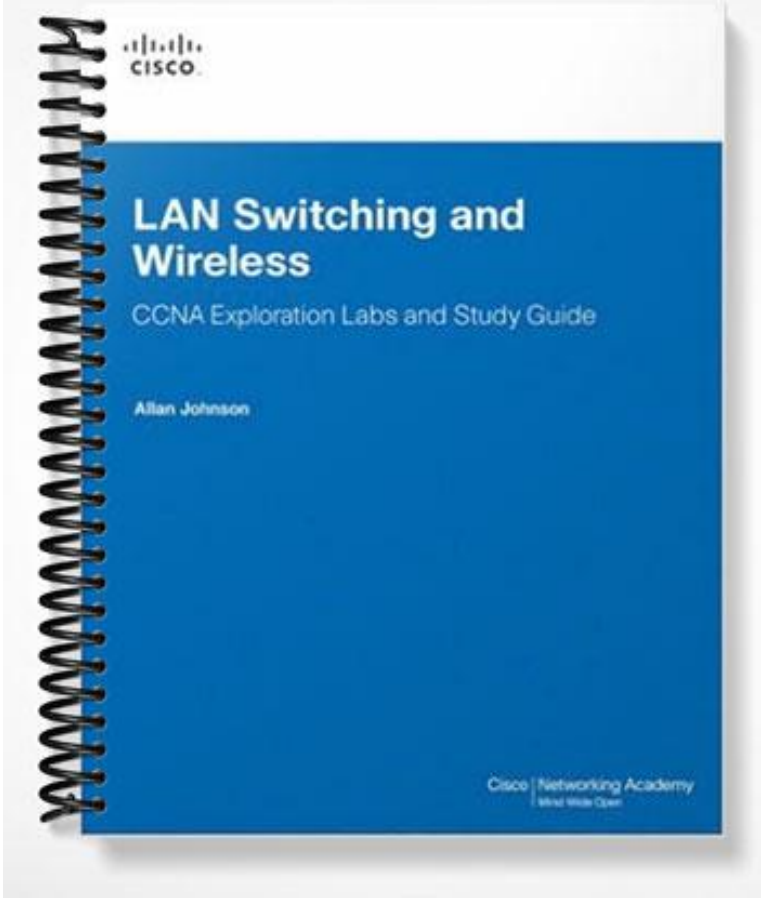
SOLUTIONS MANUAL



LAN Switching and Wireless

CCNA Exploration Labs and Study Guide

Instructor's Edition

Allan Johnson

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

LAN Switching and Wireless

CCNA Exploration Labs and Study Guide Instructor's Edition

Allan Johnson

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

Printed in the United States of America

First Printing April 2008

ISBN-13: 978-1-58705-582-9

ISBN-10: 1-58705-582-1

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Executive Editor
Mary Beth Ray

Production Manager
Patrick Kanouse

Development Editor
Andrew Cupp

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Technical Editors
Bruce R. Gottwig
Khalid Rubayi
Tara Skibar
Linda C. Watson

Editorial Assistant
Vanessa Evans

Book and Cover Designer
Louisa Adair

Composition
Mark Shirar

Proofreader
Leslie Joseph

Warning and Disclaimer

This book is designed to provide information about LAN switching and wireless as part of the Cisco Networking Academy CCNA Exploration curriculum. 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 e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

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.

About the Author

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed. in occupational training and development. He is an information technology instructor at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for the Academy in Learning Systems Development.

About the Technical Reviewers

Bruce R. Gottwig has spent most of his professional career teaching both at the K–12 and post-secondary levels. He earned an M.Ed. in Educational Technology and is currently working toward an Ed.D. in Educational Leadership. He is currently the curriculum lead and instructor for the Computer Information Technology Network support degree and certification program at Montana State University–Great Falls. Since 1998 he has also been an instructor and program director for the Montana State University–Great Falls Local, Regional Cisco Networking Academy and Cisco Academy Training Center for Sponsored Curriculum. He also teaches for Lesley University in its M.Ed. program in Educational Technology. Throughout his years in educational technology, Bruce has earned his CCNA, CCNP, CompTIA A+, Network+, Server+, and World Organization of Webmasters CPW certifications and continues to learn and pass his learning to others.

Khalid Rubayi teaches courses for the Electronics and Computer Technology Department at Victor Valley Community College in Victorville, California. He teaches all networking courses offered by the Cisco Networking Academy, including CCNA, CCNP, Security, and Wireless. He has a BS and MS in Electrical Engineering from Northrop University. He holds CCNA, CCNP, and CCAI certifications.

Tara Skibar, CCNP, was first introduced to networking in 1994 when she enlisted in the Air Force. After serving for four years as a network technician, she became an instructor. Tara has worked with major telecom companies in the United States and Europe. She has worked for the Cisco Networking Academy since 2003 as a subject matter expert for the CCNP assessment development team and for the CCNP certification exams. Most recently, Tara was the assessment lead for the newly modified CCNA curriculum and traveled with a group of development folks to Manila, Philippines, for the small market trial. Tara has a BS in Information Technology and is working toward a master's in Information Systems.

Linda C. Watson has been involved with the Cisco Networking Academy for ten years. She began as a student in version 1.1, and in the last eight years has been an instructor and director of the Academy program at Chandler-Gilbert Community College in Chandler, Arizona. After completing her own career change, she especially enjoys helping students transition from novices in the networking field to certified IT professionals. Linda has an MBA from Arizona State University and holds CCNA, CCAI, A+, and MCSE certifications.

Dedication

For my wife, Becky. Without the sacrifices you made during the project, this work would not have come to fruition. Thank you for providing me the comfort and resting place only you can give.

Acknowledgments

The reader will certainly benefit from the many hours devoted to this effort by the technical editors. A team of no less than four people served admirably as my second pair of eyes, finding and correcting technical inaccuracies and grammatical errors. Thank you Bruce Gottwig, Khalid Rubayi, Tara Skibar, and Linda Watson for doing an outstanding job.

Mary Beth Ray, executive editor, you amaze me with your ability to juggle multiple projects at once, steering each from beginning to end. I can always count on you to make the tough decisions.

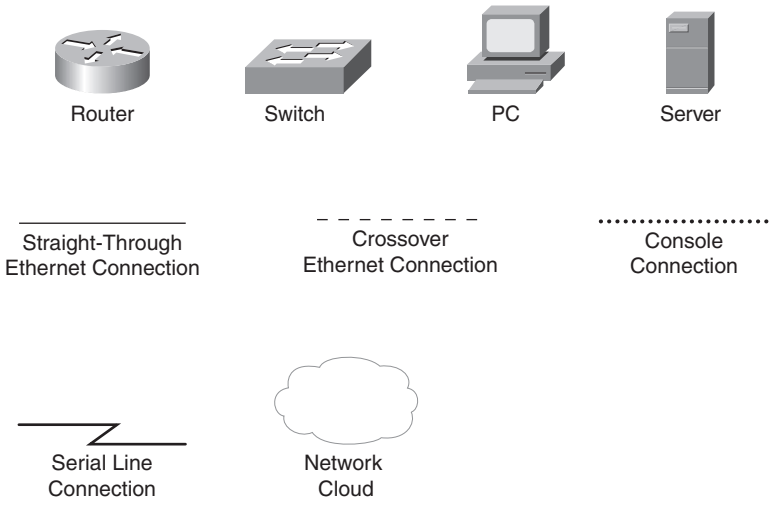
This is my second project with Andrew Cupp as development editor. His dedication to perfection pays dividends in countless, unseen ways. Thank you again, Drew, for providing me with much-needed guidance and support. This book could not be a reality without your persistence.

Last, I cannot forget to thank all my students—past and present—who have helped me over the years to create engaging and exciting activities and labs. There is no better way to test the effectiveness of an activity or lab than to give it to a team of dedicated students. They excel at finding the obscurest of errors! I could have never done this without all your support.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

The Cisco Networking Academy is a comprehensive e-learning program that provides students with Internet technology skills. A Networking Academy delivers web-based content, online assessment, student performance tracking, and hands-on labs to prepare students for industry-standard certifications. The CCNA curriculum includes four courses oriented around the topics on the Cisco Certified Network Associate (CCNA) certification.

LAN Switching and Wireless, CCNA Exploration Labs and Study Guide is a supplement to your classroom and laboratory experience with the Cisco Networking Academy. In order to be successful on the exam and achieve your CCNA certification, you should do everything in your power to arm yourself with a variety of tools and training materials to support your learning efforts. This Labs and Study Guide is just such a collection of tools. Used to its fullest extent, it will help you gain the knowledge and practice the skills associated with the content area of the CCNA Exploration LAN Switching and Wireless course. Specifically, this book will help you work on these main areas:

- LAN design principles and concepts
- Ethernet operation with switches
- Basic switch configuration and security
- VLAN concepts and configuration
- VTP concepts and configuration
- STP, RSTP, and rapid PVST+ concepts and configuration
- Inter-VLAN routing concepts and configuration
- LAN wireless concepts and security issues
- LAN wireless configuration using Linksys WRT300N routers
- Troubleshooting LAN switching and wireless configurations

Labs and Study Guides similar to this one are also available for the other three courses: *Network Fundamentals, CCNA Exploration Labs and Study Guide*, *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*, and *Accessing the WAN, CCNA Exploration Labs and Study Guide*.

Audience for This Book

This book's main audience is anyone taking the *CCNA Exploration LAN Switching and Wireless course* of the Cisco Networking Academy curriculum. Many Academies use this book as a required tool in the course, while other Academies recommend the Labs and Study Guides as an additional source of study and practice materials.

The secondary audiences for this book include people taking CCNA-related classes from professional training organizations. This book can also be used for college- and university-level networking courses, as well as anyone wanting to gain a detailed understanding of basic switching and wireless technologies.

Goals and Methods

The most important goal of this book is to help you pass the CCNA exam (640-802). Passing this foundation exam means that you not only have the required knowledge of the technologies covered by the exam, but that you can plan, design, implement, operate, and troubleshoot these technologies. In other words, these exams are rigorously application based. You can view the exam topics any time at http://www.cisco.com/go/certifications. The topics are divided into eight categories:

- Describe how a network works
- Configure, verify, and troubleshoot a switch with VLANs and inter-switch communications
- Implement an IP addressing scheme and IP services to meet network requirements in a medium-sized enterprise branch office network
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices
- Explain and select the appropriate administrative tasks required for a WLAN
- Identify security threats to a network and describe general methods to mitigate those threats
- Implement, verify, and troubleshoot NAT and ACLs in a medium-sized enterprise branch office network
- Implement and verify WAN links

The LAN Switching and Wireless course focuses on the second, fifth, and sixth bullets.

The Study Guide portion of each chapter offers exercises that help you learn the LAN switching and wireless concepts as well as the configurations crucial to your success as a CCNA exam candidate. Each chapter is slightly different and includes some or all of the following types of exercises:

- Vocabulary matching and completion
- Skill-building activities and scenarios
- Configuration scenarios
- Concept questions
- Internet research

Packet Tracer ☐ Activity

In the configuration chapters, you'll find many Packet Tracer Activities that work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in this book's CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

The Labs and Activities portion of each chapter includes a Command Reference table, all the online Curriculum Labs, and a Packet Tracer Skills Integration Challenge Activity. The Curriculum Labs are divided into three categories:

- **Basic:** The Basic Labs are procedural in nature and assume you have no experience configuring the technologies that are the topic of the lab.
- **Challenge:** The Challenge Labs are implementation in nature and assume you have a firm enough grasp on the technologies to "go it alone." These labs often only give you a general requirement that you must implement fully without the details of each small step. In other words, you must use the knowledge and skills you gained in the chapter text, activities, and Basic Lab to successfully complete the Challenge Labs. Avoid the temptation to work through

the Challenge Lab by flipping back through the Basic Lab when you are not sure of a command. Do not try to short-circuit your CCNA training. You need a deep understanding CCNA knowledge and skills to ultimately be successful on the CCNA exam.

- **Troubleshooting:** The Troubleshooting Labs will ask you to fix a broken network. These labs include corrupted scripts you purposefully load onto the routers. Then you use troubleshooting techniques to isolate problems and implement a solution. By the end of the lab, you should have a functional network with full end-to-end connectivity.

Most of the hands-on labs include Packet Tracer Companion Activities where you can use Packet Tracer to complete a simulation of the lab.

Each chapter also includes a culminating activity called the Packet Tracer Skills Integration Challenge**.** These activities require you to pull together several skills learned from the chapter—and from previous chapters and courses—to successfully complete one comprehensive exercise.

A Word About Packet Tracer

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This "e-doing" capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer v4.x is available only to Cisco Networking Academies through the Academy Connection website.

How This Book Is Organized

Because the content of *LAN Switching and Wireless, CCNA Exploration Companion Guide* and the online curriculum is sequential, you should work through this Labs and Study Guide in order beginning with Chapter 1.

The book covers the major topic headings in the same sequence as the online curriculum for the *CCNA Exploration LAN Switching and Wireless course*. This book has seven chapters, with the same numbers and names as the online course chapters.

If necessary, a chapter uses a single topology for the exercises in the Study Guide portion. The single topology per chapter allows for better continuity and easier understanding of switching commands, operations, and outputs. However, the topology is different from the one used in the online curriculum and the *Companion Guide*. A different topology affords you the opportunity to practice your knowledge and skills without just simply recording the information you find in the text.

- **Chapter 1, "LAN Design":** The exercises in the Study Guide portion focus on LAN design concepts, including vocabulary and the three-layer hierarchical model. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 2, "Basic Switch Concepts and Configuration":** The exercises in the Study Guide portion help you understand basic Ethernet and switching concepts, including building the MAC address table and collision and broadcast domains. Then, the Packet Tracer exercises

cover, in detail, how to configure a switch, including basic switch management and configuring switch security. The Labs and Activities portion includes two Basic Labs, a Challenge Lab, and a Packet Tracer Skills Integration Challenge activity.

- **Chapter 3, "VLANs":** The exercises in the Study Guide portion focus on the concepts of VLANs, including benefits of VLANs and types of VLANs. The exercises then cover VLAN trunking concepts before moving into a section devoted to a VLAN and trunk configuration Packet Tracer exercise. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 4, "VTP":** The exercises in the Study Guide portion are devoted to VTP concepts and configuration, including vocabulary, VTP modes, an Internet research exercise, and a VTP Packet Tracer exercise. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 5, "STP":** The exercises in the Study Guide portion focus on the concept of redundant LAN topologies, using STP and its variants to stop loops, and the commands to manipulate root bridge elections. The Labs and Activities portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 6, "Inter-VLAN Routing":** This short chapter focuses on how to configure inter-VLAN routing, including two Packet Tracer exercises. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 7, "Basic Wireless Concepts and Configuration":** The exercises in the Study Guide portion begin with wireless LAN concepts, including standards, operation, and security. The exercises then cover wireless configuration for LAN access using a Linksys WRT300N, including a Packet Tracer exercise. The Labs and Activities portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.

About the CD-ROM

The CD-ROM included with this book has all the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge files that are referenced throughout the book, indicated by the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge icons.

Updates to these files can be obtained from the website for this book at http://www.ciscopress.com/title/1587132028. The files will be updated to cover any subsequent releases of Packet Tracer.

About the Cisco Press Website for This Book

Cisco Press may provide additional content that can be accessed by registering your individual book at the Ciscopress.com website. Becoming a member and registering is free, and you then gain access to exclusive deals on other resources from Cisco Press.

To register this book, go to www.ciscopress.com/bookstore/register.asp and log into your account or create a free account if you do not have one already. Then enter the ISBN located on the back cover of this book.

After you register the book, it will appear on your Account page under Registered Products and you can access any online material from there.

CHAPTER 1

LAN Design

A properly designed LAN is a fundamental requirement for doing business. You must understand what a well-designed LAN is and be able to select appropriate devices to support the network specifications of a small or medium-sized business.

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, and open-ended question exercises to test your knowledge of LAN design.

The Labs and Activities portion of this chapter includes all the online curriculum labs and Packet Tracer activities to help you review information and skills you learned in the first course, Exploration Network Fundamentals.

As you work through this chapter, use Chapter 1 in *LAN Switching and Wireless, CCNA Exploration Companion Guide* or use the corresponding Chapter 1 in the Exploration LAN Switching and Wireless online curriculum for assistance.

Study Guide

Switched LAN Architecture

Compared to other network designs, a hierarchical network is easier to manage and expand, and problems are solved more quickly. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, not only is the network more manageable, but the network design becomes modular, which facilitates scalability and performance.

Vocabulary Exercise: Matching

Match the definition on the left with a term on the right. All definitions and terms are used exactly one time.

Definitions

a. Classifying and prioritizing traffic based on type of data.

b. Allow you to segment the traffic on a switch into separate subnetworks.

c. Controls which end devices are allowed to communicate on the network.

d. Distribution layer and core layer are combined into one layer.

e. High-speed backbone of the internetwork capable of forwarding large amounts of data quickly.

f. Determine the design requirements for a network.

g. Access layer switches can be configured with this option to provide control over which devices are allowed to connect to the network.

h. Cisco proprietary link aggregation technology.

i. Properly designed hierarchical networks can achieve near wire speed between all devices.

j. Consistency between the switches at each layer allows for rapid recovery and simplified troubleshooting.

k. Dramatically increases availability.

l. Controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs).

m. The process of combining voice and video communications on a data network.

n. The modularity of the hierarchical design facilitates ease of network expansion.

Terms

c access layer

f business goals

d collapsed core

m convergence

e core layer

l distribution layer

h EtherChannel

j manageability

i performance

g port security

a Quality of Service (QoS)

k redundancy

n scalability

b VLANs

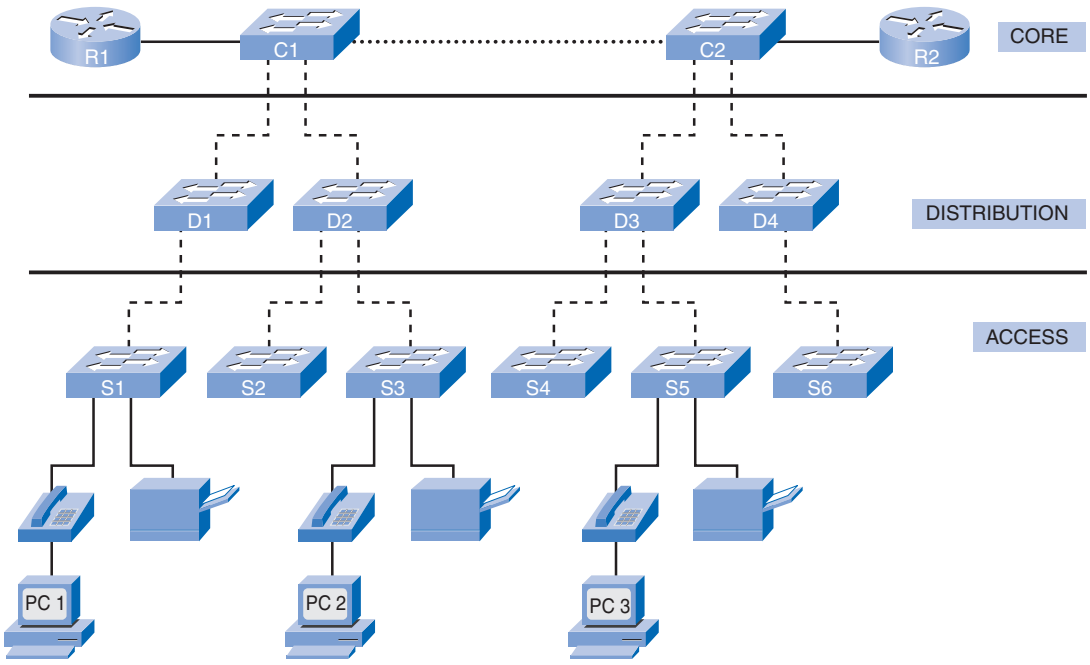
Vocabulary Exercise: Completion

Complete the paragraphs that follow by filling in the appropriate words and phrases.

The Hierarchical Network Model

The typical hierarchical design model is broken up into three layers: access, distribution, and core. Draw an example of a three-layer hierarchical network design in the blank space provided in Figure 1-1.

Figure 1-1 Three-Layer Hierarchical Network Example (answer)



Instructor Note: The example used in the answer key is straight from *LAN Switching and Wireless, CCNA Exploration Companion Guide*. The student does not have to draw this exact topology. However, all three layers should be adequately represented.

The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.

The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between VLANs defined at the access layer.

The core layer is critical for interconnectivity between distribution layer devices. It can also connect to Internet resources.

There are many benefits associated with hierarchical network designs:

- **Scalability:** The modularity of the design allows you to replicate design elements as the network grows. Because each instance of the module is consistent, expansion is easy to plan and implement.
- **Redundancy:** Access layer switches are connected to two different distribution layer switches. Distribution layer switches are connected to two or more core layer switches to ensure path availability if a core switch fails.

- **Performance:** Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases.
- **Security:** You have the flexibility to use more advanced policies at the distribution layer. You may apply access control policies that define which communication protocols are deployed on your network and where they are permitted to go.
- **Manageability:** Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. Consistency between the switches at each layer allows for rapid recovery and simplified troubleshooting.
- **Maintainability:** Because hierarchical networks are modular in nature and scale very easily, they are easy to maintain.

Principles of Hierarchical Network Design

When designing a hierarchical network topology, consider the network diameter, which is the number of devices that a packet has to cross before it reaches its destination. Keeping the network diameter low ensures low and predictable latency between devices.

Each layer in the hierarchical network model is a possible candidate for bandwidth aggregation, which allows multiple switch port links to be combined so as to achieve higher throughput between switches.

Redundancy can be provided in a number of ways, including by doubling up the network connections between devices or doubling the devices themselves.

Design requirements, such as the level of performance or redundancy necessary, are determined by the business goals of the organization.

What Is a Converged Network?

Convergence is the process of combining voice and video communications on a data network. Converged networks have existed for a while now, but were only feasible in large enterprise organizations because of the high network costs. Converged networks also required extensive management in relation to Quality of Service (QoS), because voice and video data traffic needed to be classified and prioritized on the network. Few individuals had the expertise in voice, video, and data networks to make convergence feasible and functional. In addition, legacy equipment hinders the process of moving toward a converged network.

What are two benefits to implementing a converged network as opposed to implementing three separate networks?

One network to manage

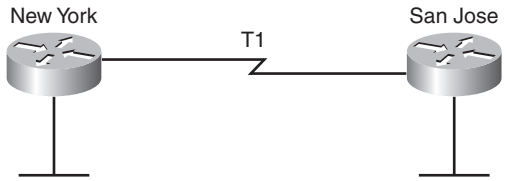
Lower costs

Converged networks give you options that had not existed previously. There is no need for an expensive handset phone or videoconferencing equipment. You can accomplish the same function using special software integrated with a personal computer. With the addition of inexpensive webcams, videoconferencing can be added to a softphone.

Three-Layer Hierarchical Model Exercise

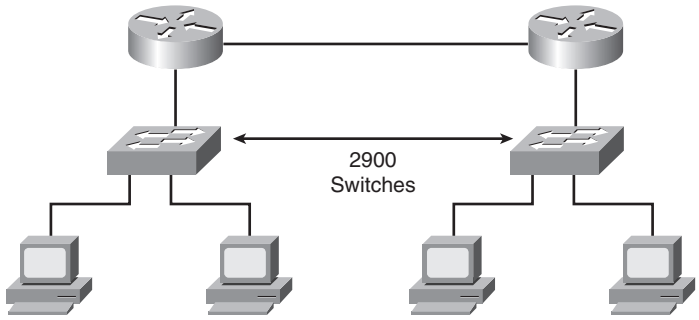
For each of the following figures, indicate whether the scenario is an **access** layer function, **distribution** layer function, or **core** layer function.

Figure 1-2 Scenario 1



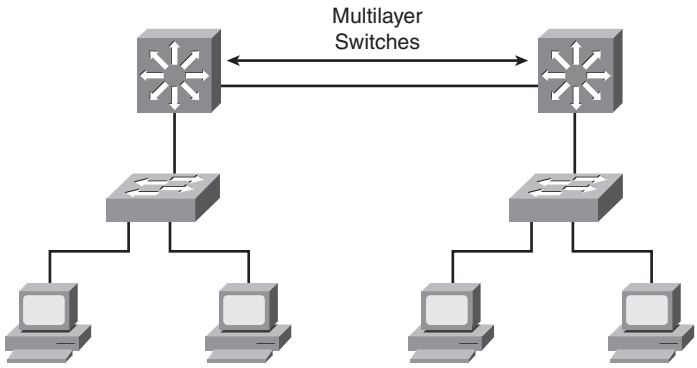
In Figure 1-2, the core layer is responsible for connecting New York and San Jose across a T1 link.

Figure 1-3 Scenario 2



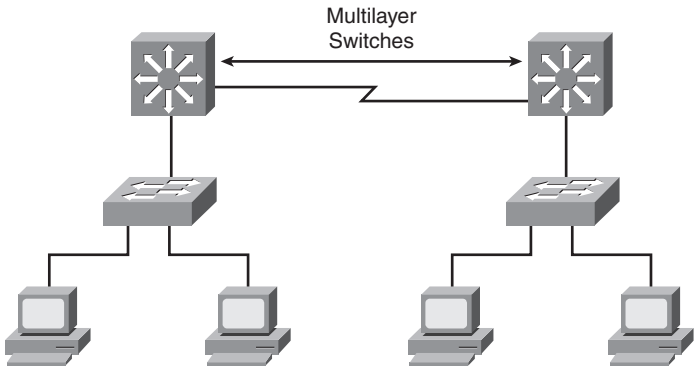
In Figure 1-3, the access layer is using 2900 series switches to connect end users to the network.

Figure 1-4 Scenario 3



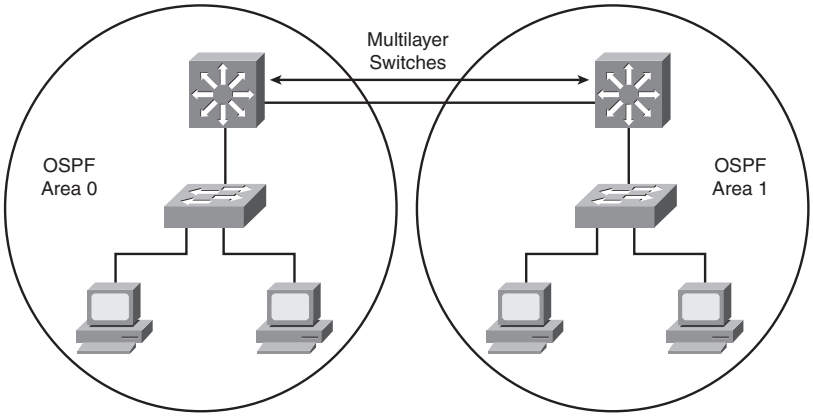
In Figure 1-4, the distribution layer is using multilayer switches for inter-VLAN routing.

Figure 1-5 Scenario 4



In Figure 1-5, the core layer is using multilayer switches between remote sites across a WAN link for fast switching and no packet manipulation.

Figure 1-6 Scenario 5



In Figure 1-6, the distribution layer is using multilayer switches to summarize OSPF routes.

Matching Switches to Specific LAN Functions

Selecting switches for each of the layers of the hierarchical design requires knowing details about traffic flows, the user community demands, data storage needs, and server availability.

Vocabulary Exercise: Matching

Match the definition on the left with a term on the right. All definitions and terms are used exactly one time.

Definitions

a. A graphical representation of a network infrastructure.

b. Cannot add hardware features or options beyond those that originally came with the switch.

c. Allow installation of different line cards.

d. A process of measuring the bandwidth usage on a network and analyzing the data for the purpose of performance tuning, capacity planning, and making hardware improvement decisions.

e. Reduces bottlenecks of traffic by allowing up to eight switch ports to be bound together for data communications.

f. The number of ports available on a single switch.

g. Uses the network cable to deliver electricity to devices.

h. Generated between data storage devices on the network.

i. Interconnected using a special backplane cable.

j. Typically traverses multiple switches to reach its destination.

k. Defines the capabilities of a switch by classifying how much data the switch can process per second.

l. Also known as Layer 3 switches.

m. A process of identifying various groups and their impact on network performance.

Terms

j	client-server traffic
b	fixed configuration switches
k	forwarding rates
e	link aggregation
c	modular switches
l	multilayer switches
f	port density
g	Power over Ethernet (PoE)
h	server-server traffic
i	stackable switches
a	topology diagram
d	traffic flow analysis
m	user community analysis

Layer Features of the Hierarchical Model Exercise

Check the appropriate column in Table 1-1 to identify which feature belongs to each layer. Some features may belong to more than one layer.

Table 1-1 Features at Each Layer of the Hierarchical Model

Feature	Access	Distribution	Core
Bandwidth aggregation	X	X	X
Fast Ethernet/Gigabit Ethernet	X		
Gigabit Ethernet/10-Gigabit Ethernet		X	X
High forwarding rate		X	
Very high forwarding rate			X
Layer 3 support		X	X
Port security	X		
Power over Ethernet (PoE)	X		
Quality of Service (QoS)	X	X	X
Redundant components		X	X
Security policies/access control lists		X	
VLANs	X		

Labs and Activities

Command Reference

The labs for this first chapter review the configuration skills you acquired in previous courses. In Table 1-2, record the command, *including the correct prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Table 1-2 Commands for Basic Router Configuration

Command	Description
`Router>enable`	Switches from user EXEC mode to privileged EXEC mode
`Router#disable`	Switches back from privileged EXEC mode to user EXEC mode
`Router#configure terminal`	Moves into global configuration mode
`Router(config)#hostname CISCO`	Names the router CISCO
`Router(config)#enable secret class`	Sets the enable password to **class** and encrypts it
`Router(config)#banner motd #Authorized Access Only#`	Configures a message-of-the-day banner that uses # as the delimiting character and displays the following when users attempt to log in: Authorized Access Only
`Router(config)#line console 0`	Enters console line configuration mode
`Router(config-line)#password cisco`	Sets the console password to **cisco**
`Router(config-line)#login`	Enables password checking when users log in
`Router(config)#line vty 0 4`	Enters line configuration mode for five Telnet lines
`Router(config)#interface fa 0/0`	Enters interface configuration mode for Fa0/0
`Router(config-if)#ip addres 192.168.1.1 255.255.255.0`	Sets an interface address as 192.168.1.1/24
`Router(config-if)#description Link to ISP`	Configures an interface with the text Link to ISP, which is used to describe the purpose of the link
`Router(config-if)#no shutdown`	Activates an interface
`Router#copy running-config startup-config`	Saves the current configuration to NVRAM
`Router#show running-config`	Displays the current configuration in RAM
`Router#show startup-config`	Displays the configuration saved in NVRAM
`Router>ping 192.168.1.1` or `Router#ping 192.168.1.1`	Tests end-to-end connectivity with a remote destination at 192.168.1.1

Command	Description

`Router>telnet 192.168.1.1`
or
`Router#telnet 192.168.1.1`
	Begins a remote management session on a device at 192.168.1.1

Lab 1-1: Review of Concepts from Exploration 1 (1.3.1)

Learning Objectives

Upon completion of this lab, you will be able to

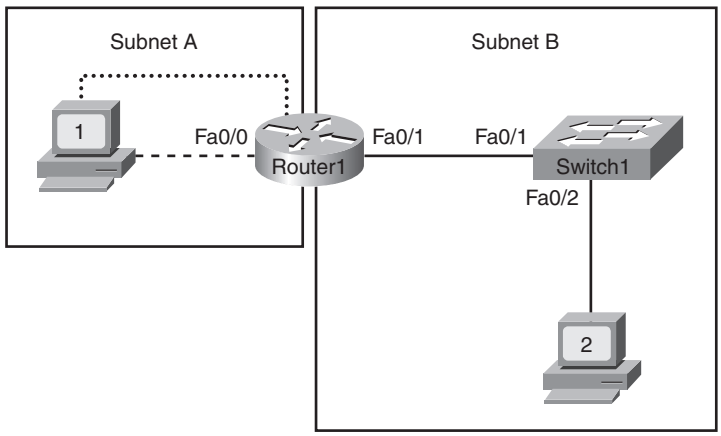
- Create a logical topology given network requirements
- Create subnets to meet host requirements
- Configure the physical topology
- Configure the logical topology
- Verify network connectivity
- Configure and verify passwords

Scenario

In this lab, you will design and configure a small routed network and verify connectivity across multiple network devices. This requires creating and assigning two subnetwork blocks, connecting hosts and network devices, and configuring host computers and one Cisco router for basic network connectivity. Switch1 has a default configuration and does not require additional configuration. You will use common commands to test and document the network. The zero subnet is used.

Figure 1-7 shows the topology diagram for this lab.

Figure 1-7 Topology Diagram for Lab 1-1



Task 1: Design a Logical LAN Topology

Step 1. Design an IP addressing scheme.

Given the IP address block of 192.168.7.0/24, design an IP addressing scheme that satisfies the following requirements:

- Subnet A has 110 hosts.
- Subnet B has 54 hosts.
- Subnet zero is used.
- Create the smallest possible subnets that satisfy the requirements for hosts.
- Complete the calculations for Subnet A in Table 1-3.
- Complete the calculations for Subnet B in Table 1-4.
- No subnet calculators may be used.

Table 1-3 Subnet Calculations for Subnet A

Subnet Specification	Calculation
Number of bits in the subnet	1
IP mask (binary)	11111111. 11111111. 11111111.10000000
New IP mask (decimal)	255.255.255.128
Maximum number of usable subnets (including the 0 subnet)	2
Number of usable hosts per subnet	126
IP subnetwork address	192.168.7.0
First IP host address	192.168.7.1
Last IP host address	192.168.7.126

Table 1-4 Subnet Calculations for Subnet B

Subnet Specification	Calculation
Number of bits in the subnet	2
IP mask (binary)	11111111. 11111111. 11111111.11000000
New IP mask (decimal)	255.255.255.192
Maximum number of usable subnets (including the 0 subnet)	2
Number of usable hosts per subnet	62
IP network address	192.168.7.128
First IP host address	192.168.7.129
Last IP host address	192.168.7.190

Step 2. Record the IP address information for each device:

- Assign the first usable IP address in the subnet to the hosts and record the information in Table 1-5.
- Assign the last usable IP address to the router interface and record the information in Table 1-5.

Table 1-5 IP Address Assignments

Device	IP Address	Subnet Mask	Default Gateway
Host1	192.168.7.1	255.255.255.128	192.168.7.126
Router1-Fa0/0	192.168.7.126	255.255.255.128	—
Host2	192.168.7.129	255.255.255.192	192.168.7.190
Router1-Fa0/1	192.168.7.190	255.255.255.192	—

Before proceeding, verify your IP addresses with the instructor.

Task 2: Configure the Physical Topology

Step 1. Cable the network.

Refer to Figure 1-7 and Table 1-6 to determine the necessary cables needed to connect the devices.

Table 1-6 Choosing the Correct Cable

Link	Cable Type
Host1 to Router1 Fa0/0	Crossover
Switch1 to Router1 Fa0/1	Straight-through
Switch1 to Host2	Straight-through
Host1 and Router1 console	Rollover

Step 2. Physically connect lab devices.

Cable the network devices as shown in Figure 1-7 and power all devices.

Step 3. Inspect the network connections.

Verify the connections visually. Link lights on the router, switch, and hosts should be green. You will not have a link light for the console connection, but it should be firmly attached at both ends.

Instructor Note: Ensure that the switch is in the default configuration and that Fa0/1 and Fa0/2 are in VLAN 1. If necessary, delete the vlan.dat file and reload the switch. Ensure that the router configuration has been erased.

Task 3: Configure the Logical Topology

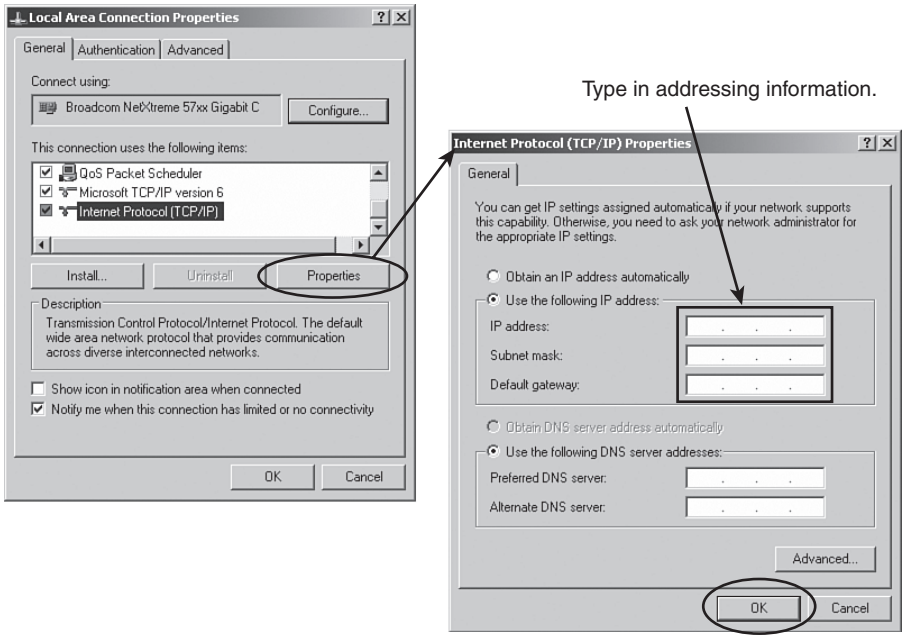
Step 1. Configure the host computers.

Configure the static IP address, subnet mask, and gateway for each host computer.

Note: The following directions are for Windows XP. To configure hosts using other operating systems, refer to the operating system manual.

To configure the host, choose **Start > Control Panel > Network Connections > Local Area Connection** and then click the **Properties** button. In the Local Area Connection Properties dialog box, click **Internet Protocol (TCP/IP)** and click the **Properties** button, as shown in Figure 1-8.

Figure 1-8 Setting Properties for Internet Protocol (TCP/IP)



In the TCP/IP Properties dialog box for each host, enter the IP address, subnet mask, and the default gateway you recorded previously in Table 1-5.

After configuring each host computer, open a command window on the host by choosing **Start > Run**. When prompted to type the name of a program, enter **cmd** in the text box. From the command window, display and verify the host network settings with the **ipconfig** command. The settings should match what you recorded previously in Table 1-5.

Step 2. Configure Router1.

From Host1, establish a console session with Router1. Directions for creating a console connection using Tera Term or HyperTerminal are in the appendixes at the end of this lab.

From the router console, enter the following commands:

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router1
```

```
Router1(config)#enable secret class
Router1(config)#line console 0
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#line vty 0 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#interface fa0/0
Router1(config-if)#ip address 192.168.7.126  255.255.255.128
Router1(config-if)#no shutdown
Router1(config-if)#description connection to host1
Router1(config-if)#interface fa0/1
Router1(config-if)#description connection to switch1
Router1(config-if)#ip address 192.168.7.190 255.255.255.192
Router1(config-if)#no shutdown
Router1(config-if)#end
Router1#
```

Task 4: Verify Network Connectivity

Use the **ping** command to verify network connectivity.

Note: If pings to the host computers fail, temporarily disable the computer firewall and retest. To disable a Windows firewall, choose **Start > Control Panel > Windows Firewall**, click the **Off** radio button, and then click **OK**.

Use Table 1-7 to verify connectivity with each network device. Take corrective action to establish connectivity if a test fails.

Table 1-7 Connectivity Verification

From	To	IP Address	Ping Results
Host1	NIC IP address	192.168.7.1	Should be successful
Host1	Router1, Fa0/0	192.168.7.126	Should be successful
Host1	Router1, Fa0/1	192.168.7.190	Should be successful
Host1	Host2	192.168.7.129	Should be successful
Host2	NIC IP address	192.168.7.129	Should be successful
Host2	Router1, Fa0/1	192.168.7.190	Should be successful
Host2	Router1, Fa0/0	192.168.7.126	Should be successful
Host2	Host1	192.168.7.1	Should be successful

In addition to the **ping** command, what other Windows command is useful in displaying network delay and breaks in the path to the destination?

tracert

Task 5: Verify Passwords

Step 1. Telnet to Router1 from Host2 to verify the Telnet password.

You should be able to telnet to either FastEthernet interface of the router.

In a command window on Host 2, type

```
C:\>telnet 192.168.7.190
```

When you are prompted for the Telnet password, type **cisco** and press **Enter**.

Was the telnet successful? Yes

Step 2. Verify that the enable secret password has been set.

From the Telnet session, enter privileged EXEC mode and verify it is password protected:

```
Router1>enable
```

Were you prompted for the enable secret password? Yes

Step 3. Verify that the console is password protected.

Terminate and then re-establish the console connection from Host1 to the router to verify that the console is password protected.

Depending on the Telnet client that you are using, the session can usually be terminated with **Ctrl-]**. When the session is re-established, you should be prompted for the console password before being allowed access to the command-line interface.

Task 6: Reflection

How are Telnet access and console access different? When might it make sense to set different passwords on these two access ports?

The network administrator must have physical access to the device to establish a console connection, whereas Telnet access can be established from a remote location. However, Telnet access depends upon a router with network access, whereas a console connection can be used to access the router regardless of the router's configuration.

Why does the switch between Host2 and the router not require configuration with an IP address to forward packets?

The switch is a Layer 2 device and does not forward traffic using Layer 3 addressing. In addition, in this lab you do not need to manage the switch remotely. Therefore, you did not set an IP address for Telnet access.

Task 7: Clean Up

Unless directed otherwise by your instructor, erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Final Router 1 Configuration

```
Router1#show run
<selective output omitted>
!
hostname Router1
```

```
!
enable secret class
!
!
 interface FastEthernet0/0
 description connection to host1
 ip address 192.168.7.126 255.255.255.128
 no shutdown
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.168.7.190 255.255.255.192
 no shutdown
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Packet Tracer Companion

Review of Concepts from Exploration 1 (1.3.1)

You can now open the file LSG03-Lab131.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Appendix 1A: Installing and Configuring Tera Term for Use in Windows XP

Tera Term is a free terminal-emulation program for Windows. It can be used in the lab environment in place of Windows HyperTerminal. Tera Term can be obtained at the following URL:

http://hp.vector.co.jp/authors/VA002416/teraterm.html

Download the ttermp23.zip file for Windows95/NT, unzip it, and install Tera Term. This version is compatible with XP and Vista.

Step 1. Open Tera Term.

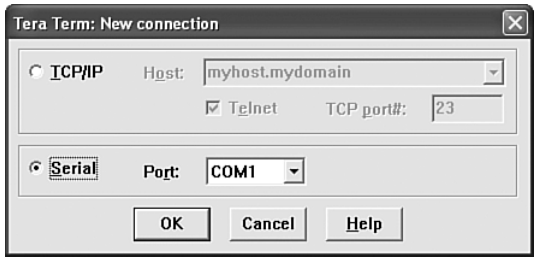
Step 2. Assign the serial port.

To use Tera Term to connect to the router console, click the **Serial** radio button, as shown in Figure 1-9.

Step 3. Set the serial port parameter.

Choose the appropriate parameter from the **Port** drop-down list. Normally, your connection is through COM1. If you are unsure what port to use, ask your instructor for assistance. When you are finished, click **OK**.

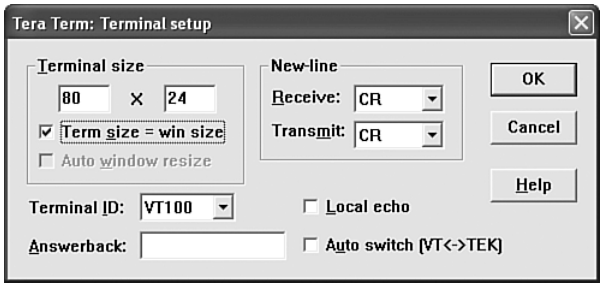
Figure 1-9 Tera Term: New Connection Dialog Box



Step 4. Configure settings.

Tera Term has some settings that can be changed to make it more convenient to use. Choose **Setup > Terminal** to open the Terminal Setup dialog box, and then check the **Term Size = Win Size** check box, as shown in Figure 1-10. This setting allows command output to remain visible when the Tera Term window is resized. Click **OK** to close the Terminal Setup dialog box.

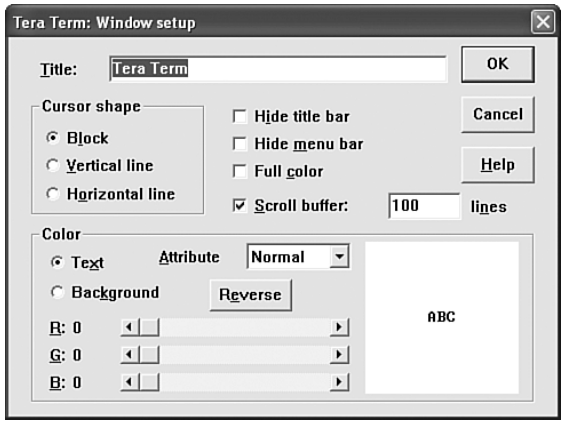
Figure 1-10 Tera Term: Terminal Setup Dialog Box



Step 5. Change the scroll buffer number.

Choose **Setup > Window** and, in the Window Setup dialog box, change the **Scroll Buffer** number to a number higher than 100, as shown in Figure 1-11. This setting allows you to scroll up and view previous commands and outputs. If there are only 100 lines available in the buffer, only the last 100 lines of output are visible. For example, set the scroll buffer to 1000 lines.

Figure 1-11 Tera Term: Window Setup Dialog Box



Appendix 1B: Configuring Tera Term as the Default Telnet Client in Windows XP

By default, Windows can be set to use HyperTerminal as the Telnet client. Windows can also be set to use the DOS version of Telnet. In the NetLab environment, you can change the Telnet client to Local Telnet Client, which means that NetLab will open the current Windows default Telnet client. This can be set to HyperTerminal or to the DOS-like version of Telnet embedded in the Windows operating system.

Complete the following steps to change your default Telnet client to Tera Term (or any other Telnet client):

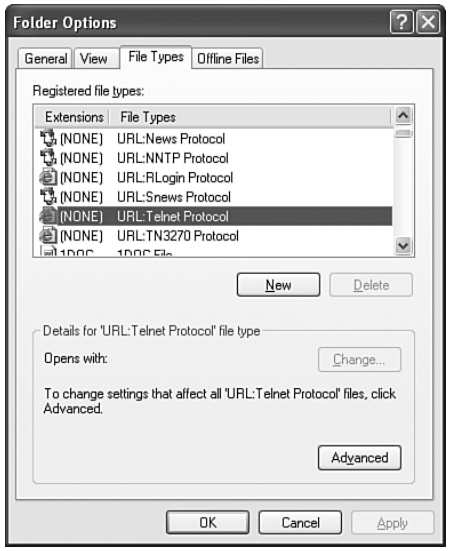
Step 1. Open the Folder Options dialog box.

Double-click **My Computer** (or choose **Start > My Computer**), and then choose **Tools > Folder Options**.

Step 2. Edit the **(NONE) URL:Telnet Protocol**.

Click the **File Types** tab, scroll down in the **Registered File Types** list and click the **(NONE) URL:Telnet Protocol** entry, as shown in Figure 1-12, and then click the **Advanced** button.

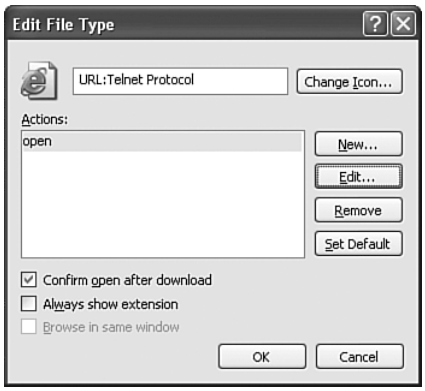
Figure 1-12 Folder Options Dialog Box



Step 3. Edit the open action.

In the Edit File Type dialog box, click **Edit** to edit the **open** action, as shown in Figure 1-13.

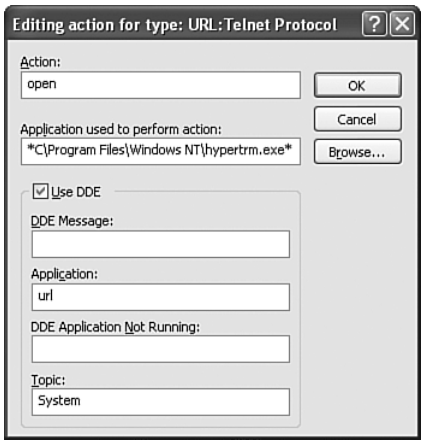
Figure 1-13 Edit File Type Dialog Box



Step 4. Change the application.

In the Editing Action for Type: URL: Telnet Protocol dialog box, the Application Used to Perform Action is currently set to HyperTerminal, as shown in Figure 1-14. Click **Browse** to change the application.

Figure 1-14 Editing Action for Type Dialog Box (Before Edit)



Step 5. Open ttermpro.exe.

Browse to the Tera Term installation folder, as shown in Figure 1-15. Click **ttermpro.exe** to specify this program for the open action, and then click **Open**.

Step 6. Confirm ttermpro.exe and close.

From the window shown in Figure 1-16, click **OK** twice and then click **Close** to close the Folder Options dialog box. The Windows default Telnet client is now set to Tera Term.

Figure 1-15 Open With Dialog Box

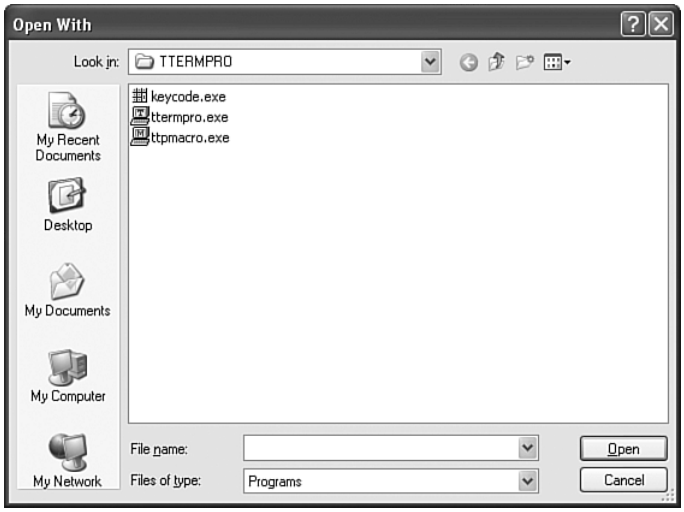
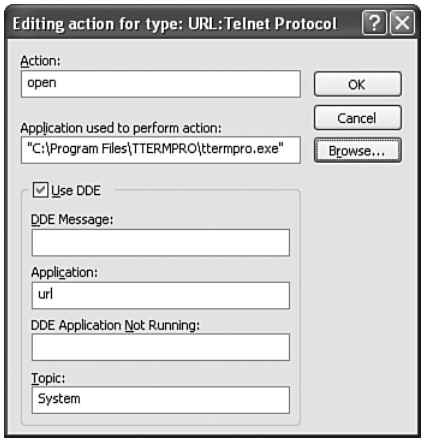


Figure 1-16 Editing Action for Type Dialog Box (After Edit)



Appendix 1C: Accessing and Configuring HyperTerminal

In most versions of Windows, you can open HyperTerminal by choosing **Start > Programs > Accessories > Communications > HyperTerminal**.

Step 1. Create a new connection.

Open HyperTerminal to create a new connection to the router. Enter an appropriate description in the Name field of the Connection Description dialog box, shown in Figure 1-17, and then click **OK**.

Step 2. Assign COM1 port.

In the Connect To dialog box, shown in Figure 1-18, make sure that the correct serial port is selected in the **Connect Using** field. Some PCs have more than one COM port. Click **OK**.

Figure 1-17 Connection Description Dialog Box

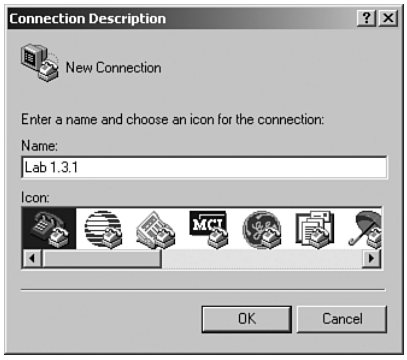
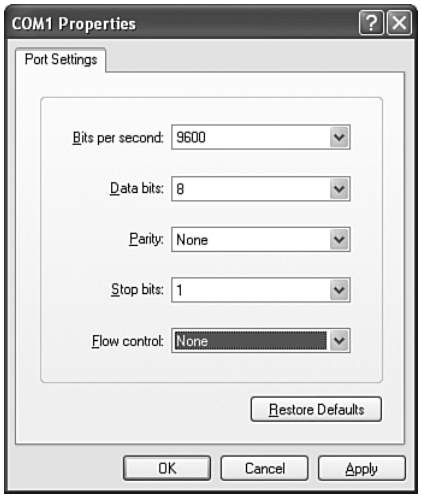


Figure 1-18 Connect To Dialog Box

Step 3. Set COM1 properties.

In the COM1 Properties dialog box, on the Port Settings tab, if the properties are not set to the values shown in Figure 1-19, click **Restore Defaults**, which normally sets the correct properties. Then click **OK**.

Figure 1-19 COM1 Properties Dialog Box



Step 4. Verify the connection.

You should now have a console connection to the router. Press **Enter** to get a router prompt.

Curriculum Lab 1-2: Review of Concepts from Exploration 1—Challenge (1.3.2)

Learning Objectives

Upon completion of this lab, you will be able to

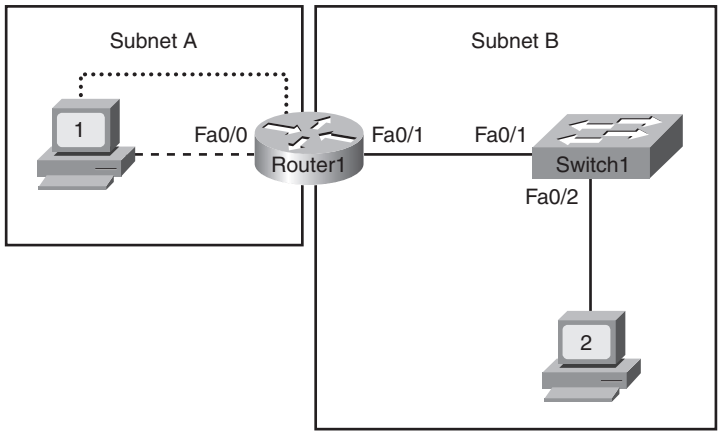
- Create a logical topology given network requirements
- Create subnets to meet host requirements
- Configure the physical topology
- Configure the logical topology
- Verify network connectivity
- Configure and verify passwords

Scenario

In this lab, you will design and configure a small routed network and verify connectivity across multiple network devices. This requires creating and assigning two subnetwork blocks, connecting hosts and network devices, and configuring host computers and one Cisco router for basic network connectivity. Switch1 has a default configuration and does not require additional configuration. You will use common commands to test and document the network. The zero subnet is used.

Figure 1-20 shows the topology diagram for this lab.

Figure 1-20 Topology Diagram for Lab 1-2



Task 1: Design a Logical LAN Topology

Step 1. Design an IP addressing scheme.

Given the IP address block of 192.168.30.0/27, design an IP addressing scheme that satisfies the following requirements:

- Subnet A has 7 hosts.
- Subnet B has 14 hosts.
- Subnet zero is used.
- Create the smallest possible subnets that satisfy the requirements for hosts.
- Complete the calculations for Subnet A in Table 1-8.

- Complete the calculations for Subnet B in Table 1-9.
- No subnet calculators may be used.

Table 1-8 Subnet Calculations for Subnet A

Subnet Specification	Calculation
Number of bits in the subnet	1
IP mask (binary)	11111111. 11111111. 11111111.11110000
New IP mask (decimal)	255.255.255.240
Maximum number of usable subnets (including the 0 subnet)	2
Number of usable hosts per subnet	14
IP subnetwork address	192.168.30.0
First IP host address	192.168.30.1
Last IP host address	192.168.30.14

Table 1-9 Subnet Calculations for Subnet B

Subnet Specification	Calculation
Number of bits in the subnet	1
IP mask (binary)	11111111. 11111111. 11111111.11110000
New IP mask (decimal)	255.255.255.240
Maximum number of usable subnets (including the 0 subnet)	2
Number of usable hosts per subnet	14
IP subnetwork address	192.168.30.16
First IP host address	192.168.30.17
Last IP host address	192.168.30.30

Step 2. Record the IP address information for each device:

- Assign the first usable IP address in the subnet to the hosts and record the information in Table 1-10.
- Assign the last usable IP address to the router interface and record the information in Table 1-10.

Table 1-10 IP Address Assignments

Device	IP Address	Mask	Gateway
Host1	192.168.30.1	255.255.255.240	192.168.30.14
Router1-Fa0/0	192.168.30.14	255.255.255.240	—
Host2	192.168.30.17	255.255.255.240	192.168.30.30
Router1-Fa0/1	192.168.30.30	255.255.255.240	—

Before proceeding, verify your IP addresses with the instructor.

Task 2: Configure the Physical Topology

Step 1. Cable the network.

Refer to Figure 1-20 and in Table 1-11 indicate the necessary cables needed to connect the devices.

Table 1-11 Choosing the Correct Cable

Correct Cabling	Cable Type
LAN cable between Host1 and Router1 Fa0/0	Crossover
LAN cable between Switch1 and Router1 Fa0/1	Straight-through
LAN cable between Switch1 and Host2	Straight-through
Console cable between Host1 and Router1	Rollover

Step 2. Physically connect lab devices.

Cable the network devices as shown in Figure 1-20 and power all devices.

Step 3. Inspect the network connections.

After cabling the network devices, verify the connections.

Instructor Note: Ensure that the switch is in the default configuration and that Fa0/1 and Fa0/2 are in VLAN 1. If necessary, delete the vlan.dat file and reload the switch. Ensure that the router configuration has been erased.

Task 3: Configure the Logical Topology

Step 1. Configure the host computers.

Configure the static IP address, subnet mask, and gateway for each host computer. After configuring each host computer, display and verify the host network settings with the **ipconfig** command.

Step 2. Configure Router1.

From Host1, establish a console connection with Router1 and configure the following:

- Use **Router1** as the hostname
- Set the encrypted privileged EXEC password to **class**
- Set the console and Telnet access password to **cisco**
- Complete the description and IP addressing on both FastEthernet interfaces

Task 4: Verify Network Connectivity

Use the **ping** command to verify network connectivity.

In Table 1-12 record IP addresses and connectivity verification results for each network device. Take corrective action to establish connectivity if a test fails.

Table 1-12 Connectivity Verification

From	To	IP Address	Ping Results
Host1	NIC IP address	192.168.30.1	Should be successful
Host1	Router1, Fa0/0	192.168.30.14	Should be successful
Host1	Router1, Fa0/1	192.168.30.30	Should be successful
Host1	Host2	192.168.30.17	Should be successful
Host2	NIC IP address	192.168.30.17	Should be successful
Host2	Router1, Fa0/1	192.168.30.30	Should be successful
Host2	Router1, Fa0/0	192.168.30.14	Should be successful
Host2	Host1	192.168.30.1	Should be successful

Task 5: Verify Passwords

Step 1. Telnet to Router1 from Host2 and verify the Telnet password.

You should be able to telnet to either Fast Ethernet interface of the router.

Step 2. Verify that the enable secret password has been set.

From the Telnet session, enter privileged EXEC mode and verify that it is password protected.

Step 3. Verify that the console is password protected.

Terminate and then re-establish the console connection from Host1 to the router to verify that the console is password protected.

Task 6: Clean Up

Unless directed otherwise by your instructor, erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Router Configuration Commands

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#enable secret class
Router1(config)#line console 0
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#line vty 0 4
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#interface fa0/0
Router1(config-if)#ip address 192.168.30.14 255.255.255.240
```

```
Router1(config-if)#no shutdown
Router1(config-if)#description connection to host1
Router1(config-if)#interface fa0/1
Router1(config-if)#description connection to switch1
Router1(config-if)#ip address 192.168.30.30 255.255.255.240
Router1(config-if)#no shutdown
Router1(config-if)#^Z
Router1#
```

Final Router 1 Configuration

```
Router1#show run

<selective output omitted>
!
hostname Router1
!
!
enable secret class
!
interface FastEthernet0/0
 description connection to host1
 ip address 192.168.30.14 255.255.255.240
 no shutdown
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.168.30.30 255.255.255.240
 no shutdown
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Packet Tracer Companion

Packet Tracer Companion: Review of Concepts from Exploration 1—Challenge (1.3.2)

You can now open the file LSG03-Lab132.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Curriculum Lab 1-3: Troubleshooting a Small Network (1.3.3)

Learning Objectives

Upon completion of this lab, you will be able to

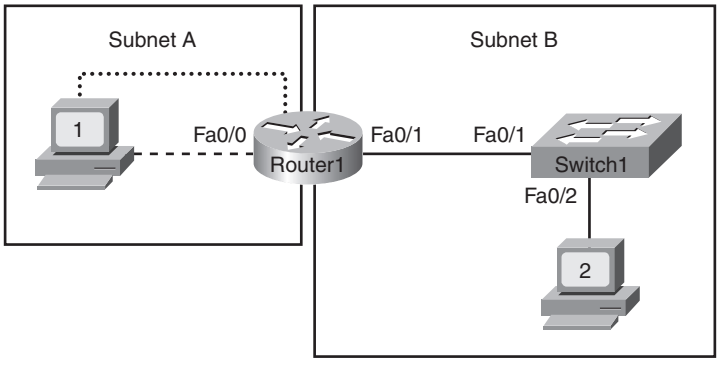
- Verify that a paper design meets stated network requirements
- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Discover where communication is not possible
- Gather information about the misconfigured portion of the network along with any other errors
- Analyze information to determine why communication is not possible
- Propose solutions to network errors
- Implement solutions to network errors

Scenario

In this lab, you are given a completed configuration for a small routed network. The configuration contains design and configuration errors that conflict with stated requirements and prevent end-to-end communication. You will examine the given design and identify and correct any design errors. You will then cable the network, configure the hosts, and load configurations onto the router. Finally, you will troubleshoot the connectivity problems to determine where the errors are occurring and correct them using the appropriate commands. When all errors have been corrected, each host should be able to communicate with all other configured network elements and with the other host.

Figure 1-21 shows the topology diagram for this lab.

Figure 1-21 Topology Diagram for Lab 1-3



Task 1: Examine the Logical LAN Topology

Step 1. Verify the IP addressing scheme.

The IP address block of 172.16.30.0/23 is already subnetted to meet the following requirements:

- Subnet A has 174 hosts.
- Subnet B has 54 hosts.
- Subnet zero is used.
- Created the smallest possible number of subnets that satisfy the requirements for hosts.
- Calculations for Subnet A are shown in Table 1-13.
- Calculations for Subnet B are shown in Table 1-14.

Table 1-13 Subnet Calculations for Subnet A

Subnet Specification	Calculated Value
IP mask (decimal)	255.255.255.0
IP address	172.16.30.0
First IP host address	172.16.30.1
Last IP host address	172.16.30.254

Table 1-14 Subnet Calculations for Subnet B

Subnet Specification	Calculated Value
IP mask (decimal)	255.255.255.128 (should be 255.255.255.192)
IP address	172.16.31.0
First IP host address	172.16.31.1
Last IP host address	172.16.31.126 (should be 172.16.31.62 based on correct mask)

Examine each of the values in Tables 1-13 and 1-14 and verify that this topology meets all requirements and specifications.

Are any of the given values incorrect? Yes

If yes, correct the values in Table 1-13 and/or Table 1-14.

Step 2. Record the correct IP address information for each device:

- Assign the first usable IP address in the subnet to the hosts and record the information in Table 1-15.
- Assign the last usable IP address to the router interface and record the information in Table 1-15.

Table 1-15 IP Address Assignments

Device	IP Address	Mask	Gateway
Host1	172.16.30.1	255.255.255.0	172.16.30.254
Router1–Fa0/0	172.16.30.254	255.255.255.0	—
Host2	172.16.31.1	255.255.255.192	172.16.31.62
Router1–Fa0/1	172.16.31.62	255.255.255.192	—

Task 2: Cable, Erase, and Reload the Routers

Step 1. Cable the network.

Step 2. Clear the configuration on each router.

Task 3: Configure the Host Computers

Step 1. Configure host computers with IP addressing.

Step 2. Verify host computer configuration.

Task 4: Load the Router with the Supplied Scripts

Apply the following configurations to Router1. Alternatively, you can open the file LSG03-Lab133-Scripts.txt on the CD-ROM that accompanies this book and copy in the scripts for each of the switches.

Instructor Note: Missing or misconfigured commands are enclosed in brackets, [ ].

```
enable
!
config term
!
hostname Router1
!
enable secret class
!
no ip domain-lookup
!
```

```
 interface FastEthernet0/0
 description connection to host1
 ip address 172.16.30.1 255.255.255.0
[duplicate ip address – should be 172.16.30.254]
 duplex auto
 speed auto
[missing command  - no shutdown]
!
interface FastEthernet0/1
 description connection to switch1
 ip address 192.16.31.1 255.255.255.192
[wrong ip address – should be 172.16.31.62]
 duplex auto
 speed auto
[missing command - no shutdown]
!
!
line con 0
 password cisco
 login
line vty 0
 login
line vty 1 4
 password cisco
 login
!
end
```

Task 5: Identify Connectivity Problems

Use the **ping** command to test network connectivity.

Use Table 1-16 to test the connectivity of each network device and record the initial results of your tests.

Table 1-16 Connectivity Verification

From	To	IP Address	Ping Results
Host1	NIC IP address	172.16.30.1	Should be successful
Host1	Router1, Fa0/0	172.16.30.254	Should fail
Host1	Router1, Fa0/1	172.16.31.126	Should fail
Host1	Host2	172.16.31.1	Should fail
Host2	NIC IP address	172.16.30.1	Should be successful
Host2	Router1, Fa0/1	172.16.31.126	Should fail
Host2	Router1, Fa0/0	172.16.30.254	Should fail
Host2	Host1	172.16.30.1	Should fail

Task 6: Troubleshoot Network Connections

Step 1. Begin troubleshooting at PC1 (the host directly connected to Router1).

From host PC1, is it possible to ping PC2? No

From host PC1, is it possible to ping the router Fa0/1 interface? No

From host PC1, is it possible to ping the default gateway? No

From host PC1, is it possible to ping itself? Yes

Where is the most logical place to begin troubleshooting the PC1 connection problems?

The first connection, PC1 to router interface Fa0/0.

Step 2. Examine the router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

Interfaces Fa0/0 and Fa0/1 are administratively down.

If there are problems with the status of the interfaces, record any commands that are necessary to correct the configuration errors:

config term; **interface fastethernet0/0**; **no shutdown**; interface **fastethernet0/1**; **no shutdown**

Step 3. Use the necessary commands to correct the router configuration.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces.

Does the information in the interface status summary indicate any configuration errors on Router1? No

If the answer is yes, troubleshoot the interface status of the interfaces.

Has connectivity been restored? No