	Germany

The second-level domain represents the name of a company, institution, or organization and is separated from the top-level domain by a period (called “dot”). An example of a second-level domain is microsoft.com. An individual or a small company typically use one domain name and one IP address, but large companies often acquire a block of IP addresses and establish subdomains. For example, microsoft.com is a domain name, and example.microsoft.com is a subdomain of the main Microsoft domain.

The Internet Corporation for Assigned Names and Numbers (ICANN) manages the assignment of domain names.

◆ Using Client Technologies

Topic Objective

To introduce the client technologies available for accessing information on the Internet.

Lead-in

You can use Web browsers, Internet protocols, and newsgroups to access information on the Web.

- **Newsreaders**
- **Web Browsers**
- **Internet Protocols**
- **Uniform Resource Locator (URL)**

*****ILLEGAL FOR NON-TRAINER USE*****

The Internet was originally created for sharing scientific and educational research information. However, users found that accessing the information available from laboratories and universities required a number of complicated steps and did not use a standard interface.

Today, many client technologies are available for easy access to information on the Internet. With Windows 2000, these common end-user tools include:

- **Newsreaders**

Newsreaders enable you to access and join online discussion groups on the Internet. You can even obtain support information for running Windows 2000 by subscribing to Windows 2000-related discussion groups.

- **Web browsers**

Web browsers enable you to browse the Internet, send and receive e-mail messages, and display Internet content.

There are many Internet protocols, such as HTTP, HTTPS, FTP, NNTP, and SMTP, which are used to communicate with other computers connected to the Internet.

In addition to addressing computers connected to the Internet, you can also locate any file on a computer on the Internet. You can do this by using a file-addressing system called the Uniform Resource Locator (URL).

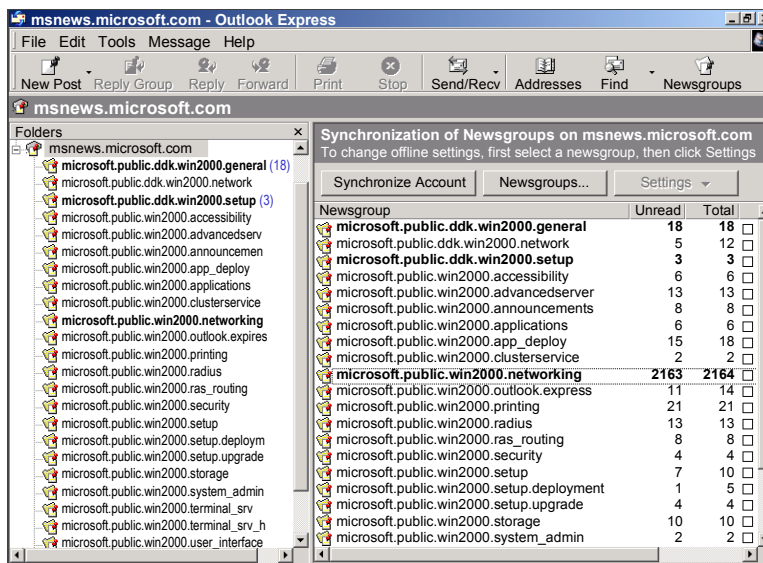
Newsreaders

Topic Objective

To describe a newsgroup and demonstrate how to use a newsreader.

Lead-in

You can exchange opinions about any conceivable interest on the Internet by using a newsreader to access various newsgroups.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Many students will be familiar with Outlook Express. Use this page to point out the usefulness of newsgroups, specifically msnews, to locate information about administering a network.

Internet News, or *Usenet*, is a popular Internet service. Usenet is a worldwide news service that you can access through the Internet. It is a 24-hour-a-day service that includes a bulletin board system (BBS) and chat rooms, as well as thousands of electronic discussion groups called *newsgroups*.

A newsgroup, also called a forum, is an online discussion group. On the Internet, thousands of newsgroups reflect the many interests and activities of their users. Online services and the bulletin board system also provide a variety of forums in which participants who share common interests can exchange messages.

There are three types of newsgroups: Usenet, public news servers, and private news servers.

■ Usenet

A huge collection of open discussion groups on a variety of topics.

■ Public news servers

Newsgroups, such as msnews, which provide specific content and are open to the public.

■ Private news servers

Newsgroups that provide specific content but are not open to the public. These newsgroups require a password to access them.

What is a Newsreader?

To view and post messages, many people use a *newsreader*, which is an application that connects you to a news server on the Internet. After obtaining a newsreader, you can subscribe to newsgroups that focus on subject matter of interest to you. When you subscribe to a newsgroup, you can download some or all articles from the news server or you can post your own opinions and responses to the opinions of others.

msnews.microsoft.com

Internet newsgroups, intranet newsgroups, and bulletin boards use Network News Transfer Protocol (NNTP) to post, distribute, and retrieve messages on the Internet. The Microsoft news server addresses customer demand for a single location to access information and services over the Internet. Any newsreader can access Microsoft-sponsored newsgroups.

The Microsoft-sponsored newsgroups offer peer-to-peer interaction on the Internet. A common news server is msnews.microsoft.com. To access the newsgroups on this server, configure your newsreader to connect to msnews.microsoft.com. No user name or password is required to access this server.

Microsoft Outlook Express News

You can use Microsoft Outlook Express News to gain access to bulletin board discussion groups, such as Usenet, by using NNTP-based news servers. Outlook Express News can also be used to receive technical support information for a variety of Microsoft products from the msnews.microsoft.com news server.

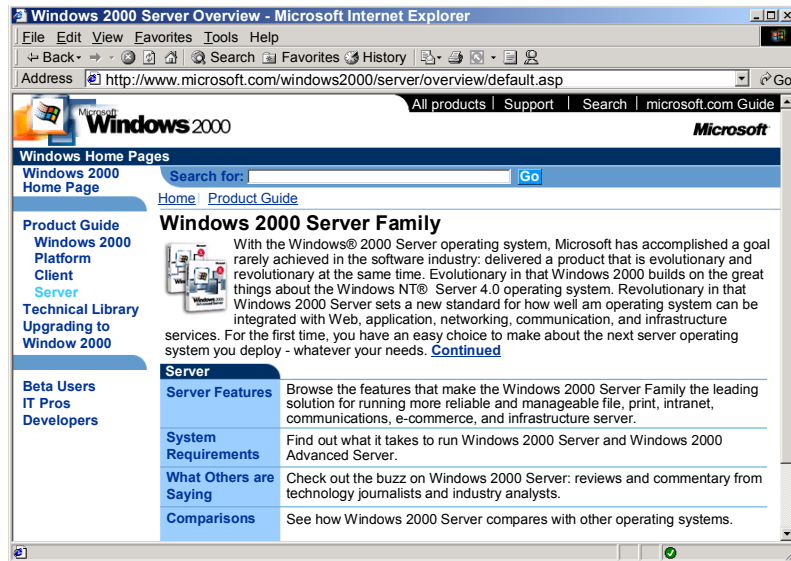
Web Browsers

Topic Objective

To introduce the functions of a Web browser by demonstrating a Web browser window.

Lead-in

A Web browser enables you to access information from the Web by using the HTTP protocol.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Students should already be familiar with Internet Explorer. Use this page to point out the advisability of using the Web to find product support information and product updates. Also point out that Internet Explorer can connect to FTP servers as well.

The World Wide Web (WWW), or Web, is the portion of the Internet that provides links to graphical content. The Web has developed into a network of interactive documents that you can easily locate and read using various Web browsers, such as Internet Explorer.

A Web browser is a client application that enables the client computer to gain access to a Web server or other server, such as an FTP server, running on the Internet. Web browsers can display text files and various graphic and multimedia format files. A browser also interprets and displays documents.

Methods of Locating Information on the Web

One of the most common uses of a Web browser is to locate information. You can use either of two methods—search engines or portals—to locate information on the Web.

■ Search engines

To reduce time spent browsing Web sites for information, many sites offer *search engines*, tools for finding specific information on the Web. Most sites allow you to conduct a search by using an advanced feature that exists in most search engines.

- Portals

A *portal* is a Web site that offers a broad array of resources and services, such as e-mail messages, forums, search features, and on-line shopping sites. Using a portal to locate information is easier than using a search engine because the information is sorted and arranged in advance. Portals are good places to begin a search and often categorize sites by type, which further helps people search and navigate Web sites.

Microsoft Internet Explorer

Microsoft Internet Explorer is one of the commonly used Web browsers and is available with Windows 2000. You can use Internet Explorer to browse the Internet, search for information, and even connect to an FTP site.

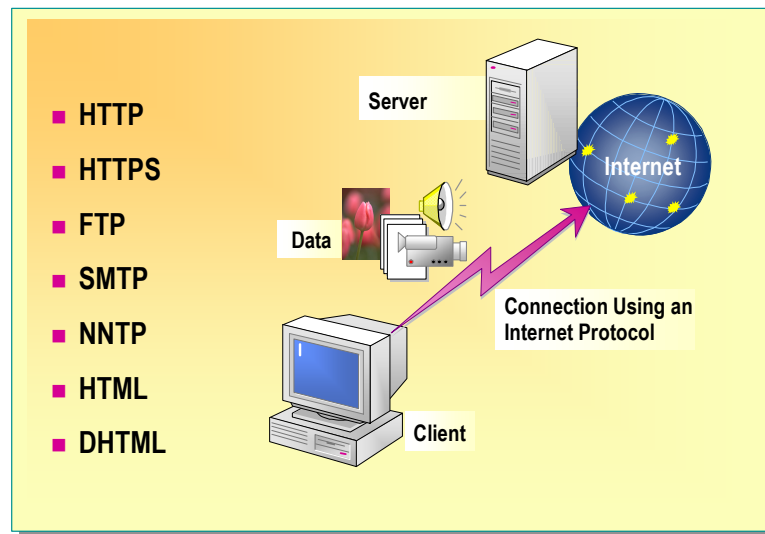
Internet Protocols

Topic Objective

To introduce the protocols used for communication over the Internet.

Lead-in

You can use different protocols to communicate over the Internet.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Compare the various protocols used on the Internet. Point out that the last two protocols are simply formatting protocols used on the Web.

Common Internet protocols that enable you to access the Internet are Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP). In addition, Hypertext Markup Language (HTML) and Dynamic HTML (DHTML) specify the formats of pages displayed on the Web.

■ HTTP

HTTP is a convention for sending messages from a server to a client by using TCP/IP. HTTP communications are in plain text and not encrypted.

■ HTTPS

HTTPS enables you to make a secure Web server connection by using Secure Sockets Layer (SSL). SSL is an encryption technology that enables a secure connection between a server and a client. The URLs for Web pages that require an SSL connection start with `https://`.

■ FTP

FTP enables you to transfer files between two computers on a network.

■ SMTP

SMTP enables you to send e-mail over the Internet.

- NNTP

NNTP enables you to post, distribute, and retrieve messages on Internet and intranet newsgroups.

- HTML

HTML is the standard language for creating and formatting Web pages.

HTML defines how text appears when viewed in a Web browser.

- DHTML

DHTML refers to HTML extensions that support animations and enable you to create interactive Web pages.

Uniform Resource Locator (URL)

Topic Objective

To introduce the concept of a URL.

Lead-in

A URL specifies a unique address for files on a computer connected to the Internet.

■ URL (<http://example.microsoft.com/tutorial/default.html>)

- Protocol used (<http://>)
- DNS address (example.microsoft.com)
- Path on the server ([/tutorial/default.html](http://example.microsoft.com/tutorial/default.html))

<http://example.microsoft.com/tutorial/default.html>

*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

The Tip at the bottom of the page mentions that URLs are not case-sensitive on a Windows 2000-based server. This is true only when the Web site you are accessing is on a Windows 2000-based server and not if you are accessing a Web site from a Windows 2000-based server.

Although a domain name provides a convenient way of referring to a specific computer on the Internet, you rarely want to just connect to a computer. More often, you want to retrieve information from a file on the computer. To access a file on a computer connected to the Internet, you must know the path to that file, known as its address. The addressing system developed for this purpose is called a Uniform Resource Locator (URL).

What is a Uniform Resource Locator (URL)?

A URL specifies a unique address for each file stored on a computer that is connected to the Internet. An example of a URL is:

<http://example.microsoft.com/tutorial/default.html>

The first part of the URL ([http](http://)) corresponds to the particular protocol you are using, such as HTTP, HTTPS, or FTP. The second part of the URL (example.microsoft.com) corresponds to a domain name or DNS address, which is translated into a numeric IP address when a request to transmit data is sent.

The information to the right of the domain name in the URL ([/tutorial/default.html](http://example.microsoft.com/tutorial/default.html)) is the path to the actual resource and includes the name and type of file you want to display or retrieve. This path is similar to the path to a file on your computer. If the path is omitted, the server normally provides a default response based on the protocol used. For example, the default response to an HTTP request may be to display the file named `Index.html` or `Default.html`.

Tip Some URLs are case-sensitive. The first part of the URL is not case-sensitive, but path and file name information may be case-sensitive on some computer operating systems. So, if a URL does not seem to work, verify that you typed it in the same case as it was given to you. However, all URLs are not case-sensitive on a Windows 2000-based server.

Lab A: Accessing an FTP Site by Using Internet Explorer

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will access an FTP site by using Internet Explorer.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Use a Uniform Resource Locator (URL) to locate information on the Internet by using Internet Explorer.
- Use Internet Explorer to access an FTP site.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how to log on to Windows 2000.

Lab Setup

To complete this lab, you need the name of the instructor's FTP server.

Estimated time to complete this lab: 15 minutes

Exercise 1

Accessing an FTP Site by Using Internet Explorer

Scenario

You are an administrator responsible for updating client computers with the most recent drivers. You need to download both the video and network adapter files from the corporate FTP site.

Goal

In this exercise, you will use Internet Explorer to connect to an FTP site and download files to your local computer.

Tasks	Detailed Steps
1. Log on as Administrator with a password of password , and then download both files from the FTP server located at london.nwtraders.msft. Log off when you are finished.	- Log on to Windows 2000 as Administrator with a password of password. - On the desktop, double-click the Internet Explorer icon.
 Which protocol in the URL is used to connect to the page that opens by default in Internet Explorer? http. 	
 Which protocol in the URL will you use to connect to an FTP site? ftp. 	
1. (continued)	- Type ftp://london.nwtraders.msft in the Address bar, and then press ENTER. - Open the Drivers folder. - Right-click the Nadriver.zip file, and then click copy to folder.  <i>The Browse for Folder dialog box appears.</i> - In the console tree, expand My Computer, Local Disk (C:) , Moc, 2151A, Labs, and Lab09, and then click OK. - Right-click the Videodriver.zip file, and then click copy to folder. - In the console tree, expand My Computer, Local Disk (C:) , Moc, 2151A, Labs, and Lab09, and then click OK. - Close all windows and log off from Windows 2000.

◆ Connecting to the Internet

Topic Objective

To introduce the physical components used to securely connect your network to the Internet.

Lead-in

Network security is an important consideration when connecting your network to the Internet.

- **Network Address Translators (NATs)**
- **Proxy Servers**
- **Firewalls**
- **Microsoft Proxy Server**

*****ILLEGAL FOR NON-TRAINER USE*****

It is important to consider network security when connecting your Windows 2000 network to the Internet. When a user connects to the Internet, other computers can access the user's computer, which increases the possibility of unauthorized access by other users. In a private intranet, however, security threats are reduced because a private intranet is internal to an organization and is not easily accessible to the public. The physical components used to securely connect a network to the Internet include network address translators (NATs), proxy servers, and firewalls.

- *Network address translators (NATs)*. Enable you to configure a home or small office network to share a single connection to the Internet.
- *Proxy servers*. Replace the private IP addresses of the computers sending requests to an Internet server with the public IP addresses assigned by an ISP to the proxy servers.
- *Firewalls*. Act as security barriers between an intranet and the Internet to guard against intrusion by unauthorized users.

Microsoft implements both a proxy server and a firewall in a single product, the Microsoft Proxy Server.

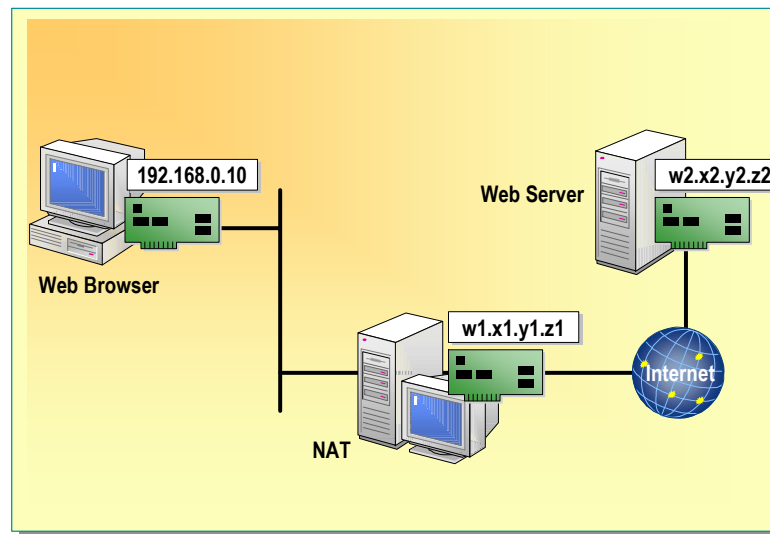
Network Address Translators (NATs)

Topic Objective

To introduce the role of NATs in Internet communications.

Lead-in

NATs enable intranets to connect to the Internet by translating the private addresses used by intranets to public addresses and vice versa.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

NAT officially stands for Network Address Translator, however many sources also use NAT to represent Network Address Translation.

Private addresses cannot receive traffic from Internet locations. Therefore, to enable a network, which uses private addresses internally, to communicate with Internet locations, you must use a *network address translator (NAT)*. The NAT is a device, or service, that translates private IP addresses to public IP addresses. Network address translation is an Internet standard that enables a public intranet to use a set of private IP addresses for internal traffic and to connect to a computer that uses a public IP address for external traffic.

How Does a NAT Work?

The NAT is a router that is placed between a public intranet, which uses private IP addresses, and the Internet, which uses public IP addresses. The NAT translates the private IP addresses of outgoing packets into public IP addresses. It also translates the public IP addresses of incoming packets from the Internet into private IP addresses.

NATs serve two main purposes:

- Increase security by hiding internal IP addresses
- Enable an organization to require fewer public IP addresses

Windows 2000 NAT Services

Microsoft Windows 2000 includes NAT services that enable you to configure your home network or small office network to share a single connection to the Internet.

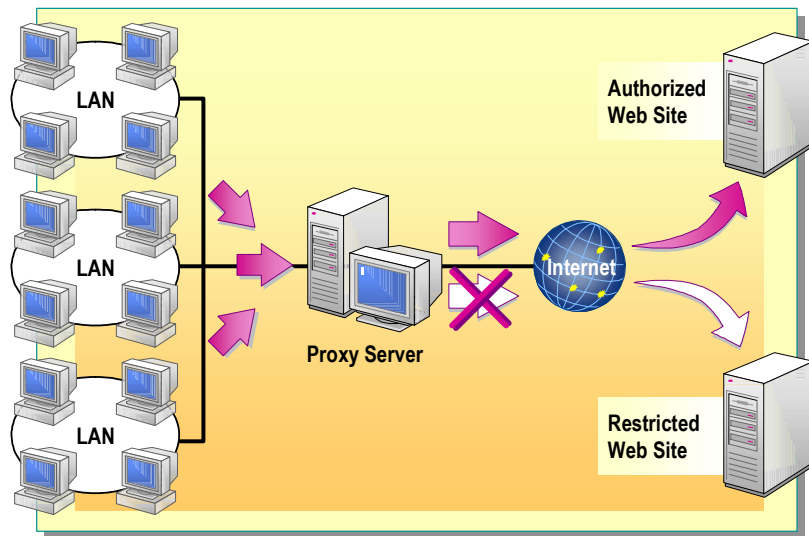
Proxy Servers

Topic Objective

To illustrate the role of a proxy server in connecting to the Internet.

Lead-in

A proxy server enables you to connect multiple users to the Internet by using a single IP address.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Point out to the class that in this topic you will be discussing the concept of a proxy server in general, not the Microsoft Proxy Server software specifically. Note that a proxy server is more robust than a NAT.

Use the slide to explain that a proxy server can be used to prevent users in a Windows 2000 network from accessing restricted Web sites.

Most home and small office networks use a dial-up or modem network connection to an ISP, which in turn connects them to the Internet. The ISP assigns a single IP address to each network for connecting to the Internet. In addition, each computer in a network requires an IP address for Internet connection. Rather than using separate IP addresses for each computer, it is more cost-effective to use a single IP address for multiple computers. A *proxy server* is a firewall component that enables you to connect multiple computers in a network to the Internet by using a single IP address.

Proxy servers have two main functions: to improve network performance and filter client requests.

■ Improve performance

Proxy servers reduce the time it takes to respond to requests made by groups of users. This is because a proxy server caches, or saves, the results of all requests made during an interval of time. If a user wants to redisplay a Web page that was requested earlier, the proxy server simply returns that page to the user rather than forwarding the request to the Web server and downloading the page again.

■ Filter client requests

Proxy servers can also be used to filter client requests for certain Internet connections. For example, a company can use a proxy server to prevent its employees from accessing a specific set of Web sites.

How Does a Proxy Server Work?

When using a proxy server, the computers on the local network are configured for private IP addresses. When a computer makes a request to connect to the Internet, the computer passes its data through the TCP/IP network to the proxy server. The proxy server modifies the request, inserts its own name and IP address, which was provided by the ISP, and sends the data out on the Internet. When a response to the request is received, the proxy server passes it back through the local network to the computer that initiated the request.

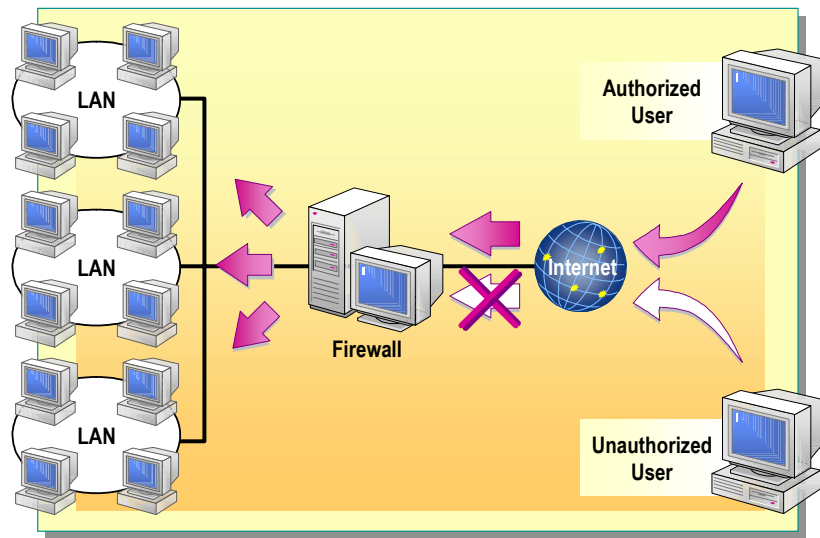
Firewalls

Topic Objective

To illustrate how firewalls function.

Lead-in

Firewalls prevent unauthorized access to a private network.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the graphics slide to explain that a firewall can be used to restrict access to a network by unauthorized users.

Any network that is connected to the Internet should pass communication through a *firewall*. A firewall is a combination of hardware and software that prevents unauthorized access to an internal network from outside. All messages entering or leaving a network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A firewall filters out traffic that should not pass between the Internet and your private network, such as messages between two computers within your private network.

How Does a Firewall Work?

A firewall prevents direct communication between network and external computers by routing communication through a proxy server located outside of the network. The firewall determines if it is safe to let a file pass to the network and from the network. A firewall is also called a security-edge gateway.

Note A gateway is a system that is connected to multiple physical TCP/IP networks and is capable of routing or delivering IP packets between them. A gateway translates between different transport protocols or data formats, such as IPX and IP, and is added to a network primarily for its translating ability.

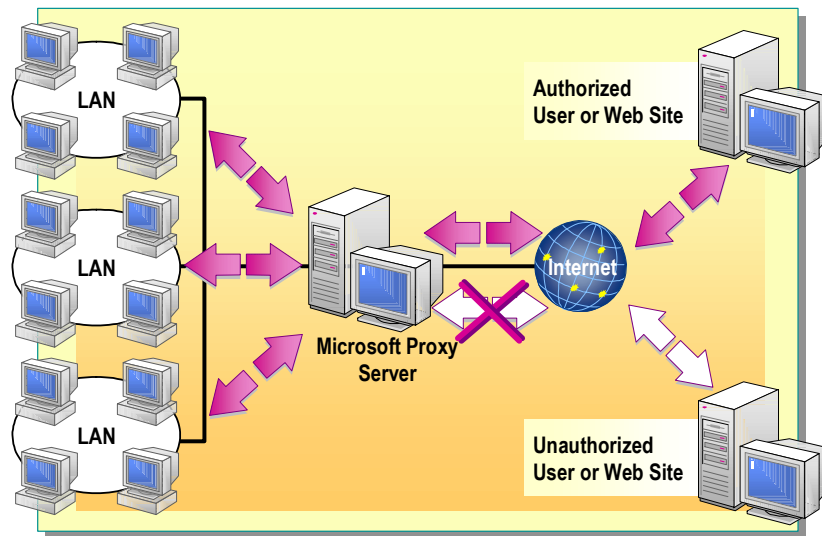
Microsoft Proxy Server

Topic Objective

To introduce Microsoft Proxy Server.

Lead-in

Microsoft Proxy Server enables users to access the Internet from a secured local area network (LAN).



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Use the slide to explain that Microsoft Proxy Server can be used to prevent users in a network from accessing restricted Web sites, as well as to deny unauthorized users access to a private network.

Microsoft provides software that combines the features of a proxy server and a firewall into a single product, Microsoft Proxy Server.

How Does Microsoft Proxy Server Work?

Microsoft Proxy Server acts as a secure gateway between your LAN and the Internet. A gateway enables two different networks to communicate. Proxy Server provides a connection to the Internet for your group, division, or your entire intranet. Proxy Server also acts as a secure gateway and a firewall by allowing inbound access from the Internet to your network.

By using a Proxy Server gateway, you can secure your network against intrusion. Proxy Server enables you to make requests to the Internet and to receive information, but it prevents unauthorized users from accessing your network.

You can configure Proxy Server to enable your workstations to communicate with remote services on the Internet. To do this, you select the appropriate hardware for Proxy Server, making sure that you have adequate bandwidth for the Internet connection, and choose the level of security at which you want to protect your LAN.

Note Microsoft Proxy Server is not a part of the Windows 2000 operating system.

◆ Identifying Web Server Concepts

Topic Objective

To introduce such concepts as Web servers and Internet Information Services.

Lead-in

You can set up a Web server to host your own Web site.

- **Defining a Web Server**
- **Microsoft Internet Information Services (IIS)**

*****ILLEGAL FOR NON-TRAINER USE*****

You can host your own Web services on the Internet by setting up a Web site. However, to set up your own Web site on the Internet, you must be familiar with the server technologies and methods available for providing content on the Internet.

Microsoft Internet Information Services (IIS) is a common software that enables you to provide content on the Internet. Using IIS, it is possible to provide services, such as Web pages, interactive applications, and catalogs for customers, and to post and track databases on the Web.

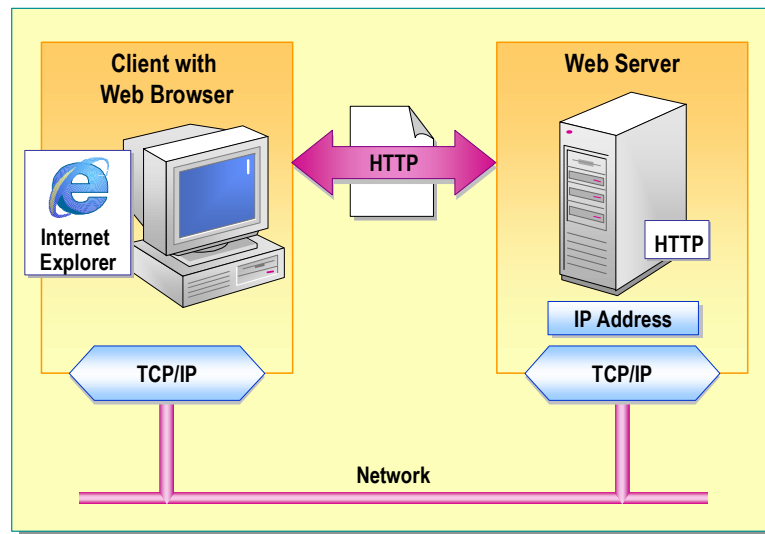
Defining a Web Server

Topic Objective

To define a Web server.

Lead-in

A Web server is a computer that sends Web page content to the client computers requesting it.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

The terms Web server and HTTP server are synonymous because URLs that identify data on a Web server begin with http.

A client computer connects to the Internet or an intranet by using a Web browser to find information stored and organized on a *Web server*.

A Web server is a computer that uses TCP/IP to send Web page content to client computers over a network. A Web server communicates with clients by using an appropriate protocol, such as HTTP or HTTPS. The terms Web server and HTTP server are synonymous, because URLs identifying data on a Web server begin with http. For example, the Microsoft Web site is <http://example.microsoft.com/>.

Every Web server has an IP address and perhaps a domain name. For example, when you enter the URL <http://example.microsoft.com/webpage.htm> in your Web browser, it sends a request to the Web server with the domain name microsoft.com. Then the Web server locates and retrieves the page ms.htm, and sends it to your browser.

Microsoft Internet Information Services (IIS)

Topic Objective

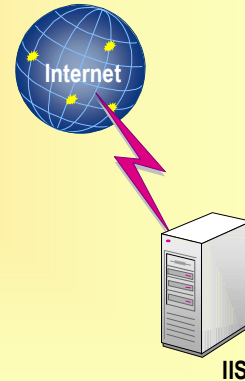
To introduce the features of IIS.

Lead-in

IIS is network file and application server software that uses HTTP and FTP to provide information over the Internet or over an intranet.

Features of IIS

- **Indexing Service**
- **Secure Sockets Layer**
- **Windows Media Services**
- **Additional Developer Support**
 - Active Server Pages
 - VBScript and JavaScript support
 - Remote administration



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

IIS provides HTTP, FTP, NNTP, and SMTP services. Note that HTTPS is supported as well but is considered a part of HTTP.

Windows 2000 includes Microsoft Internet Information Services (IIS), a network file and application server service that uses HTTP, FTP, NNTP, and SMTP to provide information over the Internet or an intranet.

IIS provides many useful features, including Microsoft Indexing Service, Secure Sockets Layer (SSL) support, Microsoft Windows Media Services, and additional developer support.

Indexing Service

Microsoft Indexing Service is a search engine that is integrated with IIS. When you install Indexing Service, it builds an index of files on the Web server. You can then search this index by using any Web browser with built-in search forms. The index is updated automatically whenever a file is added, deleted, or changed on the Web server.

Secure Sockets Layer (SSL)

IIS supports Secure Sockets Layer (SSL), which provides a security handshake between the Web server and a client before initiating a TCP/IP connection. This handshake establishes the level of security the client and Web server use and fulfills any authentication requirements for the connection. SSL also enables you to encrypt all of the information sent between the client and the Web server. HTTPS is a version of the HTTP protocol that uses SSL to secure communications between a Web server and clients.

Windows Media Services

IIS includes Microsoft Windows Media Services. Windows Media Services is a specification that enables Internet users to download live video, audio, and animation files from Web pages. It is a standards-based platform that delivers on-demand and live content for enhanced communication over the Internet.

Additional Developer Support

IIS provides additional developer support for Active Server Pages, scripting languages, such as VBScript and JavaScript, and remote administration using Microsoft FrontPage®.

- Active Server Pages (ASP) is an open environment in which developers can combine HTML and programming to create dynamic and powerful Web sites. The creation of dynamic content for Web pages is made possible by providing users with live access to a local database containing the latest information.
- VBScript and JavaScript are two of the scripting languages that developers commonly use to create dynamic Web pages. The content of such Web pages changes based on user interaction or input. For example, a Web site that requires a valid user name and access password returns different pages based on whether or not the user enters a correct user name and password.
- IIS enables developers to remotely administer Web pages by using Microsoft FrontPage, a visual authoring and Web-site management tool.

Lab B: Identifying Web Concepts

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will demonstrate your knowledge of Web concepts and terminology.



*****ILLEGAL FOR NON-TRAINER USE*****

Objectives

After completing this lab, you will be able to:

- Demonstrate your knowledge of Web concepts and terminology.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- Microsoft Internet Explorer 5 or higher.
- A minimum display resolution of 800 x 600 with 256 colors. Recommended display resolution of 800 x 600 with high color (16-bit).

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Web Concepts**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 15 minutes

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Identifying Internet Concepts**
- **Using Client Technologies**
- **Connecting to the Internet**
- **Identifying Web Server Concepts**

*****ILLEGAL FOR NON-TRAINER USE*****

1. You want to register a domain name for use on the Internet. What is a valid example of a domain name that could be used to communicate on the Internet?

example.microsoft.com.

2. You want to use a Web browser and an Internet-based application, such as a newsreader, to improve the sharing of information on your local network. Which protocol stack do you need to install before using these applications?

TCP/IP.

3. You want to find information on the Internet by using a Web browser. What must you type in the Web browser's Address bar to access a particular site? Which three pieces of information are included in the information you've typed?

A URL that includes the protocol used to connect to the Internet, the domain name, and the path to the file you want to download.

4. You want to reduce the number of public IP addresses you are leasing from an ISP. What can you install that will enable you to use private IP addresses for your internal network and still maintain connectivity with the Internet?

You can install either a NAT or a proxy server.

5. You want to create a Web site that allows your customers to view all of your products on the Internet. You also want your customers to be able to communicate online to share suggestions about using your products. What can you use to enable both HTTP and NNTP access to a computer on your network?

IIS.

Course Evaluation

Topic Objective

To direct students to a Web site to complete a course evaluation.

Lead-in

Go to the Web site listed on this page to complete a course evaluation.



*******ILLEGAL FOR NON-TRAINER USE*******

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

To complete a course evaluation, go to
<http://www.metricsthatmatter.com/survey>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.