CISCO.

CCNA Exam Preparation

CCNA ICND2

Official Exam Certification Guide

Second Edition

- ✔ Master **ICND2 640-816** and **CCNA 640-802** exam topics with the official study guide
- ✔ Assess your knowledge with **chapter-opening quizzes**
- ✔ Review key concepts with **Exam Preparation Tasks**
- ✔ Practice with **hundreds of exam questions** on the CD-ROM

Includes Video Training

ciscopress.com

Wendell Odom, CCIE® No. 1624

CCNA ICND2 Official Exam Certification Guide, Second Edition

Wendell Odom

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

Seventh Printing September 2009

Library of Congress Cataloging-in-Publication Data:

Odom, Wendell.

CCNA ICND2 official exam certification guide / Wendell Odom. -- 2nd ed.

p. cm.

ISBN 978-1-58720-181-3 (hbk : CD-ROM)

1. Electronic data processing personnel--Certification. 2. Computer network protocols--Study guides. 3. Internetworking (Telecommunication)--Study guides. I. Title.

QA76.3.O3618 2004

004.6--dc22

2007029471

ISBN-13: 978-1-58720-181-3

ISBN-10: 1-58720-181-x

Warning and Disclaimer

This book is designed to provide information about the Cisco ICND1 (640-822), ICND2 (640-816), and CCNA (640-802) exams. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact:
International Sales
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: David Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Development Editor: Andrew Cupp

Senior Project Editor: Meg Shaw and Tonya Simpson

Editorial Assistant: Vanessa Evans

Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Ken Johnson

Cisco Representative: Anthony Wolfenden

Cisco Press Program Manager: Jeff Brady

Copy Editors: Written Elegance and Gayle Johnson

Technical Editors: Teri Cook and Steve Kalman

Proofreader: Susan Eldridge

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Foreword

CCNA ICND2 Official Exam Certification Guide, Second Edition, is an excellent self-study resource for the CCNA ICND2 exam. Passing the ICND2 exam validates the knowledge and skills required to successfully install, operate, and troubleshoot a small- to medium-size enterprise branch network. It is one of two exams required for CCNA certification.

Gaining certification in Cisco technology is key to the continuing educational development of today's networking professional. Through certification programs, Cisco validates the skills and expertise required to effectively manage the modern enterprise network.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in your field of expertise, or to gain new skills. Whether used as a supplement to more traditional training or as a primary source of learning, these materials offer users the information and knowledge validation required to gain new understanding and proficiencies.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco, and they offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope that you find these materials to be an enriching and useful part of your exam preparation.

Erik Ullanderson
Manager, Global Certifications
Learning@Cisco
August, 2007

Introduction

Congratulations! If you're reading far enough to look at the introduction to this book, you've probably already decided to go for your Cisco certification. If you want to succeed as a technical person in the networking industry, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than 80 percent market share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense.

Historically speaking, the first entry-level Cisco certification has been the Cisco Certified Network Associate (CCNA) certification, first offered in 1998. The first three versions of the CCNA certification (1998, 2000, and 2002) required that you pass a single exam to become certified. However, over time, the exam kept growing, both in the amount of material covered and in the difficulty level of the questions. So, for the fourth major revision of the exams, announced in 2003, Cisco continued with a single certification (CCNA), but offered two options for the exams to get certified: a single-exam option and a two-exam option. The two-exam option allowed people to study roughly half of the material, and take and pass one exam, before moving on to the next.

Cisco announced changes to the CCNA certification and exams in June 2007. This announcement includes many changes, most notably:

- The exams collectively cover a broader range of topics.
- The exams increase the focus on proving the test taker's skills (as compared with just testing knowledge).
- Cisco created a new entry-level certification: the Cisco Certified Entry Network Technician (CCENT) certification.

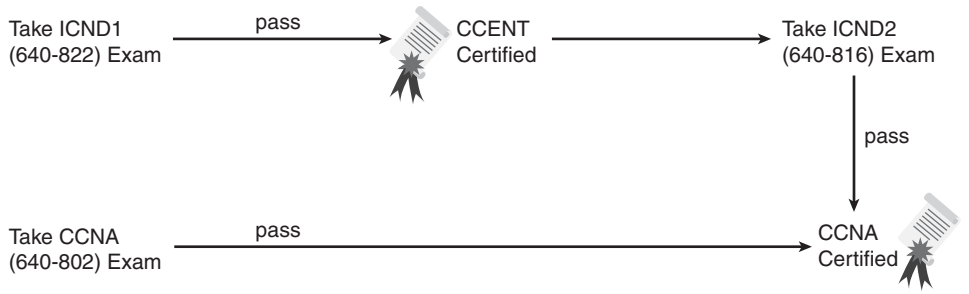
For the current certifications, announced in June 2007, Cisco created the ICND1 (640-822) and ICND2 (640-816) exams, along with the CCNA (640-802) exam. To become CCNA certified, you can pass both the ICND1 and ICND2 exams, or just pass the CCNA exam. The CCNA exam simply covers all the topics on the ICND1 and ICND2 exams, giving you two options for gaining your CCNA certification. The two-exam path gives those people with less experience a chance to study for a smaller set of topics at a time, whereas the one-exam option provides a more cost-effective certification path for those who want to prepare for all the topics at once.

Although the two-exam option will be useful for some certification candidates, Cisco designed the ICND1 exam with a much more important goal in mind. The CCNA certification has grown to the point that it tested knowledge and skills beyond what an

entry-level network technician would need to have. Cisco needed a certification that was more reflective of the skills required for entry-level networking jobs. So, Cisco designed its Interconnecting Cisco Networking Devices 1 (ICND1) course, and the corresponding ICND1 640-822 exam, to include the knowledge and skills most needed by an entry-level technician in a small enterprise network. And to show that you have the skills required for those entry-level jobs, Cisco created a new certification, CCENT, which is attained by passing the ICND1 exam.

Figure I-1 shows the basic organization of the certifications and the exams used for getting your CCENT and CCNA certifications. (Note that no separate certification exists for passing the ICND2 exam.)

Figure I-1 *Cisco Entry-Level Certifications and Exams*



As you can see from the figure, while the CCENT certification is available by taking the ICND1 exam, you do not have to first be CCENT certified before getting your CCNA certification—you can choose to just take the CCNA exam and bypass the CCENT certification.

The ICND1 and ICND2 exams cover different sets of topics, with a minor amount of overlap. For example, ICND1 covers IP addressing and subnetting, while ICND2 covers a more complicated use of subnetting called variable-length subnet masking (VLSM), so ICND2 must then cover subnetting to some degree. The CCNA exam covers all the topics covered on both the ICND1 and ICND2 exams.

While the popularity of the CCENT certification cannot be seen until a few years have passed, certainly the Cisco CCNA certification enjoys a position as the most popular entry-level networking certification program. A CCNA certification proves that you have a firm foundation in the most important components of the Cisco product line—namely, routers and switches. It also proves that you have a broad knowledge of protocols and networking technologies.

Format of the CCNA Exams

The ICND1, ICND2, and CCNA exams all follow the same general format. When you get to the testing center and check in, the proctor will give you some general instructions and then take you into a quiet room with a PC. When you're at the PC, you have a few things to do before the timer starts on your exam. For example, you can take a sample quiz, just to get accustomed to the PC and to the testing engine. Anyone who has user-level skills in getting around a PC should have no problems with the testing environment. Additionally, Chapter 18, "Final Preparation," points to a Cisco website at which you can see a demo of the Cisco test engine.

When you start the exam, you are asked a series of questions. You answer a question and then move on to the next question. *The exam engine does not let you go back and change your answer.* Yes, that's true—when you move on to the next question, that's it for the earlier question.

The exam questions can be in one of the following formats:

- Multiple-choice (MC)
- Testlet
- Drag-and-drop (DND)
- Simulated lab (Sim)
- Simlet

The first three types of questions are relatively common in many testing environments. The multiple-choice format simply requires that you point and click a circle beside the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many answers. Testlets are questions with one general scenario, with multiple MC questions about the overall scenario. Drag-and-drop questions require you to click and hold the mouse button, move a button or icon to another area, and release the mouse button to place the object somewhere else—typically into a list. So, for some questions, to get the question correct, you might need to put a list of five things into the proper order.

The last two types both use a network simulator to ask questions. Interestingly, the two types allow Cisco to assess two very different skills. First, Sim questions generally describe a problem, and your task is to configure one or more routers and switches to fix the problem. The exam then grades the question based on the configuration you changed or added. Interestingly, Sim questions are the only questions that Cisco (to date) has openly confirmed that partial credit is given.

The Simlet questions might well be the most difficult style of question on the exams. Simlet questions also use a network simulator, but instead of answering the question by changing the configuration, the question includes one or more MC questions. The questions require that you use the simulator to examine the current behavior of a network, interpreting the output of any **show** commands that you can remember to answer the question. While Sim questions require you to troubleshoot problems related to a configuration, Simlets require you to both analyze working networks and networks with problems, correlating **show** command output with your knowledge of networking theory and configuration commands.

What's on the CCNA Exam(s)?

Ever since I was in grade school, whenever the teacher announced that we were having a test soon, someone would always ask, "What's on the test?" Even in college, people would try to get more information about what would be on the exams. At heart, the goal is to know what to study hard, what to study a little, and what not to study.

Cisco does want the public to know both the variety of topics, and an idea about the kinds of knowledge and skills required for each topic, for every Cisco certification exam. To that end, Cisco publishes a set of exam objectives for each exam. The objectives list the specific topics, like IP addressing, RIP, and VLANs. The objectives also imply the kinds of skills required for that topic. For example, one objective might start with "Describe..." and another might begin with "Describe, configure, and troubleshoot...." The second objective clearly states that you need a thorough and deep understanding of that topic. By listing the topics and skill level, Cisco helps us all prepare for its exams.

While the exam objectives are helpful, keep in mind that Cisco adds a disclaimer that the posted exam topics for all its certification exams are *guidelines*. Cisco makes the effort to keep the exam questions within the confines of the stated exam objectives, and I know from talking to those involved that every question is analyzed for whether it fits within the stated exam topics.

ICND1 Exam Topics

Table I-1 lists the exam topics for the ICND1 exam, with the ICND2 exam topics following in Table I-2. Although the posted exam topics are not numbered at Cisco.com, Cisco Press does number the exam topics for easier reference. The table also notes the book parts in which each exam topic is covered. Because the exam topics might change over time, double-check the exam topics as listed on Cisco.com (specifically, http://www.cisco.com/go/ccna). If Cisco does happen to add exam topics at a later date, note that Appendix C of this book describes how to go to http://www.ciscopress.com and download additional information about those newly added topics.

NOTE The table includes gray highlights that will be explained in the upcoming section "CCNA Exam Topics."

Table I-1 *ICND1 Exam Topics*

Reference Number	ICND1 Book Part(s) Where Topic Is Covered	Exam Topic
		Describe the operation of data networks
1	I	Describe the purpose and functions of various network devices
2	I	Select the components required to meet a given network specification
3	I, II, III	Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
4	I	Describe common networking applications including web applications
5	I	Describe the purpose and basic operation of the protocols in the OSI and TCP models
6	I	Describe the impact of applications (Voice Over IP and Video Over IP) on a network
7	I–IV	Interpret network diagrams
8	I–IV	Determine the path between two hosts across a network
9	I, III, IV	Describe the components required for network and Internet communications
10	I–IV	Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach
11	II, III	Differentiate between LAN/WAN operation and features
		Implement a small switched network
12	II	Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
13	II	Explain the technology and media access control method for Ethernet technologies
14	II	Explain network segmentation and basic traffic management concepts
15	II	Explain the operation of Cisco switches and basic switching concepts
16	II	Perform, save and verify initial switch configuration tasks including remote access management
17	II	Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands

Table I-1 *ICND1 Exam Topics (Continued)*

Reference Number	ICND1 Book Part(s) Where Topic Is Covered	Exam Topic
18	II	Implement and verify basic security for a switch (port security, deactivate ports)
19	II	Identify, prescribe, and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures
		Implement an IP addressing scheme and IP services to meet network requirements for a small branch office
20	I, III	Describe the need and role of addressing in a network
21	I, III	Create and apply an addressing scheme to a network
22	III	Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment
23	IV	Explain the basic uses and operation of NAT in a small network connecting to one ISP
24	I, III	Describe and verify DNS operation
25	III, IV	Describe the operation and benefits of using private and public IP addressing
26	III, IV	Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping
27	III	Configure, verify and troubleshoot DHCP and DNS operation on a router. (including: CLI/SDM)
28	III	Implement static and dynamic addressing services for hosts in a LAN environment
29	III	Identify and correct IP addressing issues
		Implement a small routed network
30	I, III	Describe basic routing concepts (including: packet forwarding, router lookup process)
31	III	Describe the operation of Cisco routers (including: router bootup process, POST, router components)
32	I, III	Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
33	III	Configure, verify, and troubleshoot RIPv2
34	III	Access and utilize the router CLI to set basic parameters
35	III	Connect, configure, and verify operation status of a device interface

Table I-1 *ICND1 Exam Topics (Continued)*

Reference Number	ICND1 Book Part(s) Where Topic Is Covered	Exam Topic
36	III	Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities
37	III	Perform and verify routing configuration tasks for a static or default route given specific routing requirements
38	III	Manage IOS configuration files (including: save, edit, upgrade, restore)
39	III	Manage Cisco IOS
40	III	Implement password and physical security
41	III	Verify network status and router operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands
		Explain and select the appropriate administrative tasks required for a WLAN
42	II	Describe standards associated with wireless media (including: IEEE, WI-FI Alliance, ITU/FCC)
43	II	Identify and describe the purpose of the components in a small wireless network. (including: SSID, BSS, ESS)
44	II	Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
45	II	Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)
46	II	Identify common issues with implementing wireless networks
		Identify security threats to a network and describe general methods to mitigate those threats
47	I	Explain today's increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats
48	I	Explain general methods to mitigate common security threats to network devices, hosts, and applications
49	I	Describe the functions of common security appliances and applications
50	I, II, III	Describe security recommended practices including initial steps to secure network devices
		Implement and verify WAN links
51	IV	Describe different methods for connecting to a WAN
52	IV	Configure and verify a basic WAN serial connection

ICND2 Exam Topics

Table I-2 lists the exam topics for the ICND2 (640-816) exam, along with the book parts in *CCNA ICND2 Official Exam Certification Guide* in which each topic is covered.

Table I-2 *ICND2 Exam Topics*

Reference Number	ICND2 Book Part(s) Where Topic Is Covered	Exam Topic
		Configure, verify and troubleshoot a switch with VLANs and interswitch communications
101	I	Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q)
102	I	Describe how VLANs create logically separate networks and the need for routing between them
103	I	Configure, verify, and troubleshoot VLANs
104	I	Configure, verify, and troubleshoot trunking on Cisco switches
105	II	Configure, verify, and troubleshoot interVLAN routing
106	I	Configure, verify, and troubleshoot VTP
107	I	Configure, verify, and troubleshoot RSTP operation
108	I	Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network
109	I	Implement basic switch security (including: port security, unassigned ports, trunk access, etc.)
		Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network
110	II	Calculate and apply a VLSM IP addressing design to a network
111	II	Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment
112	V	Describe the technological requirements for running IPv6 (including: protocols, dual stack, tunneling, etc)
113	V	Describe IPv6 addresses
114	II, III	Identify and correct common problems associated with IP addressing and host configurations
		Configure and troubleshoot basic operation and routing on Cisco devices
115	III	Compare and contrast methods of routing and routing protocols
116	III	Configure, verify and troubleshoot OSPF

Table I-2 *ICND2 Exam Topics (Continued)*

Reference Number	ICND2 Book Part(s) Where Topic Is Covered	Exam Topic
117	III	Configure, verify and troubleshoot EIGRP
118	II, III	Verify configuration and connectivity using ping, traceroute, and telnet or SSH
119	II, III	Troubleshoot routing implementation issues
120	II, III, IV	Verify router hardware and software operation using SHOW & DEBUG commands
121	II	Implement basic router security
		Implement, verify, and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network.
122	II	Describe the purpose and types of access control lists
123	II	Configure and apply access control lists based on network filtering requirements
124	II	Configure and apply an access control list to limit telnet and SSH access to the router
125	II	Verify and monitor ACLs in a network environment
126	II	Troubleshoot ACL implementation issues
127	V	Explain the basic operation of NAT
128	V	Configure Network Address Translation for given network requirements using CLI
129	V	Troubleshoot NAT implementation issues
		Implement and verify WAN links
130	IV	Configure and verify Frame Relay on Cisco routers
131	IV	Troubleshoot WAN implementation issues
132	IV	Describe VPN technology (including: importance, benefits, role, impact, components)
133	IV	Configure and verify PPP connection between Cisco routers

CCNA Exam Topics

In the previous version of the exams, the CCNA exam covered a lot of what was in the ICND (640-811) exam, plus some coverage of topics in the INTRO (640-821) exam. The new CCNA exam (640-802) covers all the topics on both the ICND1 (640-822) and ICND2 (640-816) exams. One of the reasons for a more balanced coverage in the exams is that some of the topics that used to be in the second exam have been moved to the first exam.

The new CCNA (640-802) exam covers all topics in both the ICND1 and ICND2 exams. The official CCNA 640-802 exam topics, posted at http://www.cisco.com, include all the topics listed in Table I-2 for the ICND2 exam, plus most of the exam topics for the ICND1 exam listed in Table I-1. The only exam topics from these two tables that are not listed as CCNA exam topics are the topics highlighted in gray in Table I-1. However, note that the gray topics are still covered on the CCNA 640-802 exam. Those topics are just not listed in the CCNA exam topics because one of the ICND2 exam topics refers to the same concepts.

ICND1 and ICND2 Course Outlines

Another way to get some direction about the topics on the exams is to look at the course outlines for the related courses. Cisco offers two authorized CCNA-related courses: Interconnecting Cisco Network Devices 1 (ICND1) and Interconnecting Cisco Network Devices 2 (ICND2). Cisco authorizes Certified Learning Solutions Providers (CLSP) and Certified Learning Partners (CLP) to deliver these classes. These authorized companies can also create unique custom course books using this material, in some cases to teach classes geared toward passing the CCNA exam.

About the *CCENT/CCNA ICND1 Official Exam Certification Guide* and *CCNA ICND2 Official Exam Certification Guide*

As mentioned earlier, Cisco has separated the content covered by the CCNA exam into two parts: topics typically used by engineers who work in a small enterprise network (ICND1), with the additional topics commonly used by engineers in medium-sized enterprises being covered by the ICND2 exam. Likewise, the Cisco Press CCNA Exam Certification Guide series includes two books for CCNA—*CCENT/CCNA ICND1 Official Exam Certification Guide* and *CCNA ICND2 Official Exam Certification Guide*. These two books cover the breadth of topics on each exam, typically to a little more depth than is required for the exams, just to ensure that the books prepare you for the more difficult exam questions.

The following sections list the variety of features in both this book and *CCENT/CCNA ICND1 Official Exam Certification Guide*. Both books have the same basic features, so if you are reading both this book and the ICND1 book, you don't need to read the introduction to both books. Also, for those of you who are using both books to prepare for the CCNA 640-802 exam (rather than taking the two-exam option), the end of this introduction lists a suggested reading plan.

Objectives and Methods

The most important and somewhat obvious objective of this book is to help you pass the ICND2 exam or the CCNA exam. In fact, if the primary objective of this book were different, the book's title would be misleading! However, the methods used in this book to

help you pass the exams are also designed to make you much more knowledgeable about how to do your job.

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. The CCNA certification is the foundation for many of the Cisco professional certifications, and it would be a disservice to you if this book did not help you truly learn the material. Therefore, this book helps you pass the CCNA exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process through test questions on the CD

Book Features

To help you customize your study time using these books, the core chapters have several features that help you make the best use of your time:

- **"Do I Know This Already?" Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks:** At the end of the Foundation Topics section of each chapter, the Exam Preparation Tasks section lists a series of study activities that should be done at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:
  - **Key Topics Review:** The Key Topics icon is shown next to the most important items in the Foundation Topics section of the chapter. The Key Topics Review activity lists the key topics from the chapter, and the page number. While the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so these should be reviewed.

- **Complete Tables and Lists from Memory:** To help you exercise your memory and memorize some lists of facts, many of the more important lists and tables from the chapter are included in Appendix J on the CD. This document lists only partial information, allowing you to complete the table or list. Appendix K lists the same tables and lists, completed, for easy comparison.
- **Definition of Key Terms:** While the exams are unlikely to ask a question like "Define this term," the CCNA exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Command Reference Tables:** Some book chapters cover a large amount of configuration and EXEC commands. These tables list the commands introduced in the chapter, along with an explanation. For exam preparation, use them for reference, but also read the tables once when performing the Exam Preparation Tasks to make sure that you remember what all the commands do.

- **CD-based Practice Exam:** The companion CD contains an exam engine (from Boson software, http://www.boson.com) that includes a large number of exam-realistic practice questions. You can take simulated ICND2 exams, as well as simulated CCNA exams, with the CD in this book. (You can take simulated ICND1 and CCNA exams with the CD in *CCENT/CCNA ICND1 Official Exam Certification Guide*.)
- **Subnetting Videos:** The companion DVD contains a series of videos that show how to calculate various facts about IP addressing and subnetting, in particular using the shortcuts described in this book.
- **Subnetting Practice:** CD Appendix D contains a large set of subnetting practice problems, with the answers and with explanations of how the answers were found. This is a great resource to get ready to do subnetting well and fast.
- **CD-based Practice Scenarios:** CD Appendix F contains several networking scenarios for additional study. These scenarios describe various networks and requirements, taking you through conceptual design, configuration, and verification. These scenarios are useful for building your hands-on skills, even if you do not have lab gear.

- **Companion Website:** The website http://www.ciscopress.com/title/1587201828 posts up-to-the-minute materials that further clarify complex exam topics. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam.

How This Book Is Organized

This book contains 18 core chapters—Chapters 1 through 18, with Chapter 18 including some summary materials and suggestions for how to approach the exams. Each core chapter covers a subset of the topics on the ICND2 exam. The core chapters are organized into sections and cover the following topics:

- Part I: LAN Switching
  - **Chapter 1, "Virtual LANs"**: This chapter explains the concepts and configuration surrounding virtual LANs, including VLAN trunking and VLAN Trunking Protocol.
  - **Chapter 2, "Spanning Tree Protocol"**: This chapter dives deeply into the concepts behind the original Spanning Tree Protocol (STP), as well as the newer Rapid STP (RSTP), including concepts, configuration, and troubleshooting.
  - **Chapter 3, "Troubleshooting LAN Switching"**: This chapter explains some general ideas about how to troubleshoot networking problems, with most of the chapter focusing on the forwarding process used by LAN switches.
- Part II: IP Routing
  - **Chapter 4, "IP Routing: Static and Connected Routes"**: This chapter examines how routers add both static routes and connected routes to the routing table, while also reviewing the concepts behind how routers route, or forward, packets.
  - **Chapter 5, "VLSM and Route Summarization"**: This chapter explains how IP routing and routing protocols can support the use of different subnet masks in a single classful network (VLSM), as well as the math concepts behind how routers can summarize multiple routes into one routing table entry.
  - **Chapter 6, "IP Access Control Lists"**: This chapter examines how ACLs can filter packets so that a router will not forward the packet. The chapter examines the concepts and configuration for standard and extended ACLs, including named and numbered ACLs.

- **Chapter 7, "Troubleshooting IP Routing"**: This chapter shows a structured plan for how to isolate problems related to two hosts that should be able to send packets to each other, but cannot. The chapter also includes a variety of tips and tools for helping attack routing problems.

- Part III: Routing Protocols Configuration and Troubleshooting
  - **Chapter 8, "Routing Protocol Theory"**: This chapter explains the theory behind distance vector and link-state protocols.
  - **Chapter 9, "OSPF"**: This chapter examines OSPF, including more detail about link-state theory as implemented by OSPF, and OSPF configuration.
  - **Chapter 10, "EIGRP"**: This chapter examines EIGRP, including a description of the theory behind EIGRP, as well as EIGRP configuration and verification.
  - **Chapter 11, "Troubleshooting Routing Protocols"**: This chapter explains some of the typical reasons why routing protocols fail to exchange routing information, showing specific examples of common problems with both OSPF and EIGRP.
- Part IV: Wide-Area Networks
  - **Chapter 12, "Point-to-Point WANs"**: This short chapter reviews the basics of WANs and examines PPP, including CHAP, in more detail.
  - **Chapter 13, "Frame Relay Concepts"**: This chapter focuses on the terminology and theory behind the Frame Relay protocol, including the IP addressing options when using Frame Relay.
  - **Chapter 14, "Frame Relay Configuration and Troubleshooting"**: This chapter shows a variety of configuration options for Frame Relay, including both point-to-point and multipoint subinterfaces. It also explains how to best use **show** commands to isolate the root cause of common Frame Relay problems.
  - **Chapter 15, "Virtual Private Networks"**: This chapter examines the concepts and protocols used to create secure VPNs over the Internet. This chapter includes the basics of IPsec.

- Part V: Scaling the IP Address Space
  - **Chapter 16, "Network Address Translation"**: This chapter closely examines the concepts behind the depletion of the IPv4 address space, and how NAT, in particular the Port Address Translation (PAT) option, helps solve the problem. The chapter also shows how to configure NAT on routers using the IOS CLI.
  - **Chapter 17, "IP Version 6"**: This chapter introduces the basics of IPv6, including the 128-bit address format, OSPF and EIGRP support for IPv6, and basic native IPv6 configuration. It also introduces the concept of IPv6 tunneling and migration strategies.
- Part VI: Final Preparation
  - **Chapter 18, "Final Preparation"**: This chapter suggests a plan for final preparation after you have finished the core parts of the book, in particular explaining the many study options available in the book.
- Part VII: Appendixes (in Print)
  - **Appendix A, "Answers to the 'Do I Know This Already?' Quizzes"**: Includes the answers to all the questions from Chapters 1 through 17.
  - **Appendix B, "Decimal-to-Binary Conversion Table"**: Lists decimal values 0 through 255, along with the binary equivalents.
  - **Appendix C, "ICND2 Exam Updates: Version 1.0"**: This appendix covers a variety of short topics that either clarify or expand upon topics covered earlier in the book. This appendix is updated from time to time and posted at http://www.ciscopress.com/ccna, with the most recent version available at the time of printing included here as Appendix C. (The first page of the appendix includes instructions on how to check whether a later version of Appendix C is available online.)
  - **Glossary**: The glossary contains definitions for all the terms listed in the "Definitions of Key Terms" section at the conclusion of Chapters 1–17.

- Part VII: Appendixes (on CD)

  The following appendixes are available in PDF format on the CD that accompanies this book:

  - **Appendix D, "Subnetting Practice"**: Although not covered in any of the chapters printed in this book, subnetting is easily the most important prerequisite assumed skill for the ICND2 exam. This appendix, as well as Appendixes E, H, and I, include materials from *CCENT/CCNA ICND1 Official Exam Certification Guide* for those of you that bought this book, but not the ICND1 book. In particular, this appendix includes a large number of subnetting practice problems, with the answers listed. The answers use both binary and decimal-shortcut processes described in the ICND1 book's Chapter 12; Appendix H of this book is a duplicate of ICND1's Chapter 12.
  - **Appendix E, "Subnetting Reference Pages"**: This appendix summarizes the process to find the answer to several key subnetting questions, with the details on a single page. The goal is to give you a handy reference page to refer to when practicing subnetting.
  - **Appendix F, "Additional Scenarios"**: One method to improve your troubleshooting and network analysis skills is to examine as many unique network scenarios as is possible, think about them, and then get some feedback as to whether you came to the right conclusions. This appendix provides several such scenarios.
  - **Appendix G, "Video Scenario Reference"**: The DVD includes several subnetting videos that show how to use the processes covered in Appendix H (copied from ICND1's Chapter 12). This appendix contains copies of the key elements from those videos, which can be useful when watching the videos (so that you do not have to keep moving back and forth in the video).
  - **Appendix H, "ICND1 Chapter 12: IP Addressing and Subnetting"**: This appendix is a duplicate of Chapter 12 from *CCENT/CCNA ICND1 Official Exam Certification Guide*. This chapter explains IP addressing and subnetting, which is considered prerequisite knowledge for the ICND2 exam. Appendix H is included with this book for those of you who do not have a copy of *CCENT/CCNA ICND1 Official Exam Certification Guide*, but you need to review and learn more about subnetting.
  - **Appendix I, "ICND1 Chapter 17: WAN Configuration"**: This appendix is a duplicate of Chapter 17 from *CCENT/CCNA ICND1 Official Exam Certification Guide*. Chapter 12 of this book (ICND2), "Point-to-Point WANs," makes a suggestion to review a few prerequisite points as listed in this chapter. This chapter is included in this book for those of you who do not have a copy of *CCENT/CCNA ICND1 Official Exam Certification Guide*.

— **Appendix J, "Memory Tables"**: This appendix holds the key tables and lists from each chapter, with some of the content removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.

— **Appendix K, "Memory Tables Answer Key"**: This appendix contains the answer key for the exercises in Appendix J.

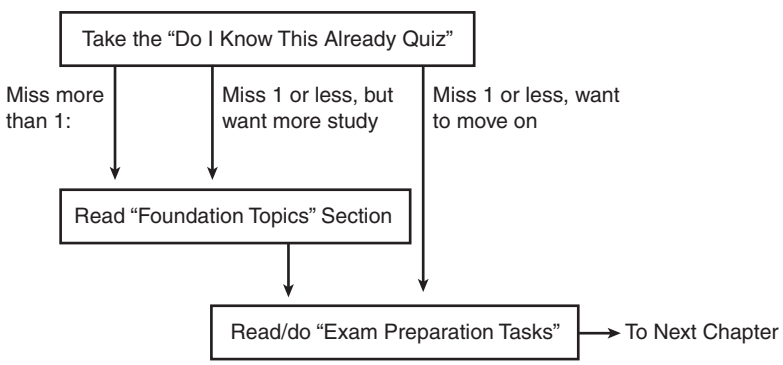
— **Appendix L, "ICND2 Open-Ended Questions"**: This appendix is a holdover from previous editions of this book. The older edition had some open-ended questions for the purpose of helping you study for the exam, but the newer features make these questions unnecessary. For convenience, the old questions are included here, unedited since the last edition.

How to Use This Book to Prepare for the ICND2 (640-816) Exam

This book was designed with two primary goals in mind: to help you study for the ICND2 exam and to help you study for the CCNA exam by using both this book and the *CCENT/CCNA ICND1 Official Exam Certification Guide*. Using this book to prepare for the ICND2 exam is straightforward—read each chapter in succession, and follow the study suggestions in Chapter 18, "Final Preparation."

For the core chapters of this book (Chapters 1–17), you do have some choices as to how much of the chapter you read. In some cases, you might already know most of or all the information covered in a given chapter. To help you decide how much time to spend on each chapter, the chapters begin with a "Do I Know This Already?" quiz. If you get all the quiz questions correct, or just miss one question, you might want to skip to the end of the chapter and the "Exam Preparation Tasks" section, and do those activities. Figure I-2 shows the overall plan.

Figure I-2 *How to Approach Each Chapter of This Book*



When you have completed Chapters 1–17, you can then use the guidance listed in Chapter 18 to detail the rest of the exam preparation tasks. That chapter includes the following suggestions:

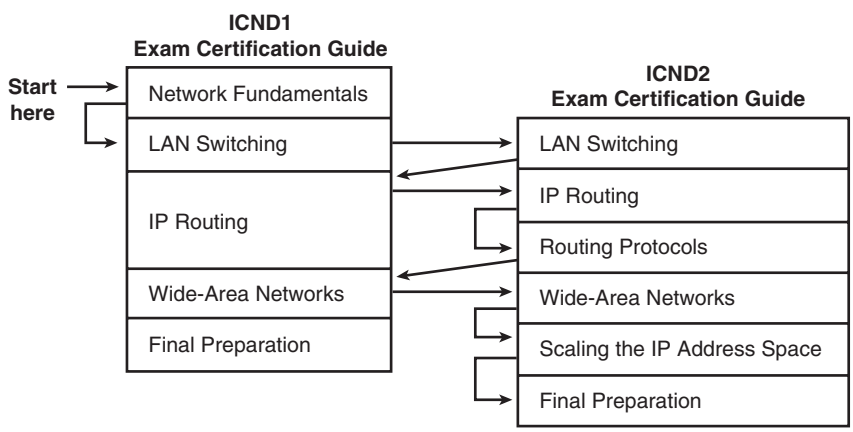
- Check http://www.ciscopress.com for the latest copy of Appendix C, which can include additional topics for study.
- Practice subnetting using the tools available in the CD appendixes.
- Repeat the tasks in all chapters' "Exam Preparation Tasks" chapter-ending sections.
- Review the scenarios in CD Appendix F.
- Review all the "Do I Know This Already?" questions.
- Practice the exam using the exam engine.

How to Use These Books to Prepare for the CCNA 640-802 Exam

If you plan to get your CCNA certification using the one-exam option of taking the CCNA 640-802 exam, you can use this book along with *CCENT/CCNA ICND1 Official Exam Certification Guide*. If you've not yet bought either book, you can generally get the pair cheaper by buying both books as a two-book set, called the CCNA Certification Library.

These two books were designed to be used together when studying for the CCNA exam. You have two options for the order in which to read the two books. The first and most obvious option is to read the ICND1 book, and then move on to this (ICND2) book. The other option is to read all of ICND1's coverage of one topic area, then read ICND2's coverage of the same topics, and then go back to ICND1 again. Figure I-3 outlines my suggested option for reading the two books.

Figure I-3 *Reading Plan When Studying for CCNA Exam*



Both reading-plan options have some benefits. Moving back and forth between books can help you to focus on one general topic at a time. However, note that some overlap exists between the two exams, so you find some overlap between the two books as well. From reader comments about the previous edition of these books, those readers who were new to networking tended to do better by completing all of the first book and then moving on to the second, while readers that had more experience and knowledge before starting the books tended to prefer to follow a reading plan like the one shown in Figure I-3.

Note that for final preparation, you can use the final chapter (Chapter 18) of this book, rather than the final preparation chapter (Chapter 18) of the ICND1 book.

In addition to the flow shown in Figure I-3, when studying for the CCNA exam (rather than for the ICND1 and ICND2 exams), you must master IP subnetting before moving on to the IP routing and routing protocol parts (Parts II and III) of this book. This book does not review subnetting or the underlying math in the printed text, assuming that you know how to find the answers. Those ICND2 chapters, particularly Chapter 5 ("VLSM and Route Summarization"), will be much easier to understand if you can easily do the related subnetting math.

For More Information

If you have any comments about the book, you can submit those through Ciscopress.com. Just go to the website, click the Contact Us link, and type in your message.

Cisco might make changes that affect the CCNA certification from time to time. You should always check http://www.cisco.com/go/ccna for the latest details.

The CCNA certification is arguably the most important Cisco certification, with the new CCENT certification possibly surpassing CCNA in the future. CCNA certainly is the most popular Cisco certification, is required for several other certifications, and is the first step in distinguishing yourself as someone who has proven knowledge of Cisco.

CCNA ICND2 Official Exam Certification Guide is designed to help you attain CCNA certification. This is the CCNA ICND2 certification book from the only Cisco-authorized publisher. We at Cisco Press believe that this book certainly can help you achieve CCNA certification—but the real work is up to you! I trust that your time will be well spent.

This chapter covers the following subjects:

The ping and traceroute Commands: This section explains how the **ping** and **traceroute** commands work, along with the nuances of how they can be used to better troubleshoot routing problems.

Troubleshooting the Packet Forwarding Process: This section examines the packet forwarding process, focusing on host routing and how routers route packets. It also covers issues related to forwarding packets in both directions between two hosts.

Troubleshooting Tools and Tips: This section covers a wide variety of topics that have some effect on the packet forwarding process. It includes many tips about various commands and concepts that can aid the troubleshooting process.

CHAPTER 7

Troubleshooting IP Routing

This troubleshooting chapter has several goals. First, it explains several tools and functions not covered in Chapters 4 through 6—specifically, tools that can be very helpful when you're analyzing problems. This chapter also reviews concepts from all three of the other chapters in Part II, "IP Routing." It pulls together the concepts by showing a suggested process for troubleshooting routing problems, as well as examples of how to use the process. The second half of the chapter focuses on a series of troubleshooting tips for many of the specific topics covered in Chapters 4 through 6.

"Do I Know This Already?" Quiz

The troubleshooting chapters of this book pull in concepts from many other chapters, including some chapters in *CCENT/CCNA ICND1 Official Exam Certification Guide*. They also show you how to approach some of the more challenging questions on the CCNA exams. Therefore, it is useful to read these chapters regardless of your current knowledge level. For these reasons, the troubleshooting chapters do not include a "Do I Know This Already?" quiz. However, if you feel particularly confident about troubleshooting IP routing features covered in this book and *CCENT/CCNA ICND1 Official Exam Certification Guide*, feel free to move to the "Exam Preparation Tasks" section near the end of this chapter to bypass the majority of the chapter.

Foundation Topics

This chapter focuses on troubleshooting the IP routing process. To that end, it begins with a section about two important troubleshooting tools: ping and traceroute. Following that, the chapter examines the IP routing process from a troubleshooting perspective, particularly focusing on how to isolate routing problems to identify the root cause of the problem. The final section covers a wide variety of small topics, all of which can be useful when you're troubleshooting IP routing problems.

NOTE This chapter, and Chapter 15 in *CCENT/CCNA ICND1 Official Exam Certification Guide*, both explain details of how to troubleshoot the IP routing process. IP routing is vitally important on both the ICND1 and ICND2 exams, as well as on the CCNA exam, so there is overlap between the exams, requiring some overlap in the books. However, this chapter covers many topics that go beyond the details required for the ICND1 exam. To be fully prepared, read this entire chapter, but feel free to skim portions if the chapter seems repetitive with the ICND1 book.

The ping and traceroute Commands

This section examines a suggested process of troubleshooting IP routing—in other words, the data plane process of how hosts and routers forward IP packets. To that end, this section first examines a set of useful tools and protocols—in particular, ICMP, **ping**, and **traceroute**. Following that, the text suggests a good general troubleshooting process for IP problems, with a few examples to show how to use the processes.

Internet Control Message Protocol (ICMP)

TCP/IP includes ICMP, a protocol designed to help manage and control the operation of a TCP/IP network. The ICMP protocol provides a wide variety of information about a network's health and operational status. *Control Message* is the most descriptive part of the name. ICMP helps control and manage IP's work by defining a set of messages and procedures about the operation of IP. Therefore, ICMP is considered part of TCP/IP's network layer. Because ICMP helps control IP, it can provide useful troubleshooting information. In fact, the ICMP messages sit inside an IP packet, with no transport layer header, so ICMP is truly an extension of the TCP/IP network layer.

RFC 792 defines ICMP. The following excerpt from RFC 792 describes the protocol well:

> Occasionally a gateway (router) or destination host will communicate with a source host, for example, to report an error in datagram processing. For such

purposes, this protocol, the Internet Control Message Protocol (ICMP), is used. ICMP uses the basic support of IP as if it were a higher level protocol; however, ICMP is actually an integral part of IP and must be implemented by every IP module.

ICMP defines several different types of messages to accomplish its varied tasks, as summarized in Table 7-1.

Table 7-1 *ICMP Message Types*

Message	Description
Destination Unreachable	Tells the source host that there is a problem delivering a packet.
Time Exceeded	The time that it takes a packet to be delivered has expired, so the packet has been discarded.
Redirect	The router sending this message has received a packet for which another router has a better route. The message tells the sender to use the better route.
Echo Request, Echo Reply	Used by the **ping** command to verify connectivity.

The ping Command and the ICMP Echo Request and Echo Reply

The **ping** command uses the ICMP Echo Request and Echo Reply messages. In fact, when people say they sent a ping packet, they really mean that they sent an ICMP Echo Request. These two messages are somewhat self-explanatory. The Echo Request simply means that the host to which it is addressed should reply to the packet. The Echo Reply is the ICMP message type that should be used in the reply. The Echo Request includes some data that can be specified by the **ping** command; whatever data is sent in the Echo Request is sent back in the Echo Reply.

The **ping** command itself supplies many creative ways to use Echo Requests and Replies. For instance, the **ping** command lets you specify the length as well as the source and destination addresses, and it also lets you set other fields in the IP header. Chapter 4, "IP Routing: Static and Connected Routes," shows an example of the extended **ping** command that lists the various options.

The Destination Unreachable ICMP Message

This book focuses on IP. But if you take a broader view, the role of the entire set of TCP/IP protocols is to deliver data from the sending application to the receiving application. Hosts and routers send ICMP Destination Unreachable messages back to the sending host when that host or router cannot deliver the data completely to the application at the destination host.

To aid in troubleshooting, the ICMP Unreachable message includes five separate unreachable functions (codes) that further identify the reason why the packet cannot be delivered. All five code types pertain directly to an IP, TCP, or UDP feature.

For example, the internetwork shown in Figure 7-1 can be used to better understand some of the Unreachable codes. Assume that Fred is trying to connect to the web server, called Web. (Web uses HTTP, which in turn uses TCP as the transport layer protocol.) Three of the ICMP unreachable codes can possibly be used by Routers A and B. The other two codes are used by the web server. These ICMP codes are sent to Fred as a result of the packet originally sent by Fred.

Figure 7-1 *Sample Network for Discussing ICMP Unreachable Codes*

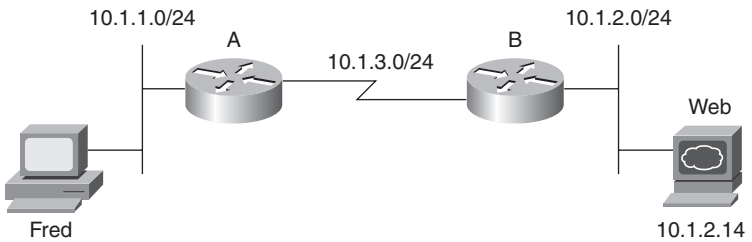


Table 7-2 summarizes the more common ICMP unreachable codes. After the table, the text explains how each ICMP code might be needed for the network shown in Figure 7-1.

Table 7-2 *ICMP Unreachable Codes*

Unreachable Code	When It Is Used	What Typically Sends It
Network unreachable	There is no match in a routing table for the packet's destination.	Router
Host unreachable	The packet can be routed to a router connected to the destination subnet, but the host is not responding.	Router
Can't fragment	The packet has the Don't Fragment bit set, and a router must fragment to forward the packet.	Router
Protocol unreachable	The packet is delivered to the destination host, but the transport layer protocol is not available on that host.	Host
Port unreachable	The packet is delivered to the destination host, but the destination port has not been opened by an application.	Host

The following list explains each code in Table 7-2 in greater detail using the network in Figure 7-1 as an example:

- **Network unreachable:** Router A uses this code if it does not have a route telling it where to forward the packet. In this case, Router A needs to route the packet to subnet 10.1.2.0/24. If it cannot, Router A sends Fred the ICMP Destination Unreachable message with the code "network unreachable" in response to Fred's packet destined for 10.1.2.14.

- **Host unreachable:** This code implies that the single destination host is unavailable. If Router A has a route to 10.1.2.0/24, the packet is delivered to Router B. If Router B's LAN interface is working, B also has a connected route to 10.1.2.0/24, so B tries to ARP and learn the web server's MAC address. However, if the web server is down, Router B does not get an ARP reply from the web server. Router B sends Fred the ICMP Destination Unreachable message with the code "host unreachable," meaning that B has a route but cannot forward the packet directly to 10.1.2.14.

- **Can't fragment:** This code is the last of the three ICMP unreachable codes that a router might send. Fragmentation defines the process in which a router needs to forward a packet, but the outgoing interface allows only packets that are smaller than the packet. The router is allowed to fragment the packet into pieces, but the packet header can be set with the "Do Not Fragment" bit in the IP header. In this case, if Router A or B needs to fragment the packet, but the Do Not Fragment bit is set in the IP header, the router discards the packet and sends Fred an ICMP Destination Unreachable message with the code "can't fragment."

- **Protocol unreachable:** If the packet successfully arrives at the web server, two other unreachable codes are possible. One implies that the protocol above IP, typically TCP or UDP, is not running on that host. This is highly unlikely, because most operating systems that use TCP/IP use a single software package that provides IP, TCP, and UDP functions. But if the host receives the IP packet and TCP or UDP is unavailable, the web server host sends Fred the ICMP Destination Unreachable message with the code "protocol unreachable" in response to Fred's packet destined for 10.1.2.14.

- **Port unreachable:** This final code field value is more likely today. If the server—the computer—is up and running, but the web server software is not running, the packet can get to the server but cannot be delivered to the web server software. In effect, the server is not listening on that application protocol's well-known port. So, host 10.1.2.14 sends Fred the ICMP Destination Unreachable message with the code "port unreachable" in response to Fred's packet destined for 10.1.2.14.

NOTE Most security policies today filter these various unreachable messages to help bolster the network's security profile.

The **ping** command lists various responses that in some cases imply that an unreachable message was received. Table 7-3 lists the various unreachable codes that may be displayed by the Cisco IOS Software **ping** command.

Table 7-3 *Codes That the* **ping** *Command Receives in Response to Its ICMP Echo Request*

ping Command Code	Description
!	ICMP Echo Reply received
.	Nothing was received before the **ping** command timed out
U	ICMP unreachable (destination) received
N	ICMP unreachable (network/subnet) received
M	ICMP Can't Fragment message received
?	Unknown packet received

The Redirect ICMP Message

The ICMP Redirect message provides a means by which routers can tell hosts to use another router as default gateway for certain destination addresses. Most hosts use the concept of a default router IP address, sending packets destined for subnets to their default router. However, if multiple routers connect to the same subnet, a host's default gateway may not be the best router on that subnet to which to forward packets sent to some destinations. The default gateway can recognize that a different router is a better option. Then it can send ICMP redirect messages to the host to tell it to send the packets for that destination address to this different router.

For example, in Figure 7-2, the PC uses Router B as its default router. However, Router A's route to subnet 10.1.4.0 is a better route. (Assume the use of mask 255.255.255.0 in each subnet in Figure 7-2.) The PC sends a packet to Router B (Step 1 in Figure 7-2). Router B then forwards the packet based on its own routing table (Step 2); that route points through Router A, which has a better route. Finally, Router B sends the ICMP redirect message to the PC (Step 3), telling it to forward future packets destined for 10.1.4.0 to Router A instead. Ironically, the host can ignore the redirect and keep sending the packets to Router B, but in this example, the PC believes the redirect message, sending its next packet (Step 4) directly to Router A.

The ICMP Time Exceeded Message

The ICMP Time Exceeded message notifies a host when a packet it sent has been discarded because it was "out of time." Packets are not actually timed, but to prevent them from being forwarded forever when there is a routing loop, each IP header uses a Time to Live (TTL) field. Routers decrement the TTL by 1 every time they forward a packet; if a router

decrements the TTL to 0, it throws away the packet. This prevents packets from rotating forever. Figure 7-3 shows the basic process.

Figure 7-2 *ICMP Redirect*

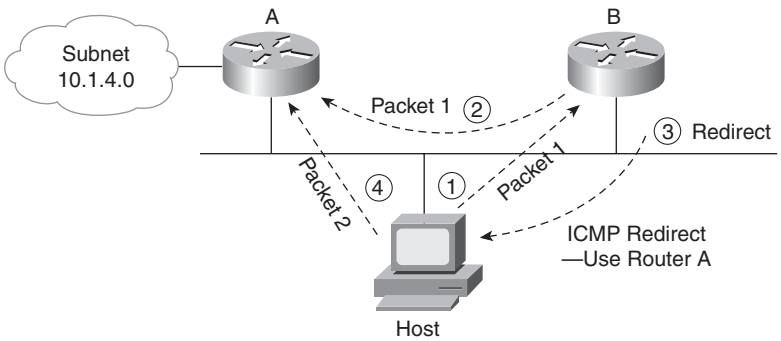
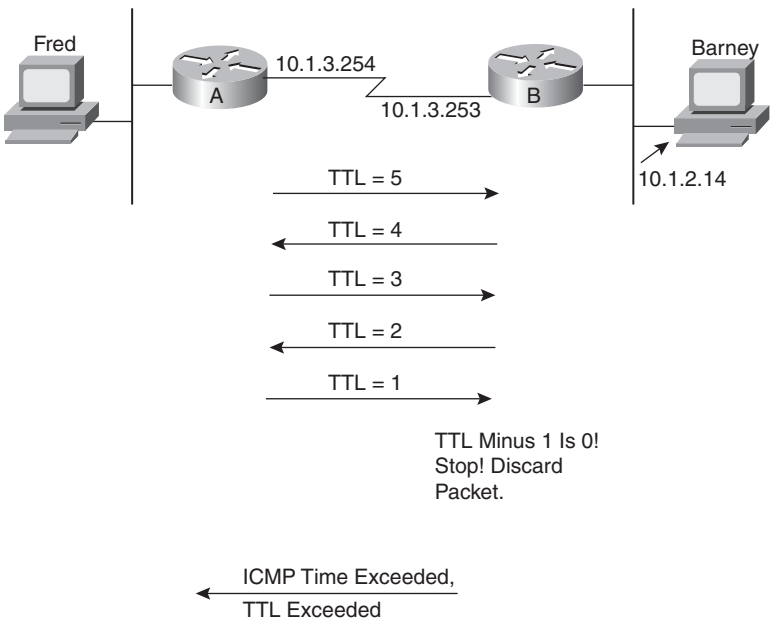


Figure 7-3 *TTL Decremented to 0*

Key Topic



As you can see in the figure, the router that discards the packet also sends an ICMP Time Exceeded message, with a Code field of "time exceeded" to the host that sent the packet. That way, the sender knows that the packet was not delivered. Getting a Time Exceeded

message can also help you when you troubleshoot a network. Hopefully, you do not get too many of these; otherwise, you have routing problems.

The traceroute Command

The **ping** command is a powerful troubleshooting tool that can be used to answer the question "Does the route from here to there work?" The **traceroute** command provides an arguably better troubleshooting tool because not only can it determine if the route works, but it can supply the IP address of each router in the route. If the route is not working, **traceroute** can identify the best places to start troubleshooting the problem.

The IOS **traceroute** command uses the Time Exceeded message and the IP TTL field to identify each successive router in a route. The **traceroute** command sends a set of messages with increasing TTL values, starting with 1. The **traceroute** command expects these messages to be discarded when routers decrement the TTL to 0, returning Time Exceeded messages to the **traceroute** command. The source IP addresses of the Time Exceeded messages identify the routers that discarded the messages, which can then be displayed by the **traceroute** command.

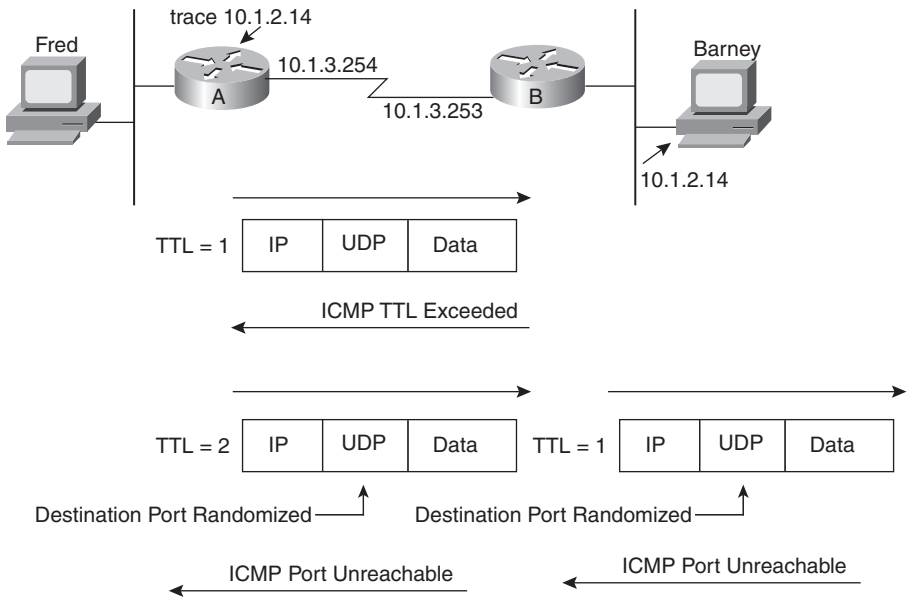
To see how this command works, consider the first set of packets (three packets by default) sent by the **traceroute** command. The packets are IP packets, with a UDP transport layer, and with the TTL set to 1. When the packets arrive at the next router, the router decrements the TTL to 0 in each packet, discards the packet, and sends a Time Exceeded message back to the host that sent the discarded packet. The **traceroute** command looks at the first router's source IP address in the received Time Exceeded packet.

Next, the **traceroute** command sends another set of three IP packets, this time with TTL = 2. The first router decrements TTL to 1 and forwards the packets, and the second router decrements the TTL to 0 and discards the packets. This second router sends Time Exceeded messages back to the router where the **traceroute** command was used, and the **traceroute** command now knows the second router in the route.

The **traceroute** command knows when the test packets arrive at the destination host because the host sends back an ICMP Port Unreachable message. The original packets sent by the IOS **traceroute** command use a destination UDP port number that is very unlikely to be used on the destination host, so as soon as the TTL is large enough to allow the packet to arrive at the destination host, the host notices that it does not have an application listening at that particular UDP port. So, the destination host returns a Port Unreachable message, which tells the **traceroute** command that the complete route has been found, and the command can stop.

Figure 7-4 shows an example, but with only one of the three messages at each TTL setting (to reduce clutter). Router A uses the **traceroute** command to try to find the route to Barney. Example 7-1 shows this **traceroute** command on Router A, with debug messages from Router B, showing the three resulting Time Exceeded messages.

Figure 7-4 *Cisco IOS Software* **traceroute** *Command: Messages Generated*



Example 7-1 *ICMP* **debug** *on Router B When Running the* **traceroute** *Command on Router A*

```
RouterA#traceroute 10.1.2.14

Type escape sequence to abort.
Tracing the route to 10.1.2.14

  1 10.1.3.253 8 msec 4 msec 4 msec
  2 10.1.2.14 12 msec 8 msec 4 msec
RouterA#
```

```
! Moving to Router B now
! The following output occurs in reaction to the traceroute command on A
RouterB#debug ip icmp
RouterB#
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
ICMP: time exceeded (time to live) sent to 10.1.3.254 (dest was 10.1.2.14)
```

The **traceroute** command lists the IP address of Router B in the first line and the IP address of the destination host in the second line. Note that it lists Router B's left-side IP address. B replies with the Time Exceeded message, using B's outgoing interface IP address as the source address in that packet. As a result, the **traceroute** command lists that IP address. If the address is known to a DNS server, or if it's in Router A's hostname table, the command can list the hostname instead of the IP address.

Similar to the extended **ping** command as described in the section titled, "The Extended **ping** Command" in Chapter 4, the extended version of the **traceroute** command does a much better job of simulating packets sent by end-user hosts, especially for testing reverse routes. For example, in Example 7-1, A's **traceroute** command uses A's 10.1.3.254 IP address as the source address of sent packets, because A uses the interface with address 10.1.3.254 to send the packets generated by the **traceroute** command. So, the **traceroute** command in Example 7-1 tests the forward route toward 10.1.2.14 and the reverse route to 10.1.3.254. By using the extended **traceroute** command, the command can be used to test a more appropriate reverse route, such as the route to the LAN subnet on the left side of Router A. Example 7-2, later in this chapter, shows an example of the extended **traceroute** command.

NOTE The **tracert** command on Microsoft operating systems works much like the IOS **traceroute** command. However, it is important to note that the Microsoft **tracert** command sends ICMP Echo Requests and does not use UDP. So, IP ACLs could cause the IOS **traceroute** to fail while the Microsoft **tracert** worked, and vice versa.

Troubleshooting the Packet Forwarding Process

Troubleshooting the IP routing process is one of the more complex tasks faced by network engineers. As usual, using a structured approach can help. Chapter 4 in particular, as well as Chapters 5 and 6, have already explained a lot about the first major part of the troubleshooting process—namely, what should happen in a network. This section focuses on the second major step: problem isolation. (For a more general reference on troubleshooting techniques, refer to Chapter 3, "Troubleshooting LAN Switching.")

NOTE This chapter defers any detailed troubleshooting of routing protocols until Chapter 11, "Troubleshooting Routing Protocols."

Isolating IP Routing Problems Related to Hosts

The troubleshooting process outlined in this chapter separates the troubleshooting steps—one part for the hosts, and one part for the routers. Essentially, for any problem in which two hosts cannot communicate, the first part of this troubleshooting process examines the

issues that might impact each host's ability to send packets to and from its respective default gateway. The second part isolates problems related to how routers forward packets.

The following list outlines the troubleshooting steps focused on testing the host's connectivity to the first router:

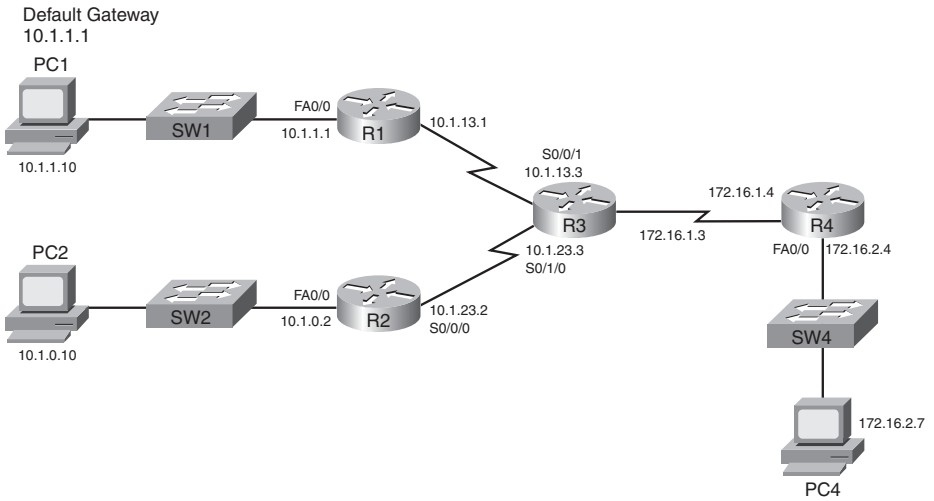
Step 1 Check the host's ability to send packets inside its own subnet. Either ping the host's default gateway IP address from the host, or ping the host's IP address from the default gateway. If the ping fails, do the following:

- **a.** Ensure that the router's interface used at the default gateway is in an "up and up" state.
- **b.** Check the source host's IP address and mask setting as compared to the router's interface used as the default gateway. Ensure that both agree as to the subnet number and mask, and therefore agree to the range of valid addresses in the subnet.
- **c.** If the router uses VLAN trunking, solve any trunk configuration issues, ensuring that the router is configured to support the same VLAN in which the host resides.
- **d.** If the other steps do not lead to a solution, investigate Layer 1/2 problems with the LAN, as covered in Chapter 3. For example, look for an undefined VLAN.

Step 2 Verify the default gateway setting on the host by pinging one of the default router's other interface IP addresses. Or, from the default router, use an extended ping of the host's IP address with a source address from another of the router's interfaces.

For example, in Figure 7-5, the problem symptoms may be that PC1 cannot browse the web server at PC4. To test PC1's ability to send packets over its local subnet, PC1 could use the **ping 10.1.1.1** command to test connectivity to the default router in its same subnet. Or the engineer could simply **ping 10.1.1.10** from R1 (Step 1). Either location for the **ping** works fine, because both ping locations require that a packet be sent in each direction. If the **ping** fails, further problem isolation should uncover the two specific problem areas listed in Steps 1A, 1B, and 1C. If not, the problem is likely to be some Layer 1 or 2 problem, as discussed in Chapter 3.

Figure 7-5 *Sample Network for Troubleshooting Scenarios*



Step 2 stresses an often-overlooked troubleshooting concept to verify that the default gateway setting is working. Neither **ping** option listed in Step 1 requires the host to use its default gateway setting, because the source and destination address in each packet are in the same subnet. Step 2 forces the host to send a packet to an IP address in another subnet, thereby testing the host's default gateway setting. Also, by pinging an IP address on the default gateway (router), instead of some faraway host IP address, this step removes much of the IP routing complexity from the test. Instead, the focus is on whether the host's default gateway setting works. For example, in Figure 7-5, a **ping 10.1.13.1** command on PC1 forces PC1 to use its default gateway setting because 10.1.13.1 is not in PC1's subnet (10.1.1.0/24). But the IP address is on router R1, which removes most of the rest of the network as being a possible cause if the ping fails.

Isolating IP Routing Problems Related to Routers

When the host problem isolation process is complete, and the pings all work, on both the sending and receiving hosts, any remaining IP routing issues should be between the first and last router in both the forward and reverse route between the two hosts. The following list picks up the troubleshooting process with the source host's default gateway/router, relying on the **traceroute** command on the router. (Note that the host's equivalent command, such as **tracert** on Microsoft operating systems, can also be used.)

NOTE Although the following list may be useful for reference, it is rather long. Do not get bogged down in the details, but do read the examples of its use that follow this list; that should clarify many of the steps. As usual, you do not need to memorize any troubleshooting processes listed here. They are meant as learning tools to help you build your skills.

Step 3 Test connectivity to the destination host by using the extended **traceroute** command on the host's default gateway, using the router's interface attached to the source host for the source IP address of the packets. If the command successfully completes:

- **a.** No routing problems exist in the forward route or reverse route directions.
- **b.** If the end-user traffic still does not work (even though the **traceroute** worked), troubleshoot any ACLs on each interface on each router in the route, in both directions.

Step 4 If the **traceroute** command in Step 3 does not complete, test the *forward route* as follows:

- **a.** **telnet** to the last traced router (the last router listed in the **traceroute** command).
- **b.** Find that router's route that matches the destination IP address that was used in the original **traceroute** command (**show ip route**, **show ip route** *ip-address*).
- **c.** If no matching route is found, investigate why the expected route is missing. Typically it's either a routing protocol issue or a static route misconfiguration. It could also be related to a missing connected route.
- **d.** If a matching route is found, and the route is a default route, confirm that it will be used based on the setting for the **ip classless/no ip classless** commands.
- **e.** If a matching route is found, **ping** the next-hop IP address listed in the route. Or, if the route is a connected route, **ping** the true destination IP address.
  - If the **ping** fails, investigate Layer 2 problems between this router and the IP address that was pinged, and investigate possible ACL problems.
  - If the **ping** works, investigate ACL issues.

f. If a matching route is found, and no other problems are found, confirm that the route is not errantly pointing in the wrong direction.

Step 5 If Step 4 does not identify a problem in the forward route, test the *reverse route*:

a. If the forward route on the last traced router refers to another router as the next-hop router, repeat the substeps of Step 3 from that next-hop router. Analyze the reverse route—the route to reach the source IP address used by the failed **traceroute** command.

b. If the forward route on the last traced router refers to a connected subnet, check the destination host's IP settings. In particular, confirm the settings for the IP address, mask, and default gateway.

For example, if PC1 cannot communicate with PC4 in Figure 7-5, and the hosts can both communicate through their respective default gateways, Step 3 of the router-oriented problem isolation process could start with a **traceroute 172.16.2.7**, using R1's Fa0/0 IP address (10.1.1.1) as the source IP address. If that **traceroute** command lists 10.1.13.3 as the last IP address in the command output, rather than completing, you would then start Step 4, which examines R3's forward route toward 172.16.2.7. If the analysis at Step 4 does not uncover the problem, Step 5 would then move on to the next-hop router, R4 in this case, and examine R4's reverse route—its route back to the original source address of 10.1.1.1.

Next, two separate scenarios show how to use these troubleshooting steps to isolate some sample problems.

Troubleshooting Scenario 1: Forward Route Problem

This first example of the router troubleshooting process uses the same internetwork shown in Figure 7-5. In this case, PC1 cannot use a web browser to connect to the web service running on PC4. After further investigation, PC1 cannot ping 172.16.2.7 (PC4). Example 7-2 shows the commands used on R1 and R4 for the host-oriented Steps 1 and 2, as well as a beginning of the router-oriented Step 3.

Example 7-2 *Troubleshooting Scenario 1: Steps 1 and 2 and Part of Step 3*

```
R1#ping 10.1.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
```

Example 7-2 *Troubleshooting Scenario 1: Steps 1 and 2 and Part of Step 3 (Continued)*

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.13.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
Packet sent with a source address of 10.1.13.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

```
! Now moving to R4 to repeat the test
R4#ping 172.16.2.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R4#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.2.4      YES manual administratively down down
FastEthernet0/1        172.16.1.4      YES manual up                    up
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            unassigned      YES unset  administratively down down
Serial0/1/0            unassigned      YES unset  administratively down down
```

The standard and extended pings on R1 at the beginning of the example essentially perform Steps 1 and 2, the host-oriented steps, to confirm that PC1 seems to be working well. However, the example next shows that R4 cannot reach PC4 because R4's LAN interface has been shut down, as shown at the end of the example. Although this scenario may seem a bit simple, it provides a good starting point for troubleshooting a problem.

To get a fuller view of the troubleshooting process, next consider this same scenario, with the same root problem, but now you do not have access to router R4. So, you can only perform Steps 1 and 2 for PC1, which work, but you cannot do those same steps for PC4 from R4. So, Example 7-3 moves on to Steps 3 and 4. The beginning of the example shows Step 3, where R1 uses **traceroute 172.16.2.7**, with a source IP address of 10.1.1.1. This

command does not complete, referencing 10.1.13.3 (R3) as the last router. Step 4 proceeds by looking at how R3 then routes packets destined for 172.16.2.7.

Example 7-3 *Troubleshooting Scenario 1: Step 4*

```
R1#traceroute
Protocol [ip]:
Target IP address: 172.16.2.7
Source address: 10.1.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 172.16.2.7

  1 10.1.13.3 0 msec 4 msec 0 msec
  2 10.1.13.3 !H  *  !H
! Note above that the command did stop by itself, but it does not list the
! destination host 172.16.2.7
R3#show ip route 172.16.2.7
% Subnet not in table
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 4 subnets
C       10.1.13.0 is directly connected, Serial0/0/1
R       10.1.1.0 [120/1] via 10.1.13.1, 00:00:04, Serial0/0/1
R       10.1.0.0 [120/1] via 10.1.23.2, 00:00:01, Serial0/1/0
C       10.1.23.0 is directly connected, Serial0/1/0
```

The extended **traceroute** command at the beginning of the example shows output identifying R3 (10.1.13.3) as the last listed device in the command output (Step 3). Step 4

then proceeds with an examination of the forward route on R3 toward IP address 172.16.2.7. The **show ip route 172.16.2.7** command gets right to the point. The message "subnet not in table" means that R3 does not have a route matching destination address 172.16.2.7. If the question does not supply access to a simulator, only the output of the **show ip route** command, you would need to examine the routes to determine that none of them refer to a range of addresses that includes 172.16.2.7.

Any time the problem isolation process points to a missing route, the next step is to determine how the router should have learned about the route. In this case, R3 should have used RIP-2 to learn the route. So, the next steps would be to troubleshoot any problems with the dynamic routing protocol.

The root cause of this problem has not changed—R4 has shut down its Fa0/0 interface—but the symptoms are somewhat interesting. Because the interface is shut down, R4 does not advertise a route for subnet 172.16.2.0/24 to R3. However, R3 advertises an autosummarized route to network 172.16.0.0/16 to both R1 and R2, so both R1 and R2, because of RIP-2's default autosummary setting, can forward packets destined for 172.16.2.7 to R3. As a result, the **traceroute** command on R1 can forward packets to R3.

Troubleshooting Scenario 2: Reverse Route Problem

This next example uses the same network diagram as shown in Figure 7-5, with all the information shown in the figure still being true. However, the details mentioned in the previous section may have changed—particularly the problem that exists to make the example more interesting. So, approach this second problem only relying on the figure as being true.

In this scenario, PC1 again cannot ping 172.16.2.7 (PC4). The host default gateway checks suggested in Steps 1 and 2 again work for PC1, but the tests cannot be performed for the reverse direction, because the engineer cannot access PC4 or router R4. So, Example 7-4 picks up the suggested troubleshooting process at Step 3, showing the result of the extended **traceroute** command on R1. Note that the command does not even list R3's 10.1.13.3 IP address in this case. So, the rest of Example 7-4 shows the investigations into the specific substeps of Step 4.

Example 7-4 *Troubleshooting Scenario 2: Steps 3 and 4*

```
R1#traceroute ip 172.16.2.7 source fa0/0

Type escape sequence to abort.
Tracing the route to 172.16.2.7

  1  *  *  *
  2  *  *  *
  3  *
```

continues

Example 7-4 *Troubleshooting Scenario 2: Steps 3 and 4 (Continued)*

```
R1#show ip route 172.16.2.7
Routing entry for 172.16.0.0/16
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 10.1.13.3 on Serial0/1/0, 00:00:05 ago
  Routing Descriptor Blocks:
  * 10.1.13.3, from 10.1.13.3, 00:00:05 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1

R1#ping 10.1.13.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#show ip access-lists

! Switching to router R3 next
R3#show ip access-lists

R3#
```

The example starts by showing the Step 3 part of the process, with the **traceroute** command only listing lines of asterisks. This means that the command did not successfully identify even the very next router in the route.

Next, moving on to Step 4, the following list outlines the substeps of Step 4 as applied to this example:

Step 4a The example had already begun with a Telnet into R1, so no extra work is required.

Step 4b The next command, **show ip route 172.16.2.7**, shows that R1 has a nondefault route for network 172.16.0.0, pointing to R3 (10.1.13.3) as the next hop.

Step 4c This step does not apply in this case, because a matching route was found in Step 4B.

Step 4d This step does not apply in this case, because the matching route is not a route to 0.0.0.0/0 (the default route).

Step 4e The next listed command, **ping 10.1.13.3**, tests R1's ability to send packets over the link to the next-hop router identified in Step 4B. The ping works.

Step 4f On both R1 and the next-hop router (R3), the **show ip access-lists** command confirms that neither router has any IP ACLs configured.

Because all the steps to examine the forward route passed, the process then moves on to Step 5. The original **traceroute** command in Example 7-4 used R1's Fa0/0 interface IP address, 10.1.1.1, as the source IP address. For Step 5, the process begins at R3 with an analysis of R3's reverse route to reach 10.1.1.1. Examine the output in Example 7-5, and look for any problems before reading the explanations following the example.

Example 7-5 *Troubleshooting Scenario 2: Step 5*

```
! The next command shows the matched route, for subnet 10.1.1.0/26,
! with next-hop 10.1.23.2.
R3#show ip route 10.1.1.1
Routing entry for 10.1.1.0/26
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.1.23.2
      Route metric is 0, traffic share count is 1

! The next command shows the overlapping subnets - 10.1.1.0/26 and 10.1.1.0/24.
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
R       172.16.2.0 [120/1] via 172.16.1.4, 00:00:18, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.13.0/24 is directly connected, Serial0/0/1
S       10.1.1.0/26 [1/0] via 10.1.23.2
R       10.1.1.0/24 [120/1] via 10.1.13.1, 00:00:10, Serial0/0/1
R       10.1.0.0/24 [120/1] via 10.1.23.2, 00:00:11, Serial0/1/0
C       10.1.23.0/24 is directly connected, Serial0/1/0
```

R3 has an incorrectly configured static route for subnet 10.1.1.0/26. This subnet includes the address range 10.1.1.0–10.1.1.63, which includes IP address 10.1.1.1. When R3 attempts to send a packet back to 10.1.1.1, R3 has two routes that match the destination address. But R3 picks the more specific (longer prefix) route for subnet 10.1.1.0/26. This route causes R3 to forward packets intended for 10.1.1.1 out R3's link to R2, instead of to R1.

Although you cannot necessarily determine the true intent of this static route, this process has identified the root cause—the static route to 10.1.1.0/26 on R3. If the LAN off R1 should include all addresses between 10.1.1.0 and 10.1.1.255, the static route should just be deleted.

An Alternative Problem Isolation Process for Steps 3, 4, and 5

The router-oriented steps of the IP routing problem isolation process depend on the **traceroute** command, relying on this command's ability to identify on which router the router-oriented troubleshooting should begin. As an alternative, the **ping** and **telnet** commands can be used. However, because these commands cannot quickly identify the most likely routers on which the problem exists, using **ping** and **telnet** requires that you perform a set of tasks on the first router (the host's default gateway/router) in a route, and then the next router, and the next, and so on, until the problem is identified.

So, just to be complete, note that you can do the same specific subtasks as already explained in Steps 4 and 5, but when using **ping**, just repeat the steps at each successive router. For example, to apply this revised process to the first of the two just-completed scenarios, the process would begin with router R1, PC1's default router. In the first scenario, R1 did not have any forward route issues for forwarding packets to 172.16.2.7 (PC4), and R1 had no reverse route issues and no ACLs. This new alternative process would then suggest moving on to the next router (R3). In this example, R3's forward route problem—not having a route that matches destination address 172.16.2.7—would be found.

Troubleshooting Tools and Tips

The second half of this chapter covers a wide variety of troubleshooting tools and tips that can be helpful when you're troubleshooting real networks. Some of the information in this section may apply directly to the CCNA exams. Other parts of this section will be indirectly useful for the exams. The information may help you learn as you work with networks in your job, making you better prepared for the unique scenarios on the exams.

Host Routing Tools and Perspectives

This section covers two short topics related to how hosts process IP packets. The first topic lists several tips for troubleshooting hosts. The second topic reviews information covered in *CCENT/CCNA ICND1 Official Exam Certification Guide* on how a LAN switch's IP configuration works like a host.

Host Troubleshooting Tips

When you're trying to isolate the cause of networking problems, the tips in Table 7-4 may help you more quickly find problems related to hosts. The tips are organized by typical symptoms, along with common root causes. Note that the table does not list all possible causes, just the more common ones.

Table 7-4 *Common Host Problem Symptoms and Typical Reasons*

Symptom	Common Root Cause
The host can send packets to hosts in the same subnet, but not to other subnets.	The host does not have a default gateway configured, or the default gateway IP address is incorrect.
The host can send packets to hosts in the same subnet, but not to other subnets.	The host's default gateway is in a different subnet than the host's IP address (according to the host's perception of the subnet).
Some hosts in a subnet can communicate with hosts in other subnets, but others cannot.	This may be caused by the default gateway (router) using a different mask than the hosts. This may result in the router's connected route not including some of the hosts on the LAN.
Some hosts on the same VLAN can send packets to each other, but others cannot.	The hosts may not be using the same mask.

When troubleshooting networking problems in real life, it's helpful to get used to thinking about the symptoms, because that's where the problem isolation process typically begins. However, for the exams, most host communication problems are caused by just a handful of issues:

Step 1 Check all hosts and routers that should be in the same subnet to ensure that they all use the same mask and that their addresses are indeed all in the same subnet.

Step 2 Compare each host's default gateway setting with the router's configuration to ensure that it is the right IP address.

Step 3 If the first two items are correct, next look at Layer 1/2 issues, as covered in Chapters 1 through 3.

LAN Switch IP Support

Ethernet switches do not need to know anything about Layer 3 to perform their basic Layer 2 function of forwarding Ethernet frames. However, to support several important features, such as the ability to telnet and SSH to the switch to troubleshoot problems, LAN switches need an IP address.

Switches act like hosts when it comes to IP configuration. As compared to a PC, a Cisco switch does not use a NIC. Instead, it uses an internal virtual interface associated with VLAN 1 that essentially gives the switch itself an interface in VLAN 1. Then, the same kinds of items that can be configured on a host for IP can be configured on this VLAN interface: IP address, mask, and default gateway. DNS server IP addresses can also be configured.

The following list repeats the LAN switch IP configuration checklist from *CCENT/CCNA ICND1 Official Exam Certification Guide*. Following the list, Example 7-6 shows the IP address configuration for switch SW1 in Figure 7-5 from earlier in the chapter.

Step 1 Enter VLAN 1 configuration mode using the **interface vlan 1** global configuration command (from any config mode).

Step 2 Assign an IP address and mask using the **ip address** *ip-address mask* interface subcommand.

Step 3 Enable the VLAN 1 interface using the **no shutdown** interface subcommand.

Step 4 Add the **ip default-gateway** *ip-address* global command to configure the default gateway.

Example 7-6 *Switch Static IP Address Configuration*

```
SW1#configure terminal
SW1(config)#interface vlan 1
SW1(config-if)#ip address 10.1.1.200 255.255.255.0
SW1(config-if)#no shutdown
00:25:07: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:25:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
  state to up
SW1(config-if)#exit
SW1(config)#ip default-gateway 10.1.1.1
```

NOTE The VLAN interface on a switch stays in an administratively down state until the user issues the **no shutdown** command; the switch cannot send IP packets until the VLAN 1 interface is up.

A common oversight when configuring or troubleshooting IP connectivity problems to LAN switches relates to VLAN trunking. Cisco generally suggests that you avoid putting end-user devices into VLAN 1, but the switch IP address may well be configured in VLAN 1. To support the ability for the switch to send and receive packets to hosts in different subnets, thereby supporting Telnet into the switch from those end-user subnets, the router's trunking configuration must include configuration for VLAN 1 as well as the end-user VLANs.

show ip route Reference

The **show ip route** command plays a huge role in troubleshooting IP routing and IP routing protocol problems. Many chapters in this book and in the ICND1 book mention various facts about this command. This section pulls the concepts together in one place for easier reference and study.

Figure 7-6 shows the output of the **show ip route** command from back in Example 7-3. The figure numbers various parts of the command output for easier reference, with Table 7-5 describing the output noted by each number.

Figure 7-6 **show ip route** *Command Output Reference*

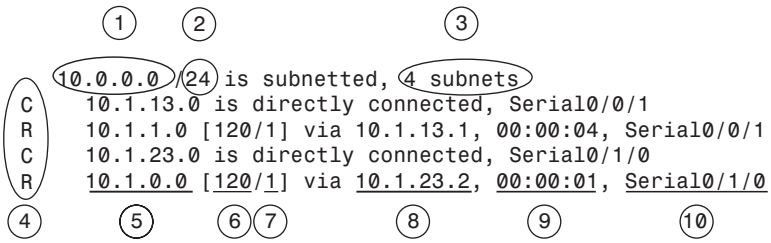


Table 7-5 *Descriptions of the* **show ip route** *Command Output*

Item Number	Item	Value in the Figure	Description
1	Classful network	10.0.0.0	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0.0.
2	Prefix length	/24	When this router knows only one subnet mask for all subnets of the network, this location lists that one mask, by default in prefix notation.
3	Number of subnets	4 subnets	Lists the number of routes for subnets of the classful network known to this router.
4	Legend code	R, C	A short code that identifies the source of the routing information. R is for RIP, and C is for connected. The figure omits the legend text at the top of the **show ip route** command output, but it can be seen in Example 7-3.
5	Subnet number	10.1.0.0	The subnet number of this particular route.
6	Administrative distance	120	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest AD.
7	Metric	1	The metric for this route.
8	Next-hop router	10.1.23.2	For packets matching this route, the IP address of the next router to which the packet should be forwarded.
9	Timer	00:00:01	Time since this route was learned in a routing update.
10	Outgoing interface	Serial0/1/0	For packets matching this route, the interface out which the packet should be forwarded.

The output of the command differs slightly when VLSM is used. The figure shows an example in which VLSM is not used in network 10.0.0.0, with mask /24 used for all subnets of that network. So, IOS lists the mask once, in the heading line (/24 in this case). If VLSM were in use, the heading line would simply note that the network is variably subnetted, and each route would list the mask. For an example, see Example 5-1 in Chapter 5, "VLSM and Route Summarization."

Interface Status

One of the steps in the IP routing troubleshooting process described earlier, in the "Troubleshooting the Packet Forwarding Process" section, says to check the interface status, ensuring that the required interface is working. For a router interface to be working, the two interface status codes must both be listed as "up," with engineers usually saying the interface is "up and up."

This chapter does not explain the troubleshooting steps for router interfaces, simply assuming that each interface is indeed in an up/up state. Chapter 12's section titled "Troubleshooting Serial Links" covers many of the details for troubleshooting router interfaces. For router LAN interfaces connected to a LAN switch, the main items to check on routers are that the router and switch match each other's duplex and speed settings, and that if trunking is configured, both the router and switch have been manually configured for trunking, because routers do not dynamically negotiate LAN trunking.

VLSM Issues

This section examines several issues when using VLSM:

- Recognizing whether VLSM is used and, if so, which routing protocols can be used
- Understanding the conditions in which routers can allow the misconfiguration of overlapping VLSM subnets
- Understanding the outward symptoms that can occur when overlapping VLSM subnets exist

Recognizing When VLSM Is Used

One common oversight when troubleshooting a problem in an unfamiliar internetwork is failing to recognize whether VLSM is used. As defined in Chapter 5, an internetwork uses VLSM when multiple subnet masks are used for different subnets of *a single classful network*. For example, if in one internetwork all subnets of network 10.0.0.0 use a 255.255.240.0 mask, and all subnets of network 172.16.0.0 use a 255.255.255.0 mask, the design does not use VLSM. If multiple masks were used for subnets of network 10.0.0.0, VLSM would be in use.

The follow-on concept is that only classless routing protocols (RIP-2, EIGRP, OSPF) can support VLSM; classful routing protocols (RIP-1, IGRP) cannot. So, a quick determination of whether VLSM is actually used can then tell you whether a classless routing protocol is required. Note that the routing protocol does not require any special configuration to support VLSM. It is just a feature of the routing protocol.

Configuring Overlapping VLSM Subnets

IP subnetting rules require that the address ranges in the subnets used in an internetwork should not overlap. IOS can recognize when a new **ip address** command creates an overlapping subnet, but only in some cases. This section examines the conditions under which overlapping subnets can be configured, beginning with the following general statements about when the overlaps cannot and can be configured:

- **Preventing the overlap:** IOS detects the overlap when the **ip address** command implies an overlap with another **ip address** command *on the same router*. If the interface being configured is up/up, IOS rejects the **ip address** command. If not, IOS accepts the **ip address** command, but IOS will never bring up the interface.
- **Allowing the overlap:** IOS cannot detect an overlap when an **ip address** command overlaps with an **ip address** command on another router.

The router shown in Example 7-7 prevents the configuration of an overlapping VLSM subnet. The example shows router R3 configuring Fa0/0 with IP address 172.16.5.1/24, and Fa0/1 with 172.16.5.193/26. The ranges of addresses in each subnet are:

Subnet 172.16.5.0/24: 172.16.5.1– 172.16.5.254
Subnet 172.16.5.192/26: 172.16.5.193–172.16.5.254

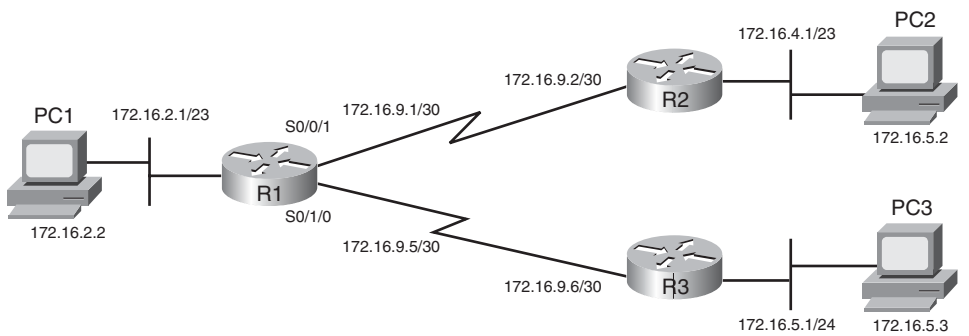
Example 7-7 *Single Router Rejects Overlapped Subnets*

```
R3#configure terminal
R3(config)#interface Fa0/0
R3(config-if)#ip address 172.16.5.1 255.255.255.0
R3(config-if)#interface Fa0/1
R3(config-if)#ip address 172.16.5.193 255.255.255.192
% 172.16.5.192 overlaps with FastEthernet0/0
R3(config-if)#
```

IOS knows that it is illegal to overlap the ranges of addresses implied by a subnet. In this case, because both subnets would be connected subnets, this single router knows that these two subnets should not coexist, because that would break subnetting rules, so IOS rejects the second command.

However, it is possible to configure overlapping subnets if they are connected to different routers. Figure 7-7 shows a figure very similar to Figure 5-2 in Chapter 5—used in that chapter to explain the problem of overlapping subnets. Example 7-8 shows the configuration of the two overlapping subnets on R2 and R3, with the resulting routing table on R2.

Figure 7-7 *Internetwork That Allows the Configuration of Overlapped Subnets*



Example 7-8 *Two Routers Accept Overlapped Subnets*

```
R2#configure terminal
R2(config)#interface Fa0/0
R2(config-if)#ip address 172.16.4.1 255.255.254.0
```

```
R3#configure terminal
R3(config)#interface Fa0/0
R3(config-if)# ip address 172.16.5.1 255.255.255.0
```

For the exams, keep in mind that overlapped subnets can be configured if the subnets do not connect to the same router. So, if a question asks you to pick a new subnet number and configure an interface to be in that subnet, the router's acceptance of your **ip address** command does not necessarily tell you that you did the math correctly.

The next topic explains some of the problem symptoms you might see if such an overlap exists.

Symptoms with Overlapping Subnets

> **NOTE** Although this section is included for the sake of completeness, the types of problems described here may well be beyond the scope of the CCNA exams.

The outward problem symptoms differ depending on whether the address in question is in the overlapped portion of the subnets and if multiple hosts are attempting to use the exact same IP address. The addresses in the nonoverlapped parts of the subnet typically work fine, whereas those in the overlapped area may or may not work at all. For example, continuing with the overlapped subnets shown in Figure 7-6, subnets 172.16.4.0/23 and 172.16.5.0/24 overlap—specifically, addresses 172.16.5.0–172.16.5.255. Hosts in the nonoverlapped range of 172.16.4.0–172.16.4.255 probably work fine.

For the addresses in the overlapped address range, in many cases, hosts in the smaller of the two overlapped subnets work fine, but hosts in the larger of the two subnets do not. To see why, consider the case in which PC1 in Figure 7-7 tries to ping both 172.16.5.2 (PC2, off R2) and 172.16.5.3 (PC3, off R3). (For the sake of this example, assume that PC2's and PC3's IP addresses are not duplicated in the opposite overlapped subnet.) As you can see from the routing tables on R1 and R3 and the **traceroute 172.16.5.2** command in Example 7-9, the packet sent by PC1 to PC2 would actually be delivered from R1 to R3, and then onto R3's LAN.

Example 7-9 *Two Routers Accept Overlapped Subnets*

```
! R1's route to reach 172.16.5.2, off R2, points to R3
R1#show ip route 172.16.5.2
Routing entry for 172.16.5.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 172.16.9.6 on Serial0/1/0, 00:00:25 ago
  Routing Descriptor Blocks:
  * 172.16.9.6, from 172.16.9.6, 00:00:25 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1
! R1's route to reach 172.16.5.3, off R3, points to R3
R1#show ip route 172.16.5.3
Routing entry for 172.16.5.0/24
  Known via "rip", distance 120, metric 1
```

continues

Example 7-9 *Two Routers Accept Overlapped Subnets (Continued)*

```
  Redistributing via rip
  Last update from 172.16.9.6 on Serial0/1/0, 00:00:01 ago
  Routing Descriptor Blocks:
  * 172.16.9.6, from 172.16.9.6, 00:00:01 ago, via Serial0/1/0
      Route metric is 1, traffic share count is 1

! The traceroute to PC2 shows R3, not R2, as the first router, so the packet never
! reaches PC2, and the command never completes until stopped by the user.
R1#traceroute 172.16.5.2

Type escape sequence to abort.
Tracing the route to 172.16.5.2

  1 172.16.9.6 4 msec 0 msec 4 msec
  2  *  *  *
  3  *  *  *
  4
R1#traceroute 172.16.5.3

Type escape sequence to abort.
Tracing the route to 172.16.5.3

  1 172.16.9.6 0 msec 4 msec 0 msec
  2 172.16.5.3 4 msec *  0 msec
```

The example shows that R1 forwards packets to hosts 172.16.5.2 (PC2) and 172.16.5.3 (PC3) by sending them to R3 next. R3 then tries to send them onto R3's LAN subnet, which works well for PC3 but not so well for PC2. So, PC3, in the smaller of the two overlapped subnets, works fine, whereas PC2, in the larger of the two overlapped subnets, does not.

The symptoms can get even worse when addresses are duplicated. For example, imagine that PC22 has been added to R2's LAN subnet, with IP address 172.16.5.3 duplicating PC3's IP address. Now when the PC22 user calls to say that his PC cannot communicate with other devices, the network support person uses a **ping 172.16.5.3** to test the problem—and the ping works! The ping works to the wrong instance of 172.16.5.3, but it works. So, the symptoms may be particularly difficult to track down.

Another difficultly with overlapped VLSM subnets is that the problem may not show up for a while. In this same example, imagine that all addresses in both subnets were to be assigned by a DHCP server, beginning with the smallest IP addresses. For the first six months, the server assigned only IP addresses that began with 172.16.4.*x* on the R2 LAN subnet. Finally, enough hosts were installed on the R2 LAN to require the use of addresses that begin with 172.16.5, like PC2's address of 172.16.5.2 used in the preceding example.

Unfortunately, no one can send packets to those hosts. At first glance, the fact that the problem showed up long after the installation and configuration were complete may actually cloud the issue.

VLSM Troubleshooting Summary

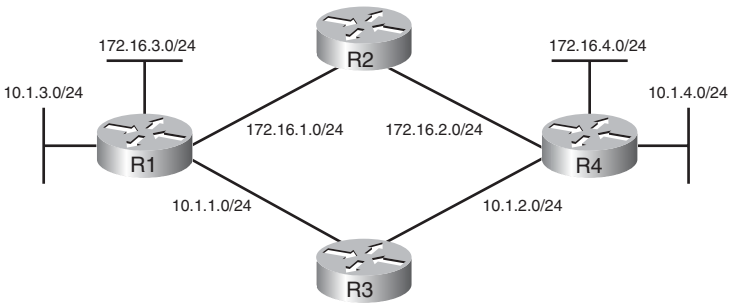
The following list summarizes the key troubleshooting points to consider when you're troubleshooting potential VLSM problems on the exams:

- Pay close attention to whether the design really uses VLSM. If it does, note whether a classless routing protocol is used.
- Be aware that overlapping subnets can indeed be configured.
- The outward problem symptoms may be that some hosts in a subnet work well, but others cannot send packets outside the local subnet.
- Use the **traceroute** command to look for routes that direct packets to the wrong part of the network. This could be a result of the overlapped subnets.
- On the exams, you might see a question you think is related to VLSM and IP addresses. In that case, the best plan of attack may well be to analyze the math for each subnet and ensure that no overlaps exist, rather than troubleshooting using **ping** and **traceroute**.

Discontiguous Networks and Autosummary

Chapter 5 explained the concept of discontiguous networks, along with the solution: using a classless routing protocol with autosummarization disabled. This section examines one particular case in which a discontiguous network exists only part of the time. Figure 7-8 shows an internetwork with two classful networks: 10.0.0.0 and 172.16.0.0. The design shows two contiguous networks because a route consisting of only subnets of each network exists between all subnets of that network.

Figure 7-8 *Internetwork with (Currently) Contiguous Networks*



In this figure, with all links up and working, using a routing protocol with autosummary enabled by default, all hosts can ping all other hosts. In this design, packets for network 172.16.0.0 flow over the high route, and packets for network 10.0.0.0 flow over the low route.

Unfortunately, a problem can occur later when one of the four links between routers fails. If any link between the routers fails, one of the two classful networks becomes discontiguous. For example, if the link between R3 and R4 fails, the route from R1 to R4 passes through subnets of network 172.16.0.0, so network 10.0.0.0 is discontiguous. Even with a classless routing protocol, but with autosummarization enabled, both R1 and R4 advertise a route for 10.0.0.0/8 to R2, and R2 sees two routes to all of network 10.0.0.0—one through R1, and another through R4. The solution, as always, is to use a classless routing protocol with autosummary disabled.

Although the design in Figure 7-8 may seem a bit contrived, it happens more often than you might think—particularly as companies are bought and sold. Both for real life and the exams, keep the concept of discontiguous networks in mind for normal working cases and for cases in which redundant links fail.

Access List Troubleshooting Tips

Troubleshooting problems that are impacted by ACLs may well be one of the most difficult tasks for real networking jobs. One of the major difficulties is that the traditional troubleshooting tools such as **ping** and **traceroute** do not send packets that look like the packets matched by the variety of fields in extended ACLs. So, although a **ping** may work, the end-user host may not be able to get to the right application, or vice versa.

This section summarizes some tips for attacking ACL-related problems in real life and on the exams:

Key Topic

Step 1 Determine on which interfaces ACLs are enabled, and in which direction (**show running-config, show ip interfaces**).

Step 2 Determine which ACL statements are matched by test packets (**show access-lists, show ip access-lists**).

Step 3 Analyze the ACLs to predict which packets should match the ACL, focusing on the following points:

- **a.** Remember that the ACL uses first-match logic.
- **b.** Consider using the (possibly) faster math described in Chapter 6, "IP Access Control Lists," which converts ACL address/wildcard mask pairs into address/subnet mask pairs that allow the use of the same math as subnetting.
- **c.** Note the direction of the packet in relation to the server (going to the server, coming from the server). Make sure that the packets have particular values as either the source IP address and port, or as the destination IP address and port, when processed by the ACL enabled for a particular direction (in or out).
- **d.** Remember that the **tcp** and **udp** keywords must be used if the command needs to check the port numbers. (See Table 6-5 in Chapter 6 for a list of popular TCP and UDP port numbers.)
- **e.** Note that ICMP packets do not use UDP or TCP. ICMP is considered to be another protocol matchable with the **icmp** keyword (instead of **ip**, **tcp**, and **udp**).
- **f.** Instead of using the implicit deny any at the end of each ACL, use an explicit configuration command to deny all traffic at the end of the ACL so that the **show** command counters increment when that action is taken.

Chapter 6 covered the background information behind the tips listed in Step 3. The remainder of this section focuses on commands available for you to investigate problems in the first two steps.

If a problem in forwarding IP packets is occurring, and existing ACLs may be impacting the problem, the first problem isolation step is to find the location and direction of the ACLs. The fastest way to do this is to look at the output of the **show running-config** command and to look for **ip access-group** commands under each interface. However, in some cases, enable mode access may not be allowed, and **show** commands are required. The only way to find the interfaces and direction for any IP ACLs is the **show ip interfaces** command, as shown in Example 7-10.

Example 7-10 *Sample* **show ip interface** *Command*

```
R1>show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.2.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set
  Inbound  access list is 102
! roughly 26 more lines omitted for brevity
```

Note that the command output lists whether an ACL is enabled, in both directions, and which ACL it is. The example shows an abbreviated version of the **show ip interface S0/0/1** command, which lists messages for just this one interface. The **show ip interface** command would list the same messages for every interface in the router.

Step 2 then says that the contents of the ACL must be found. Again, the most expedient way to look at the ACL is to use the **show running-config** command. If enable mode is not allowed, the **show access-lists** and **show ip access-lists** commands give the same output. The only difference is that if other non-IP ACLs have been configured, the **show access-lists** command lists the non-IP ACLs as well. The output provides the same details shown in the configuration commands, as well as a counter for the number of packets matching each line in the ACL. Example 7-11 shows an example.

Example 7-11 *Sample* **show ip access-lists** *Command*

```
R1#show ip access-lists
Extended IP access list 102
    10 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255 (15 matches)
```

After the locations, directions, and configuration details of the various ACLs have been discovered in Steps 1 and 2, the hard part begins—interpreting what the ACL really does. Of particular interest is the last item in the troubleshooting tips list, item 3E. In the ACL shown in Example 7-11, some packets (15 so far) have matched the single configured **access-list** statement in ACL 102. However, some packets have probably been denied because of the implied deny all packets logic at the end of an ACL. By configuring the **access-list 102 deny ip any any** command at the end of the ACL, which explicitly matches all packets and discards them, the **show ip access-lists** command would then show the number of packets being denied at the end of the ACL. Cisco sometimes recommends adding the explicit deny all statement at the end of the ACL for easier troubleshooting.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, noted with the key topics icon. Table 7-6 lists these key topics and where each is discussed.

Table 7-6 *Key Topics for Chapter 7*

Key Topic Element	Description	Page Number
Table 7-1	Popular ICMP messages and their purpose	271
Figure 7-3	Diagram of how the TTL IP header field and the ICMP Time Exceeded message work	275
Figure 7-4	Demonstration of how the **traceroute** command uses the TTL field and Time Exceeded message	277
List	Two major steps and several substeps in a suggested host routing problem isolation process	279
List	Three major steps for problem isolation with IP routing in routers, with the list numbered as a continuation of the host routing problem isolation list	281
List	Three tips for general items to check when troubleshooting host connectivity problems	289
List	Configuration step list for LAN switch IP details	290
List	Conditions under which overlapping subnets can be configured, and when IOS can prevent this error	293
List	Summary of troubleshooting tips for questions in which VLSM may be causing a problem	297
List	Three steps for troubleshooting ACL problems, particularly when the configuration cannot be displayed	298-299

Complete the Tables and Lists from Memory

Print a copy of Appendix J, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix K, "Memory Tables Answer Key," also on the CD, includes completed tables and lists for you to check your work.

Definitions of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

Forward route, reverse route

Index

NUMBERS

A

B - C

D

E

F

G - H - I

J - K - L

M

N

Q - R

S

T

U -V

W -X -Y -Z