Networking Essentials

A CompTIA Network+ N10-006 Textbook

Fourth Edition

Jeffrey S. Beasley
Piyasat Nilkaew

CompTIA Network+

Software Enclosed

PEARSON IT CERTIFICATION

Special Offer–Save 70%

CompTIA Network+ N10-006 Complete Video Course

Increase comprehension, retention, and exam readiness with the ideal complement to your Introduction to Networking or CompTIA Network+ Course.

To take advantage of this special offer, you can redeem the unique coupon code printed on the card in the CD-ROM sleeve at the back of this book. Simply follow the instructions printed on the card to redeem the code on our website.

CompTIA Network+ N10-006 Complete Video Course is a comprehensive training course that brings CompTIA Network+ exam topics to life through the use of real-world demonstrations, animations, live instruction, and configurations, making learning these foundational networking topics easy and fun.

Best-selling author, expert instructor, and double CCIE Kevin Wallace walks you through the full range of topics on the CompTIA Network+ N10-006 exam, including protocol reference models; network devices, topologies, and services; WAN technologies; network cables and connectors; network design; LAN technologies; network addressing and routing; unified communication; virtualization; network security; and network maintenance. This unique product contains multiple types of video presentations, including live instructor whiteboarding, real-world demonstrations, animations of network activity, dynamic KeyNote presentations, doodle videos, and hands-on router and switch CLI configuration and troubleshooting in real lab environments, enabling you to learn both the concepts and the hands-on application.

The 200+ videos contained in this product provide more than 17 hours of instruction. Modules are divided into easy-to-digest lessons and conclude with summaries and interactive module and glossary quizzes to help assess your knowledge. In addition to the review quizzes, the product contains interactive exercises to help you truly learn the topics in each module. The product concludes with a series of lessons that give you valuable advice to help prepare for the actual exam.

Designed to take you inside Network+ concepts in a unique and interactive way, CompTIA Network+ N10-006 Complete Video Course is guaranteed to help you master the foundational networking topics that will help you succeed on the exam and on the job.

NETWORKING ESSENTIALS: FOURTH EDITION

A COMPTIA NETWORK+ N10-006 TEXTBOOK

INSTRUCTOR EDITION

JEFFREY S. BEASLEY AND PIYASAT NILKAEW

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

NETWORKING ESSENTIALS: FOURTH EDITION

Networking Essentials, Fourth Edition

ISBN-13: 978-0-7897-5819-4
ISBN-10: 0-7897-5819-9

Instructor's Guide for Networking Essentials, Fourth Edition

ISBN-13: 978-0-13-446716-0
ISBN-10: 0-13-446716-7

Library of Congress Control Number: 2015955285

Printed in the United States of America

First Printing: December 2015

ASSOCIATE PUBLISHER
Dave Dusthimer

EXECUTIVE EDITOR
Brett Bartow

SENIOR DEVELOPMENT EDITOR
Chris Cleveland

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Mandie Frank

COPY EDITOR
Bart Reed

INDEXER
Ken Johnson

PROOFREADER
Jess DeGabriele

TECHNICAL EDITORS
Anthony Sequeria
Dr. Kenneth L Hawkins
Douglas E. Maume

PEER REVIEWERS
DeAnnia Clements
Osman GuzideGene Carwile
Dr. Theodor Richardson

PUBLISHING COORDINATOR
Vanessa Evans

DESIGNERS
Mark Shirar
Alan Clements

COMPOSITOR
Tricia Bronkella

CONTENTS AT A GLANCE

TABLE OF CONTENTS

CHAPTER 13 Cloud Computing and Virtualization 602

CHAPTER 14 Codes and Standards 624

ABOUT THE AUTHORS

Jeffrey S. Beasley is a professor in the Information and Communications Technology program at New Mexico State University, where he teaches computer networking and many related topics. He is the author of *Networking, Second Edition,* as well as coauthor of *Modern Electronic Communication*, Ninth Edition, *Networking Essentials 3e,* and *A Practical Guide to Advance Networking*.

Piyasat Nilkaew is the director of Telecommunications and Networking at New Mexico State University, with more than 15 years of experience in network management and consulting. He has extensive expertise in deploying and integrating multiprotocol and multivendor data, voice, and video network solutions. He is coauthor of *Networking Essentials 3e* and *A Practical Guide to Advance Networking*.

DEDICATIONS

This book is dedicated to my family: Kim, Damon, and Dana. —Jeff Beasley

This book is dedicated to my family: June, Ariya, and Atisat. —Piyasat Nilkaew

ACKNOWLEDGMENTS

I am grateful to the many people who have helped with this text. My sincere thanks go to the following technical consultants:

- Danny Bosch and Matthew Peralta for sharing their expertise with optical networks and unshielded twisted-pair cabling, Don Yates for his help with the initial Net-Challenge software, and Abel Sanchez for his assistance the newest version of Net-Challenge.

I would also like to thank my many past and present students for their help with this book.

- Kathryn Sager and Joshua Cook for their work on the Net-Challenge software; Adam Segura for his help with taking pictures of the steps for CAT6 termination; Marc Montez, Carine George-Morris, Brian Morales, Michael Thomas, Jacob Ulibarri, Scott Leppelman, and Aarin Buskirk for their help with laboratory development; and Josiah Jones and Raul Marquez Jr. for their help with the Wireshark material.
- Aaron Shapiro and Aaron Jackson for their help in testing the many network connections presented in the text.
- Paul Bueno and Anthony Bueno for reading through the early draft of the text.

Your efforts are greatly appreciated.

We appreciate the excellent feedback of the following reviewers: Phillip Davis, DelMar College, TX; Thomas D. Edwards, Carteret Community College, NC; William Hessmiller, Editors & Training Associates; Bill Liu, DeVry University, CA; and Timothy Staley, DeVry University, TX.

Our thanks to the people at Pearson for making this project possible: Dave Dusthimer, for providing us with the opportunity to work on the fourth edition of this text, and Vanessa Evans, for helping make this process enjoyable. Thanks to Christopher Cleveland, and the all the people at Pearson IT Certification, and also to the many technical editors for their help with editing the manuscript.

Special thanks to our families for their continued support and patience.

—Jeffrey S. Beasley and Piyasat Nilkaew

ABOUT THE TECHNICAL REVIEWERS

Anthony Sequeria began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies. Anthony has lectured to massive audiences around the world while working for Mastering Computers. Anthony has never been happier in his career than he is now as a full-time trainer for CBT Nuggets. He is an avid tennis player, a private pilot, and a semi-professional poker player, and he enjoys getting beaten up by women and children at the martial arts school he attends with his daughter.

Dr. Kenneth L. Hawkins is the Program Director of Information Technology at the Hampton campus of Bryant and Stratton College. He earned his doctorate in Education from Nova Southeastern University, a master's degree in Computer Science from Boston University, a master's degree in Education from Old Dominion University, a master's degree in Management from Troy State University, and his undergraduate degree in Mathematics from Michigan Technological University. Dr. Hawkins, a retired military officer, has worked in post-secondary education for the past 14 years as department head, campus dean, and faculty for undergraduate and graduate business and information technology courses at six Tidewater universities. A graduate of the Leadership Institute of the Virginia Peninsula, he is actively involved both professionally and socially in the community, having served as district chairman for the Boy Scouts of America, educational administration consultant for a local private school, board member of two area businesses, member of the international professional society Phi Gamma Sigma, and member of the Old Point Comfort Yacht Club.

Douglas E. Maume is currently the Lead Instructor for the Computer Networking program at Centura College Online. He has been conducting new and annual course reviews for both the CN and IT programs since 2006. He is also an adjunct professor for Centura College, teaching Computer Networking, Information Technology, and Business Management courses since 2001. Mr. Maume owned his own business called Wish You Were Here, Personal Postcards, creating digital postcards on location at the Virginia Beach oceanfront. He earned a Bachelor's degree in Graphic Design from Old Dominion University, and an Associate's in Applied Science degree in Graphic Design from Tidewater Community College. Mr. Maume is currently Esquire to the District Deputy Grand Exalted Ruler for Southeast Virginia in the Benevolent and Protective Order of Elks. He has been actively involved with the Elks since 1999, serving the veterans and youth of the Norfolk community. He is also the Registrar for the adult men's league Shipps Corner Soccer Club, and has been playing competitively since 1972.

WE WANT TO HEAR FROM YOU!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

READER SERVICES

Register your copy of ***Networking Essentials*** at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN, 9780789758194, and click Submit. Once the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us in order to receive exclusive discounts on future editions of this product.

INTRODUCTION

This book provides a look at computer networking from the point of view of the network administrator. It guides readers from an entry-level knowledge in computer networks to advanced concepts in Ethernet networks; router configuration; TCP/IP networks; routing protocols; local, campus, and wide area network configuration; network security; wireless networking; optical networks; Voice over IP; the network server; and Linux networking. After covering the entire text, readers will have gained a solid knowledge base in computer networks.

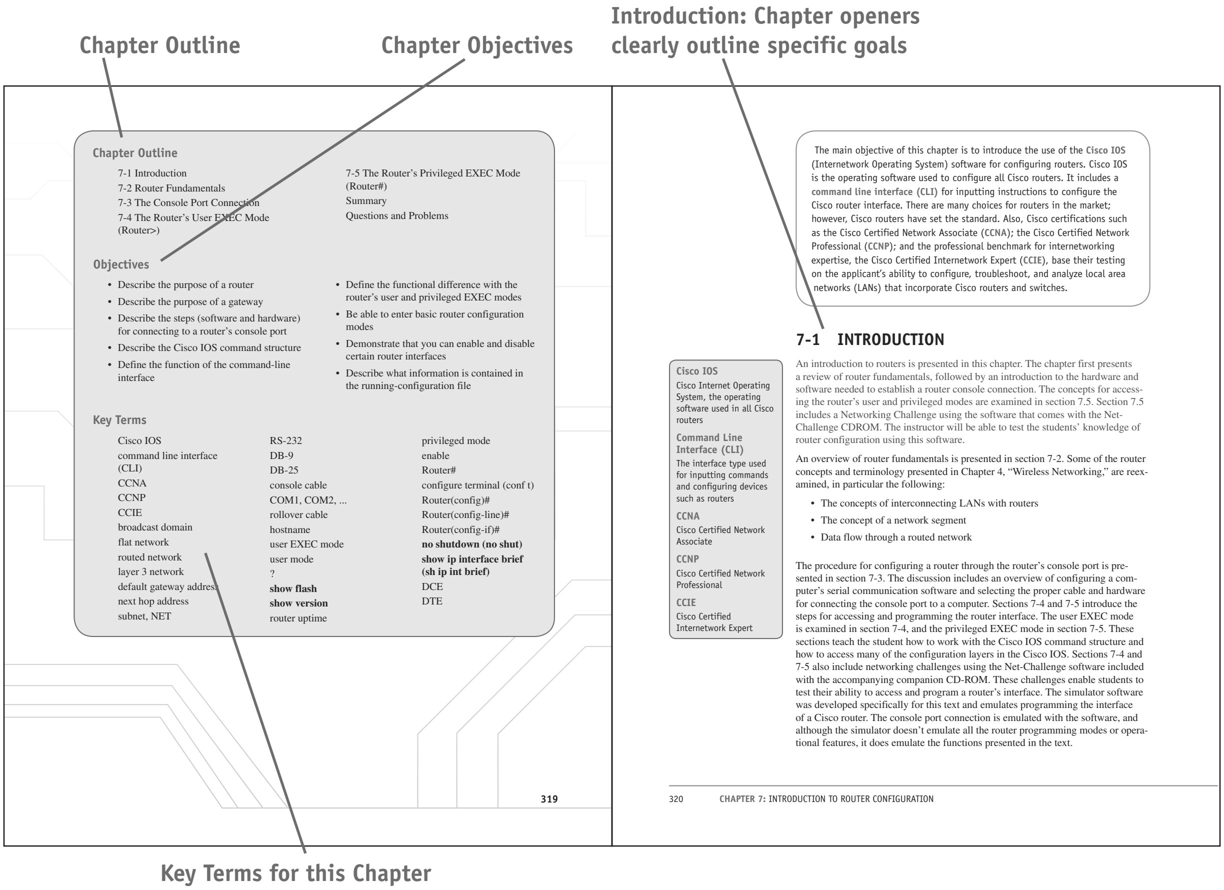
In our years of teaching, we have observed that technology students prefer to learn "how to swim" after they have gotten wet and taken in a little water. Then they are ready for more challenges. Show the students the technology, how it is used, and why, and they will take the applications of the technology to the next level. Allowing them to experiment with the technology helps them to develop a greater understanding. This book does just that.

ORGANIZATION OF THE TEXT

Thoroughly updated to reflect the latest version of CompTIA's Network+ exam, ***Networking Essentials*, 4th Edition,** is a practical, up-to-date, and hands-on guide to the basics of networking. Written from the viewpoint of a working network administrator, it requires absolutely no experience with either network concepts or day-to-day network management. This first volume has been revised and reorganized around the needs of introductory networking students, and assumes no previous knowledge. Throughout the text, the students will gain an appreciation of how basic computer networks and related hardware are interconnected to form a network. This involves understanding the concepts of twisted-pair cable, fiber optics, interconnecting LANs, configuring TCP/IP, subnet masking, basic router configuration, switch configuration and management, wireless networking, and network security.

Key Pedagogical Features

- *Chapter Outline, Network+ Objectives, Key Terms,* and *Introduction* at the beginning of each chapter clearly outline specific goals for the reader. An example of these features is shown in Figure P-1.



Chapter Outline

7-1 Introduction
7-2 Router Fundamentals
7-3 The Console Port Connection
7-4 The Router's User EXEC Mode (Router>)
7-5 The Router's Privileged EXEC Mode (Router#)
Summary
Questions and Problems

Objectives

- Describe the purpose of a router
- Describe the purpose of a gateway
- Describe the steps (software and hardware) for connecting to a router's console port
- Describe the Cisco IOS command structure
- Define the function of the command-line interface
- Define the functional difference with the router's user and privileged EXEC modes
- Be able to enter basic router configuration modes
- Demonstrate that you can enable and disable certain router interfaces
- Describe what information is contained in the running-configuration file

Key Terms

Cisco IOS
command line interface (CLI)
CCNA
CCNP
CCIE
broadcast domain
flat network
routed network
layer 3 network
default gateway address
next hop address
subnet, NET
RS-232
DB-9
DB-25
console cable
COM1, COM2, ...
rollover cable
hostname
user EXEC mode
user mode
?
show flash
show version
router uptime
privileged mode
enable
Router#
configure terminal (conf t)
Router(config)#
Router(config-line)#
Router(config-if)#
no shutdown (no shut)
show ip interface brief (sh ip int brief)
DCE
DTE

319

The main objective of this chapter is to introduce the use of the Cisco IOS (Internetwork Operating System) software for configuring routers. Cisco IOS is the operating software used to configure all Cisco routers. It includes a command line interface (CLI) for inputting instructions to configure the Cisco router interface. There are many choices for routers in the market; however, Cisco routers have set the standard. Also, Cisco certifications such as the Cisco Certified Network Associate (CCNA); the Cisco Certified Network Professional (CCNP); and the professional benchmark for internetworking expertise, the Cisco Certified Internetwork Expert (CCIE), base their testing on the applicant's ability to configure, troubleshoot, and analyze local area networks (LANs) that incorporate Cisco routers and switches.

7-1 INTRODUCTION

An introduction to routers is presented in this chapter. The chapter first presents a review of router fundamentals, followed by an introduction to the hardware and software needed to establish a router console connection. The concepts for accessing the router's user and privileged modes are examined in section 7.5. Section 7.5 includes a Networking Challenge using the software that comes with the Net-Challenge CDROM. The instructor will be able to test the students' knowledge of router configuration using this software.

An overview of router fundamentals is presented in section 7-2. Some of the router concepts and terminology presented in Chapter 4, "Wireless Networking," are reexamined, in particular the following:

- The concepts of interconnecting LANs with routers
- The concept of a network segment
- Data flow through a routed network

The procedure for configuring a router through the router's console port is presented in section 7-3. The discussion includes an overview of configuring a computer's serial communication software and selecting the proper cable and hardware for connecting the console port to a computer. Sections 7-4 and 7-5 introduce the steps for accessing and programming the router interface. The user EXEC mode is examined in section 7-4, and the privileged EXEC mode in section 7-5. These sections teach the student how to work with the Cisco IOS command structure and how to access many of the configuration layers in the Cisco IOS. Sections 7-4 and 7-5 also include networking challenges using the Net-Challenge software included with the accompanying companion CD-ROM. These challenges enable students to test their ability to access and program a router's interface. The simulator software was developed specifically for this text and emulates programming the interface of a Cisco router. The console port connection is emulated with the software, and although the simulator doesn't emulate all the router programming modes or operational features, it does emulate the functions presented in the text.

Cisco IOS
Cisco Internet Operating System, the operating software used in all Cisco routers

Command Line Interface (CLI)
The interface type used for inputting commands and configuring devices such as routers

CCNA
Cisco Certified Network Associate

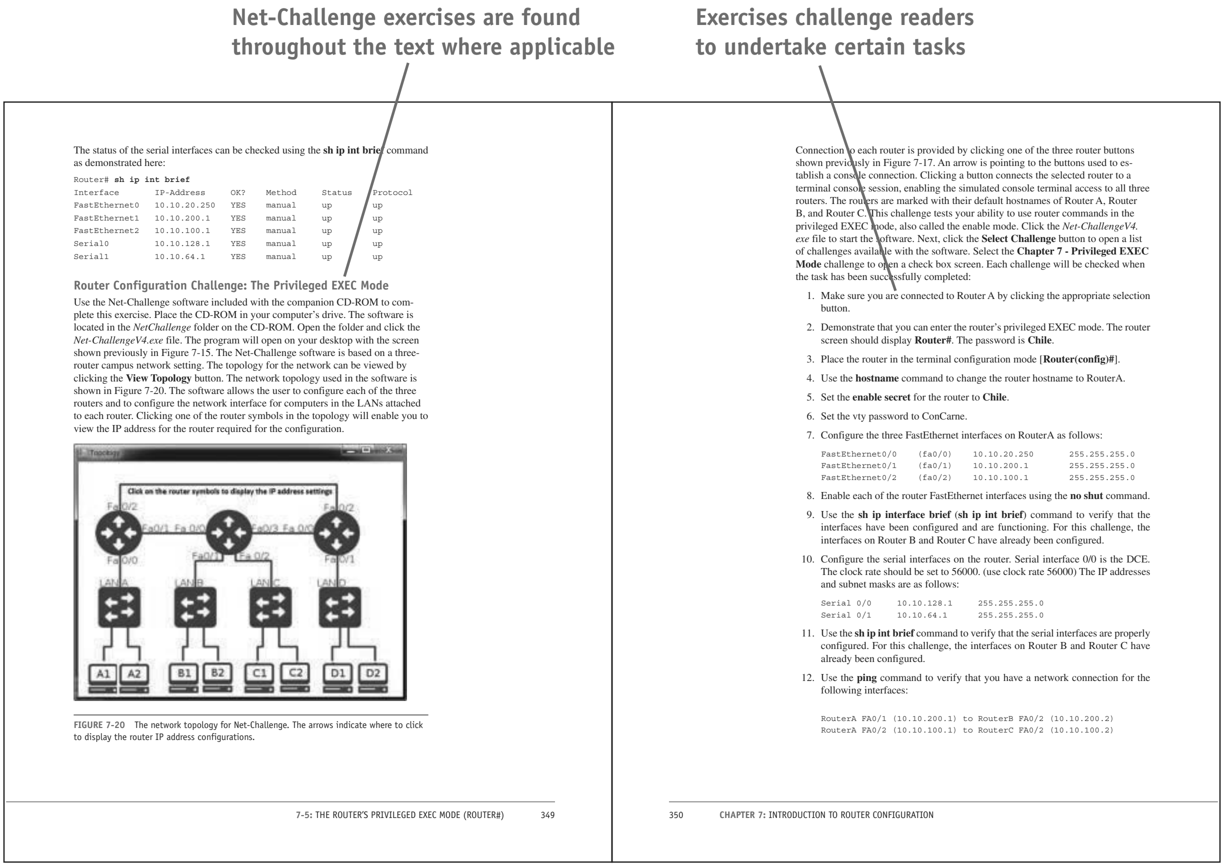
CCNP
Cisco Certified Network Professional

CCIE
Cisco Certified Internetwork Expert

320 CHAPTER 7: INTRODUCTION TO ROUTER CONFIGURATION

FIGURE P-1

- *Net-Challenge Software* provides a simulated, hands-on experience in configuring routers and switches. Exercises provided in the text (see Figure P-2) and on the CD-ROM challenge readers to undertake certain router/network configuration tasks. The challenges check the students' ability to enter basic networking commands and to set up router functions, such as configuring the interface (Ethernet and Serial) and routing protocols (that is, RIP and static). The software has the look and feel of actually being connected to the router's console port.



The status of the serial interfaces can be checked using the **sh ip int brief** command as demonstrated here:

```
Router# sh ip int brief
Interface        IP-Address     OK?   Method    Status    Protocol
FastEthernet0    10.10.20.250   YES   manual    up        up
FastEthernet1    10.10.200.1    YES   manual    up        up
FastEthernet2    10.10.100.1    YES   manual    up        up
Serial0          10.10.128.1    YES   manual    up        up
Serial1          10.10.64.1     YES   manual    up        up
```

Router Configuration Challenge: The Privileged EXEC Mode

Use the Net-Challenge software included with the companion CD-ROM to complete this exercise. Place the CD-ROM in your computer's drive. The software is located in the *NetChallenge* folder on the CD-ROM. Open the folder and click the *Net-ChallengeV4.exe* file. The program will open on your desktop with the screen shown previously in Figure 7-15. The Net-Challenge software is based on a three-router campus network setting. The topology for the network can be viewed by clicking the **View Topology** button. The network topology used in the software is shown in Figure 7-20. The software allows the user to configure each of the three routers and to configure the network interface for computers in the LANs attached to each router. Clicking one of the router symbols in the topology will enable you to view the IP address for the router required for the configuration.

FIGURE 7-20 The network topology for Net-Challenge. The arrows indicate where to click to display the router IP address configurations.

7-5: THE ROUTER'S PRIVILEGED EXEC MODE (ROUTER#) 349

Connection to each router is provided by clicking one of the three router buttons shown previously in Figure 7-17. An arrow is pointing to the buttons used to establish a console connection. Clicking a button connects the selected router to a terminal console session, enabling the simulated console terminal access to all three routers. The routers are marked with their default hostnames of Router A, Router B, and Router C. This challenge tests your ability to use router commands in the privileged EXEC mode, also called the enable mode. Click the *Net-ChallengeV4.exe* file to start the software. Next, click the **Select Challenge** button to open a list of challenges available with the software. Select the **Chapter 7 - Privileged EXEC Mode** challenge to open a check box screen. Each challenge will be checked when the task has been successfully completed:

1. Make sure you are connected to Router A by clicking the appropriate selection button.
2. Demonstrate that you can enter the router's privileged EXEC mode. The router screen should display **Router#**. The password is **Chile**.
3. Place the router in the terminal configuration mode [**Router(config)#**].
4. Use the **hostname** command to change the router hostname to RouterA.
5. Set the **enable secret** for the router to **Chile**.
6. Set the vty password to ConCarne.
7. Configure the three FastEthernet interfaces on RouterA as follows:

```
FastEthernet0/0    (fa0/0)    10.10.20.250     255.255.255.0
FastEthernet0/1    (fa0/1)    10.10.200.1      255.255.255.0
FastEthernet0/2    (fa0/2)    10.10.100.1      255.255.255.0
```

8. Enable each of the router FastEthernet interfaces using the **no shut** command.
9. Use the **sh ip interface brief** (**sh ip int brief**) command to verify that the interfaces have been configured and are functioning. For this challenge, the interfaces on Router B and Router C have already been configured.
10. Configure the serial interfaces on the router. Serial interface 0/0 is the DCE. The clock rate should be set to 56000. (use clock rate 56000) The IP addresses and subnet masks are as follows:

```
Serial 0/0     10.10.128.1     255.255.255.0
Serial 0/1     10.10.64.1      255.255.255.0
```

11. Use the **sh ip int brief** command to verify that the serial interfaces are properly configured. For this challenge, the interfaces on Router B and Router C have already been configured.
12. Use the **ping** command to verify that you have a network connection for the following interfaces:

```
RouterA FA0/1 (10.10.200.1) to RouterB FA0/2 (10.10.200.2)
RouterA FA0/2 (10.10.100.1) to RouterC FA0/2 (10.10.100.2)
```

350 CHAPTER 7: INTRODUCTION TO ROUTER CONFIGURATION

FIGURE P-2

- The textbook features and introduces how to use the *Wireshark Network Protocol Analyzer*. Examples of using the software to analyze data traffic are included throughout the text. *Numerous worked-out examples* are included in every chapter to reinforce key concepts and aid in subject mastery, as shown in Figure P-3.

Examples using the Wireshark protocol analyzer are included throughout the text where applicable

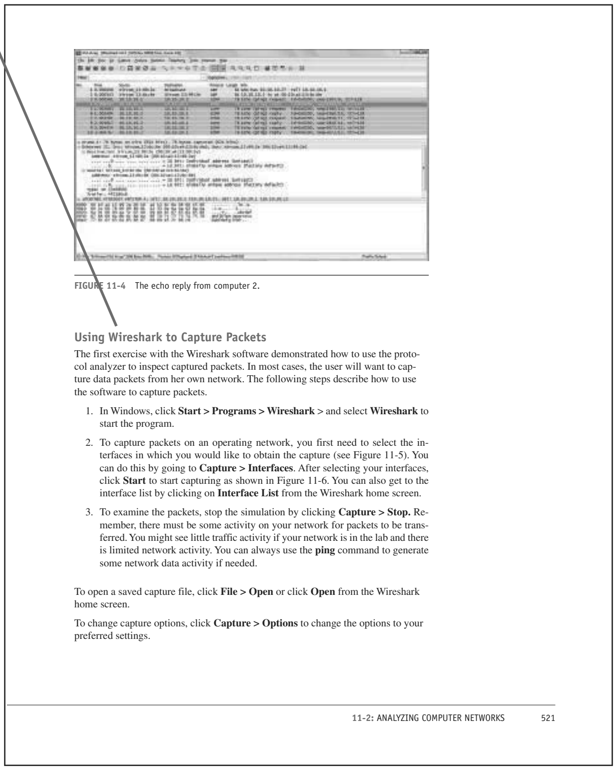


FIGURE 11-4 The echo reply from computer 2.

Using Wireshark to Capture Packets

The first exercise with the Wireshark software demonstrated how to use the protocol analyzer to inspect captured packets. In most cases, the user will want to capture data packets from her own network. The following steps describe how to use the software to capture packets.

1. In Windows, click **Start > Programs > Wireshark >** and select **Wireshark** to start the program.
2. To capture packets on an operating network, you first need to select the interfaces in which you would like to obtain the capture (see Figure 11-5). You can do this by going to **Capture > Interfaces**. After selecting your interfaces, click **Start** to start capturing as shown in Figure 11-6. You can also get to the interface list by clicking on **Interface List** from the Wireshark home screen.
3. To examine the packets, stop the simulation by clicking **Capture > Stop.** Remember, there must be some activity on your network for packets to be transferred. You might see little traffic activity if your network is in the lab and there is limited network activity. You can always use the **ping** command to generate some network data activity if needed.

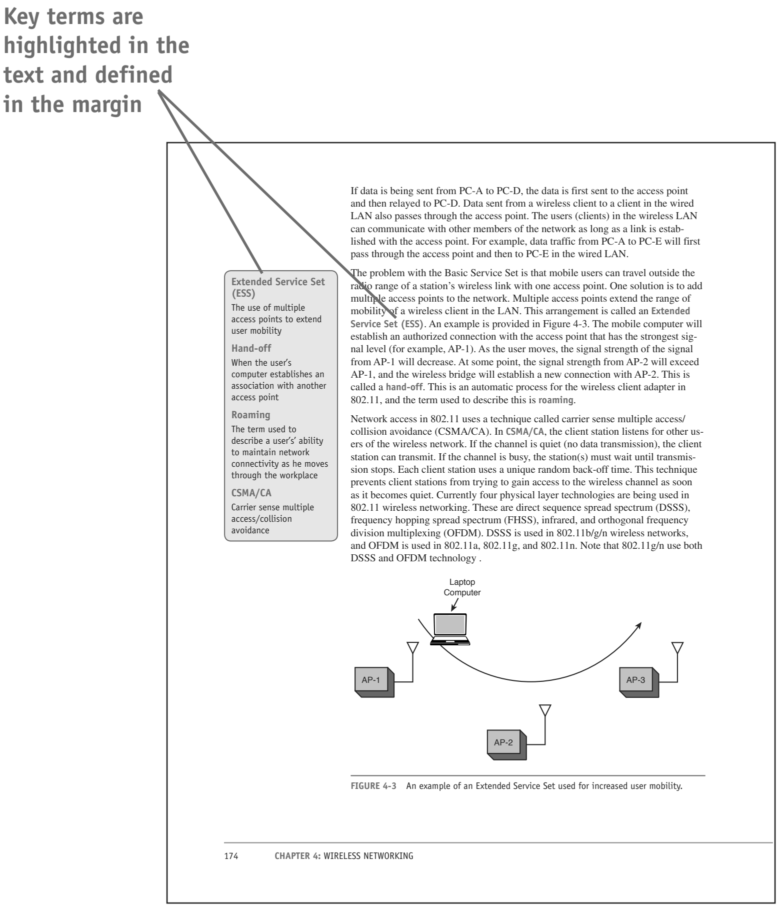
To open a saved capture file, click **File > Open** or click **Open** from the Wireshark home screen.

To change capture options, click **Capture > Options** to change the options to your preferred settings.

11-2: ANALYZING COMPUTER NETWORKS 521

FIGURE P-3

- *Key Terms* and their definitions are highlighted in the margins to foster inquisitiveness and ensure retention. Illustrations and photos are used throughout to aid in understanding the concepts discussed. This is illustrated in Figure P-4.



If data is being sent from PC-A to PC-D, the data is first sent to the access point and then relayed to PC-D. Data sent from a wireless client to a client in the wired LAN also passes through the access point. The users (clients) in the wireless LAN can communicate with other members of the network as long as a link is established with the access point. For example, data traffic from PC-A to PC-E will first pass through the access point and then to PC-E in the wired LAN.

The problem with the Basic Service Set is that mobile users can travel outside the radio range of a station's wireless link with one access point. One solution is to add multiple access points to the network. Multiple access points extend the range of mobility of a wireless client in the LAN. This arrangement is called an **Extended Service Set (ESS)**. An example is provided in Figure 4-3. The mobile computer will establish an authorized connection with the access point that has the strongest signal level (for example, AP-1). As the user moves, the signal strength of the signal from AP-1 will decrease. At some point, the signal strength from AP-2 will exceed AP-1, and the wireless bridge will establish a new connection with AP-2. This is called a **hand-off**. This is an automatic process for the wireless client adapter in 802.11, and the term used to describe this is **roaming**.

Network access in 802.11 uses a technique called carrier sense multiple access/collision avoidance (CSMA/CA). In **CSMA/CA**, the client station listens for other users of the wireless network. If the channel is quiet (no data transmission), the client station can transmit. If the channel is busy, the station(s) must wait until transmission stops. Each client station uses a unique random back-off time. This technique prevents client stations from trying to gain access to the wireless channel as soon as it becomes quiet. Currently four physical layer technologies are being used in 802.11 wireless networking. These are direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), infrared, and orthogonal frequency division multiplexing (OFDM). DSSS is used in 802.11b/g/n wireless networks, and OFDM is used in 802.11a, 802.11g, and 802.11n. Note that 802.11g/n use both DSSS and OFDM technology .

Extended Service Set (ESS)
The use of multiple access points to extend user mobility

Hand-off
When the user's computer establishes an association with another access point

Roaming
The term used to describe a user's' ability to maintain network connectivity as he moves through the workplace

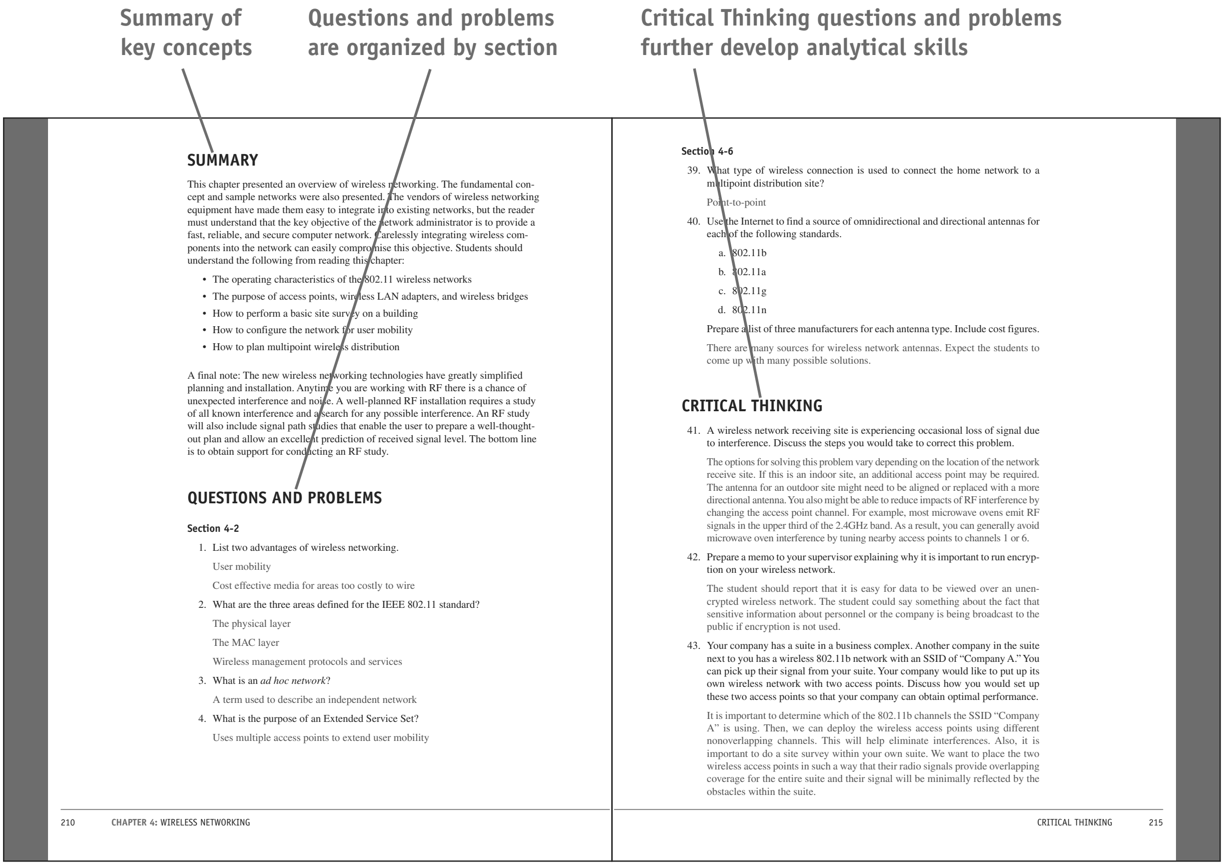
CSMA/CA
Carrier sense multiple access/collision avoidance

FIGURE 4-3 An example of an Extended Service Set used for increased user mobility.

174 CHAPTER 4: WIRELESS NETWORKING

FIGURE P-4

- *Extensive Summaries, Questions and Problems, Critical Thinking*, as well as *Network+-specific Certification Questions* are found at the end of each chapter, as shown in Figure P-5



SUMMARY

This chapter presented an overview of wireless networking. The fundamental concept and sample networks were also presented. The vendors of wireless networking equipment have made them easy to integrate into existing networks, but the reader must understand that the key objective of the network administrator is to provide a fast, reliable, and secure computer network. Carelessly integrating wireless components into the network can easily compromise this objective. Students should understand the following from reading this chapter:

- The operating characteristics of the 802.11 wireless networks
- The purpose of access points, wireless LAN adapters, and wireless bridges
- How to perform a basic site survey on a building
- How to configure the network for user mobility
- How to plan multipoint wireless distribution

A final note: The new wireless networking technologies have greatly simplified planning and installation. Anytime you are working with RF there is a chance of unexpected interference and noise. A well-planned RF installation requires a study of all known interference and a search for any possible interference. An RF study will also include signal path studies that enable the user to prepare a well-thought-out plan and allow an excellent prediction of received signal level. The bottom line is to obtain support for conducting an RF study.

QUESTIONS AND PROBLEMS

Section 4-2

1. List two advantages of wireless networking.

   User mobility

   Cost effective media for areas too costly to wire
2. What are the three areas defined for the IEEE 802.11 standard?

   The physical layer

   The MAC layer

   Wireless management protocols and services
3. What is an *ad hoc network*?

   A term used to describe an independent network
4. What is the purpose of an Extended Service Set?

   Uses multiple access points to extend user mobility

210 CHAPTER 4: WIRELESS NETWORKING

Section 4-6

39. What type of wireless connection is used to connect the home network to a multipoint distribution site?

    Point-to-point
40. Use the Internet to find a source of omnidirectional and directional antennas for each of the following standards.

    a. 802.11b

    b. 802.11a

    c. 802.11g

    d. 802.11n

    Prepare a list of three manufacturers for each antenna type. Include cost figures.

    There are many sources for wireless network antennas. Expect the students to come up with many possible solutions.

CRITICAL THINKING

41. A wireless network receiving site is experiencing occasional loss of signal due to interference. Discuss the steps you would take to correct this problem.

    The options for solving this problem vary depending on the location of the network receive site. If this is an indoor site, an additional access point may be required. The antenna for an outdoor site might need to be aligned or replaced with a more directional antenna. You also might be able to reduce impacts of RF interference by changing the access point channel. For example, most microwave ovens emit RF signals in the upper third of the 2.4GHz band. As a result, you can generally avoid microwave oven interference by tuning nearby access points to channels 1 or 6.
42. Prepare a memo to your supervisor explaining why it is important to run encryption on your wireless network.

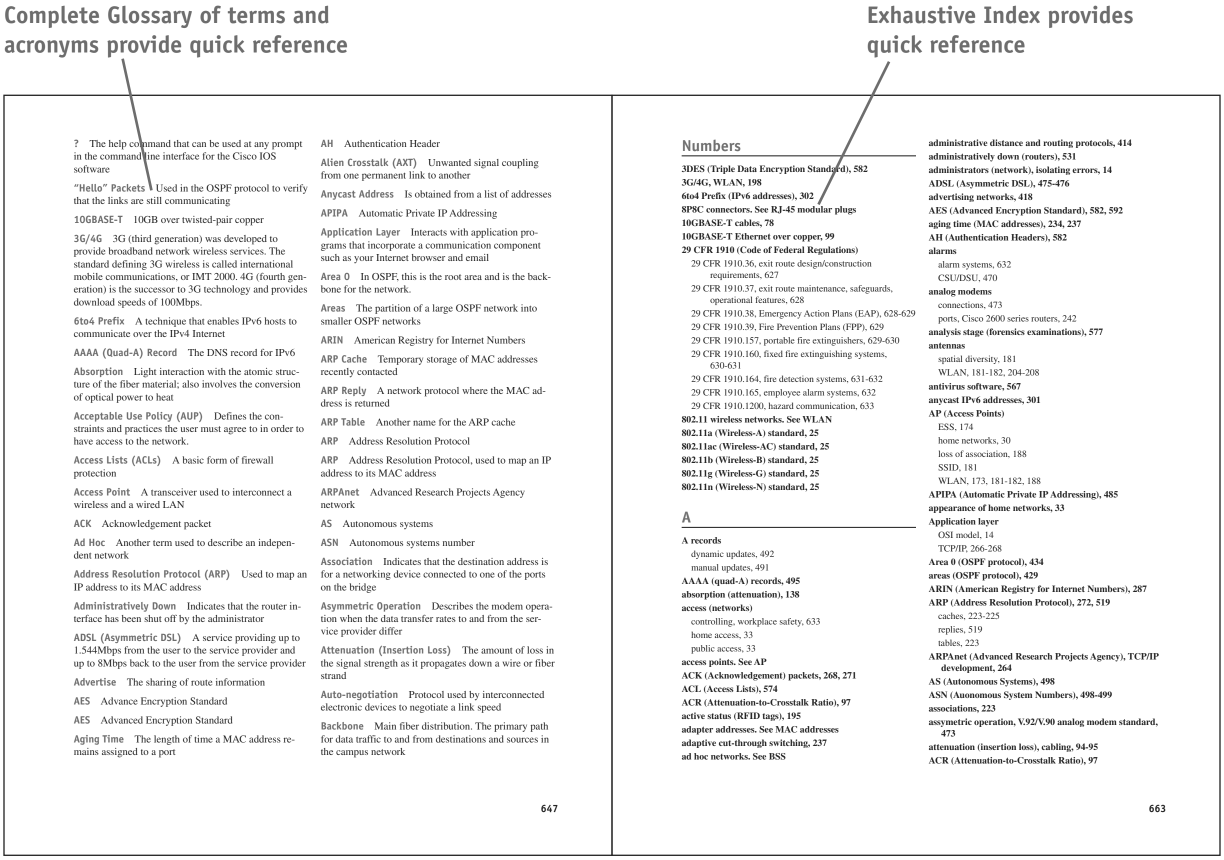
    The student should report that it is easy for data to be viewed over an unencrypted wireless network. The student could say something about the fact that sensitive information about personnel or the company is being broadcast to the public if encryption is not used.
43. Your company has a suite in a business complex. Another company in the suite next to you has a wireless 802.11b network with an SSID of "Company A." You can pick up their signal from your suite. Your company would like to put up its own wireless network with two access points. Discuss how you would set up these two access points so that your company can obtain optimal performance.

    It is important to determine which of the 802.11b channels the SSID "Company A" is using. Then, we can deploy the wireless access points using different nonoverlapping channels. This will help eliminate interferences. Also, it is important to do a site survey within your own suite. We want to place the two wireless access points in such a way that their radio signals provide overlapping coverage for the entire suite and their signal will be minimally reflected by the obstacles within the suite.

CRITICAL THINKING 215

FIGURE P-5

- An extensive *Glossary* is found at the end of the book and offers quick, accessible definitions to key terms and acronyms, as well as an exhaustive *Index* (see Figure P-6).



? The help command that can be used at any prompt in the command line interface for the Cisco IOS software

"Hello" Packets Used in the OSPF protocol to verify that the links are still communicating

10GBASE-T 10GB over twisted-pair copper

3G/4G 3G (third generation) was developed to provide broadband network wireless services. The standard defining 3G wireless is called international mobile communications, or IMT 2000. 4G (fourth generation) is the successor to 3G technology and provides download speeds of 100Mbps.

6to4 Prefix A technique that enables IPv6 hosts to communicate over the IPv4 Internet

AAAA (Quad-A) Record The DNS record for IPv6

Absorption Light interaction with the atomic structure of the fiber material; also involves the conversion of optical power to heat

Acceptable Use Policy (AUP) Defines the constraints and practices the user must agree to in order to have access to the network.

Access Lists (ACLs) A basic form of firewall protection

Access Point A transceiver used to interconnect a wireless and a wired LAN

ACK Acknowledgement packet

Ad Hoc Another term used to describe an independent network

Address Resolution Protocol (ARP) Used to map an IP address to its MAC address

Administratively Down Indicates that the router interface has been shut off by the administrator

ADSL (Asymmetric DSL) A service providing up to 1.544Mbps from the user to the service provider and up to 8Mbps back to the user from the service provider

Advertise The sharing of route information

AES Advance Encryption Standard

AES Advanced Encryption Standard

Aging Time The length of time a MAC address remains assigned to a port

AH Authentication Header

Alien Crosstalk (AXT) Unwanted signal coupling from one permanent link to another

Anycast Address Is obtained from a list of addresses

APIPA Automatic Private IP Addressing

Application Layer Interacts with application programs that incorporate a communication component such as your Internet browser and email

Area 0 In OSPF, this is the root area and is the backbone for the network.

Areas The partition of a large OSPF network into smaller OSPF networks

ARIN American Registry for Internet Numbers

ARP Cache Temporary storage of MAC addresses recently contacted

ARP Reply A network protocol where the MAC address is returned

ARP Table Another name for the ARP cache

ARP Address Resolution Protocol

ARP Address Resolution Protocol, used to map an IP address to its MAC address

ARPAnet Advanced Research Projects Agency network

AS Autonomous systems

ASN Autonomous systems number

Association Indicates that the destination address is for a networking device connected to one of the ports on the bridge

Asymmetric Operation Describes the modem operation when the data transfer rates to and from the service provider differ

Attenuation (Insertion Loss) The amount of loss in the signal strength as it propagates down a wire or fiber strand

Auto-negotiation Protocol used by interconnected electronic devices to negotiate a link speed

Backbone Main fiber distribution. The primary path for data traffic to and from destinations and sources in the campus network

647

Numbers

A

663

FIGURE P-6

Accompanying CD-ROM

The CD-ROM packaged with the text includes the captured data packets used in the text. It also includes the Net-Challenge Software, which was developed specifically for this text. The CD-ROM also includes sample videos on the topic of network virtualization from the CompTIA Network+ N10-006 Complete Video Course. See the special offer for a discount on the full version of this product in the sleeve in the back of the book.

This page intentionally left blank

5

CHAPTER

INTERCONNECTING THE LANS

Chapter Outline

Objectives

- Describe how a bridge is used to interconnect LANs
- Describe how a switch is used to interconnect LANs
- Discuss the advantages of using a switch instead of a hub
- Describe the function of a router when used to interconnect LANs
- Describe the interface associated with a router
- Describe the function of a gateway in a computer network
- Describe the concept of a network segment
- Describe the concept of auto-negotiation

Key Terms

campus network
bridge
bridging table
association
broadcast
ARP
broadcast storm
network slowdown
ARP cache
ARP table
transparent bridge
translation bridge
layer 2 switch
multiport bridge
multicast
managed switch
Cisco Network Assistant (CNA)
dynamic assignment
static assignment
secure addresses
aging time
isolating the collision–domain
content addressable memory (CAM)
flooding
broadcast domain
store-and-forward
cut-through
switch latency
error threshold
multilayer switch (MLS)
wire speed routing
network address
logical address
router interface
power on/off
auxiliary input
console input
serial ports
AUI port
media converter
enterprise network
FastEthernet port (FA0/0, FA0/1, FA0/2, …)
serial port (S0/0, S0/1, S0/2, …)
routing table
gateway
auto-negotiation
fast link pulse (FLP)
half-duplex

The utility of LANs led to the desire to connect two (or more) networks together. For example, a large corporation might have had separate networks for research and engineering and another for its manufacturing units. These network systems probably used totally different networking technologies and specifications for communicating and were located in different cities, states, or even countries, but it was deemed necessary to "tie" them together. The objective of this and subsequent chapters is to introduce the concepts and issues behind interconnecting LANs. Interconnecting LANs in a **campus network** or even interconnecting LANs in wide area networks (WANs) incorporate similar concepts and issues. The campus network is a collection of two or more interconnected LANs, either within a building or housed externally in multiple buildings.

5-1 INTRODUCTION

Campus Network
A collection of two or more interconnected LANs in a limited geographic area

The concept of interconnecting LANs is introduced in this chapter. The concept of the bridge, switch, and router is introduced here. The students are also introduced to the function of the network gateway. This is an important concept and will be used by the student when determining where data packets are delivered when they need to exit the LAN. The chapter concludes with a section on the technique of auto-negotiation. This section examines how interconnected networking devices negotiate an operating speed.

The framework defining the network layers for linking networks together is defined by the OSI model and was introduced in Chapter 1, "Introduction to Computer Networks," section 1-3. The OSI model provides a framework for networking that ensures compatibility in the network hardware and software. The concepts behind the hardware technologies used to interconnect LANs are presented in sections 5-2 to 5-5. The properties of a networking bridge are defined in section 5-2. The layer 2 switch is examined in section 5-3, and the router is introduced in section 5-4. An example of interconnecting LANs is provided in section 5-5. The chapter concludes with a section on the concept of auto-negotiation, examining the advantages and disadvantages of this network configuration option.

Table 5-1 lists and identifies, by chapter section, where each of the CompTIA Network+ objectives are presented in this chapter. The chapter sections where each objective is presented are identified. At the end of each chapter section is a review with comments of the Network+ objectives presented in that section. These comments are provided to help reinforce the reader's understanding of a particular Network+ objective. The chapter review also includes "Test Your Knowledge" questions to aid in the understanding of key concepts before the reader advances to the next section of the chapter. The end of the chapter includes a complete set of question plus sample certification type questions.

TABLE 5-1 **Chapter 5 CompTIA Network+ Objectives**

Domain/ Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	***Network Architecture***	
1.1	Explain the functions and applications of various network devices	5-3, 5-4
1.3	Install and configure the following networking services/applications	5-4
1.4	Explain the characteristics and benefits of various WAN technologies	5-4
1.7	Differentiate between network infrastructure implementations	5-2
1.8	Given a scenario, implement and configure the appropriate addressing schema	5-2, 5-3
1.9	Explain the basics of routing concepts and protocols	5-3, 5-5
2.0	***Network Operations***	
2.6	Given a scenario, configure a switch using proper features	5-4
4.0	***Troubleshooting***	
4.2	Given a scenario, analyze and interpret the output of troubleshooting tools	5-3
4.6	Given a scenario, troubleshoot and resolve common network issues	5-5
5.0	***Industry standards, practices, and network theory***	
5.2	Explain the basics of network theory and concepts	5-2, 5-4, 5-6

5-2 THE NETWORK BRIDGE

This section examines how a bridge is used in computer networks to interconnect LANs. This section establishes how the bridge builds a table of connected users on the bridge ports. This concept is used with switches and access points in wireless LANs. It is important that the student understands that a bridge can be used to isolate data traffic.

A bridge can be used in computer networks to interconnect two LANs together and separate network segments. Recall that a *segment* is a section of a network separated by bridges, switches, and routers. The **bridge** is a layer 2 device in the OSI model, meaning that it uses the MAC address information to make decisions regarding forwarding data packets. Only the data that needs to be sent across the bridge to the adjacent network segment is forwarded. This makes it possible to

Bridge
A networking device that uses the MAC address to forward data and interconnect two LANs

isolate or segment the network data traffic. An example of using a bridge to segment two Ethernet LANs is shown in Figure 5-1. The picture shows that LAN A connects to port 1 of the bridge and LAN B connects to port 2 on the bridge, creating two segments, as shown. There are four computers in LAN A and three computers in LAN B. It is important to note that bridges are now legacy networking devices, but studying these will help you better understand the functionality of switches, especially how data traffic is sent to connected LANs.

Bridging Table
List of MAC addresses and port locations for hosts connected to the bridge ports

Bridges monitor all data traffic in each of the LAN segments connected to its ports. Recall that a *port* is an input/output connection on a networking device. The bridges use the MAC addresses to build a **bridging table** of MAC addresses and port locations for hosts connected to the bridge ports. A sample bridging table is provided in Table 5-2. The table shows the stored MAC address and the port where the address was obtained.

TABLE 5-2 **Bridging Table**

MAC Address	Port
00-40-96-25-85-BB	1
00-40-96-25-8E-BC	1
00-60-97-61-78-5B	2
00-C0-4F-27-20-C7	2

The source MAC address is stored in the bridge table as soon as a host talks (transmits a data packet) on the LAN. For example, if computer 1 in LAN A sends a message to computer 2 (see Figure 5-1), the bridge will store the MAC addresses of both computers and record that both of these computers are connected to port 1. If computers 5 or 6 are placing data packets on the network, then the source MAC addresses for 5 and 6 are stored in the bridge table and it is recorded that these computers connect to port 2 on the bridge. The MAC addresses for computers 3 and 4 will not be added to the bridging table until each transmits a data packet.

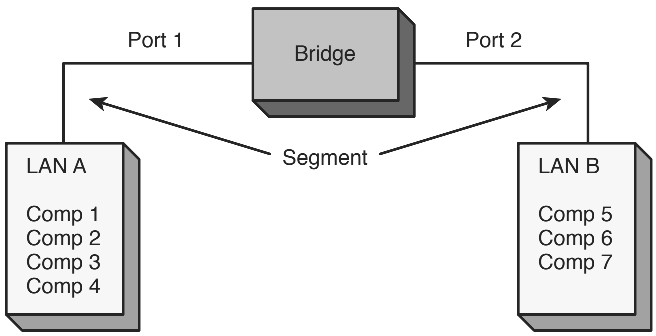


FIGURE 5-1 Using a bridge to interconnect two Ethernet LANs.

The bridge monitors the data on its ports to check for an **association** between the destination MAC address of the Ethernet frames to any of the hosts connected to its ports. An association indicates that the destination MAC address for a host is connected to one of the ports on the bridge. If an association is found, the data is forwarded to that port. For example, assume that computer 1 sends a message to computer 5 (see Figure 5-1). The bridge detects an association between the destination MAC address for computer 5 and port 2. The bridge then forwards the data from computer 1 to computer 5 in LAN B via port 2.

Association
Indicates that the destination address is for a networking device connected to one of the ports on the bridge

The capability of a bridge to forward data packets only when there is an association is used to isolate data traffic in each segment. For example, assume that computer 1 and computer 2 in LAN A generate a lot of data traffic. The computers in LAN B will not see any of the data traffic as long as there is not an association between the destination MAC addresses of the Ethernet packets and any of the hosts in LAN B (computers 5, 6, and 7).

A potential problem with bridges has to do with the way broadcasts are handled. A **broadcast** means the message is being sent to all computers on the network; therefore, all broadcasts in a LAN will be forwarded to all hosts connected within the bridged LANs. For example, the broadcast associated with an ARP will appear on all hosts. **ARP** stands for Address Resolution Protocol, which is a protocol used to map an IP address to its MAC address. In the address resolution protocol, a broadcast is sent to all hosts in a LAN connected to the bridge. This is graphically shown in Figure 5-2. The bridge forwards all broadcasts; therefore, an ARP request broadcasting the message "Who has this IP address?" is sent to all hosts on the LAN. The data packets associated with ARP requests are small, but it requires computer time to process each request. Excessive amounts of broadcasts being forwarded by the bridge can lead to a **broadcast storm**, resulting in degraded network performance, called a **network slowdown**.

Broadcast
Transmission of the data to all connected devices

ARP
Address Resolution Protocol

Broadcast Storm
Excessive amounts of broadcasts

Network Slowdown
Degraded network performance

The MAC address entries stored in a bridge table are temporary. Each MAC address entry to the bridge table remains active as long as there is periodic data traffic activity from that host on its port. However, an entry into the table is deleted if the port becomes inactive. In other words, the entries stored into the table have a limited lifetime. An expiration timer will commence once the MAC address is entered into the bridge table. The lifetime for the entry is renewed by new data traffic by the computer, and the MAC address is reentered.

In a similar manner, all networking devices (for example, computers) contain an **ARP cache**, a temporary storage of MAC addresses recently contacted. This is also called the **ARP table**. The ARP cache holds the MAC address of a host, and this enables the message to be sent directly to the destination MAC address without the computer having to issue an ARP request for a MAC address. The following list outlines typical steps of a communication process between computer 1 and computer 2.

ARP Cache
Temporary storage of MAC addresses recently contacted

ARP Table
Another name for the ARP cache

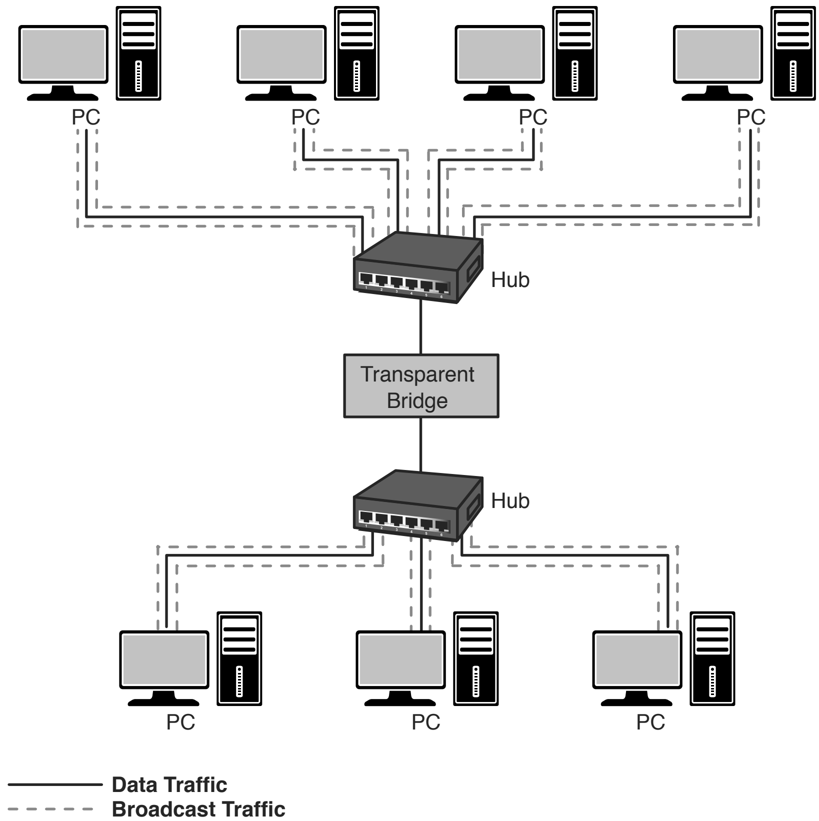


FIGURE 5-2 An example of using a bridge to isolate data traffic.

1. Computer 1 checks its ARP cache to determine if it already has the MAC address of computer 2. If it does, it will skip to the final step; otherwise, it proceeds to the next step.
2. Computer 1 generates an ARP request message for computer 2 with its own MAC and IP information included.
3. Computer 1 then broadcasts the ARP request message on its local network.
4. Every local network device processes the ARP request message. Those computers that are not computer 2 will discard the message.
5. Only a match, which is computer 2, generates an ARP reply message and updates its ARP cache with computer 1 MAC and IP information.
6. Computer 2 sends an ARP reply message directly to computer 1.
7. Computer 1 receives the ARP reply message and updates its ARP cache with the MAC and IP of computer 2.

The ARP cache contents on a Windows computer can be viewed using the **arp -a** command while in the command prompt, as shown here:

Windows			Mac OS X
C:**arp –a**			jmac:~mymac$ **arp –a**
Interface: 10.10.20.2 on Interface x1000002			C1.salsa.org (192.168.12.1) at
Internet Address	Physical Address	Type	00-08-a3-a7-78-0c on en1
10.10.20.3	00-08-a3-a7-78-0c	dynamic	[ethernet]
10.10.20.4	00-03-ba-04-ba-ef	dynamic	C3.salsa.org (192.168.12.1) at
			00-08-a3-a7-78-0c on en1
			[ethernet]

The ARP cache contents on a Mac OS X computer can be viewed using the **arp -a** command while in the terminal mode.

The following message is generated if all the ARP entries have expired:

```
c:\arp -a
No ARP Entries Found
```

The name for the type of bridge used to interconnect two LANs running the same type of protocol (for example, Ethernet) is a **transparent bridge**. Bridges are also used to interconnect two LANs that are operating two different networking protocols. For example, LAN A could be an Ethernet LAN and LAN B could be a token ring. This type of bridge is called a **translation bridge**. An example is provided in Figure 5-3. The bridge allows data from one LAN to be transferred to another. Also the MAC addressing information is standardized so the same address information is used regardless of the protocol.

Transparent Bridge
Interconnects two LANs running the same type of protocol

Translation Bridge
Used to interconnect two LANs that are operating two different networking protocols

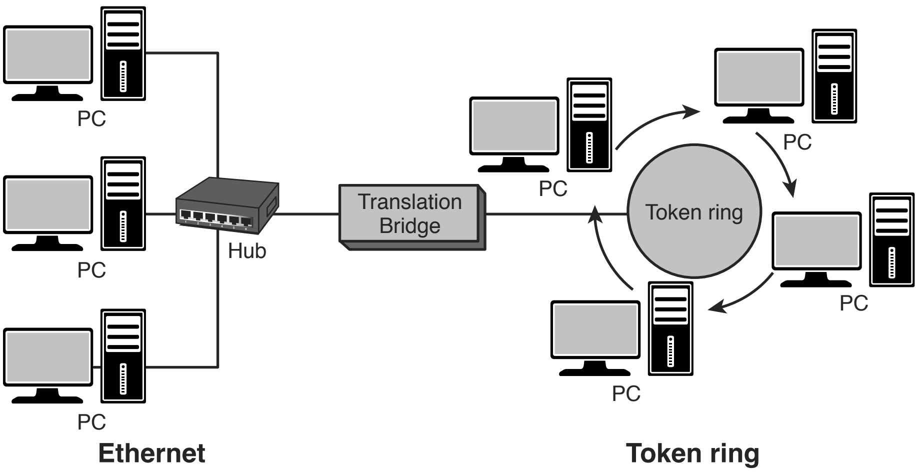


FIGURE 5-3 Using a translation bridge to interconnect an Ethernet and token-ring LAN.

A common application today using a bridge is interconnecting LANs using wireless technology. The use of wireless bridges in LANs is a popular choice for interconnecting the LANs when the cost of physically connecting them is prohibitive. Wireless technology and its LAN applications were presented in Chapter 4, "Wireless Networking."

The use of a bridge is not as common as it used to be except for wireless network applications. New networking technologies are available that provide similar capabilities to the bridge but that are much more powerful. However, the bridge still is useful and has several advantages. Table 5-3 provides a summary of the advantages and disadvantages of a networking bridge.

TABLE 5-3 **Summary of the Advantages and Disadvantages of a Bridge for Interconnecting LANs**

Advantages	Disadvantages
Easy to install	Works best in low-traffic areas
Does an excellent job of isolating the data traffic in two segments	Forwards broadcasts and is susceptible to broadcast storms
Relatively inexpensive	
Can be used to interconnect two LANs with different protocols and hardware	
Reduces collision domains (remember how the CSMA/CD protocol works)	

Section 5-2 Review

This section has covered the following **Network+** Exam objectives.

1.7 Differentiate between network infrastructure implementations

This section presents a look at the network bridge. The advantages and disadvantages of the network bridge are presented in Table 5-3. A key concept presented in this section is an "association" that indicates that the destination address for a networking device has been obtained.

1.8 Given a scenario, implement and configure the appropriate addressing schema

Another important concept presented in this section is that a bridge will pass a broadcast to all devices connected to its ports. Excessive broadcast can potentially have a negative impact on data traffic and result in a network slowdown. The purpose of the bridging table for storing the MAC addresses of connected devices was also presented. Each MAC address entry to the bridge table remains active as long as there is periodic data traffic activity from that host on its port. However, an entry into the table is deleted if the port becomes inactive.

5.2 Explain the basics of network theory and concepts

An important concept presented in this section is that a bridge will pass a broadcast to all devices connected to its ports. Excessive broadcast can potentially have a negative impact on data traffic and result in a network slowdown.

Test Your Knowledge

1. Which command is used on a computer to view the contents of the ARP cache?
    a. **arp -c**
    b. **arp -l**
    c. **arp -a**
    d. **arp -b**
    e. **arp**
2. An association indicates which of the following?
    a. That the destination address for a networking device is connected to one of its ports
    b. That the source address is for a networking device connected to one of the ports on the bridge
    c. That the destination address is for a networking device connected to one of the ports on the hub
    d. That the source address is for a networking device connected to one of the ports on the hub
3. An ARP cache is which of the following?
    a. A temporary storage of IP addresses for networking devices recently contacted
    b. A temporary storage of MAC addresses for networking devices to be contacted
    c. A temporary storage of IP addresses for networking devices to be contacted
    d. A temporary storage of MAC addresses for networking devices recently contacted

5-3 THE NETWORK SWITCH

The network switch provides a method for isolating collision domains for interconnected LANs. In fact, most new networks should be using a layer 2 switch rather than a hub. Make sure the student understands why this is called a layer 2 switch (MAC address). This section contains a Hub-Switch comparison that shows how the switch isolates data traffic. Use this comparison to show the student the improvement with the switch using the a network analyzer such as Wireshark. You might want to have the students try to duplicate this task in lab. The section concludes with an overview of a managed switch. Switches vary for make and manufacturer, but the basic concepts are the same. The use of the Cisco Network Assistant (CNA) software for managing switches is presented. The two modes used in a switch to forward frames (**store-and-forward** and **cut-through**) are presented. The student should be familiar with this and any related concepts.

The bridge provides a method for isolating the collision domains for interconnected LANs but lacks the capability to provide a direct data connection for the hosts. The bridge forwards the data traffic to all computers connected to its port. This was shown in Figure 5-2. The networking hub provides a technology for sharing access to the network with all computers connected to its ports in the LAN but lacks the capability to isolate the data traffic and provide a direct data connection from the source to the destination computer. The increase in the number of computers being used in LANs and the increased data traffic are making bridges and hubs of limited use in larger LANs. Basically, there is too much data traffic to be shared by the entire network. What is needed is a networking device that provides a direct data connection between communicating devices. Neither the bridge nor the hub provides a direct data connection for the hosts. A technology developed to improve the efficiency of the data networks and address the need for direct data connections is the layer 2 switch.

Layer 2 Switch
An improved network technology that provides a direct data connection for network devices in a LAN

Multiport Bridge
Another name for a layer 2 switch

The **layer 2 switch** is an improved network technology that addresses the issue of providing direct data connections, minimizing data collisions, and maximizing the use of a LAN's bandwidth; in other words, that improves the efficiency of the data transfer in the network. The switch operates at layer 2 of the OSI model and therefore uses the MAC or Ethernet address for making decisions for forwarding data packets. The switch monitors data traffic on its ports and collects MAC address information in the same way the bridge does to build a table of MAC addresses for the devices connected to its ports. The switch has multiple ports similar to the hub and can switch in a data connection from any port to any other port, similar to the bridge. This is why the switch is sometimes called a **multiport bridge**. The switch minimizes traffic congestion and isolates data traffic in the LAN. Figure 5-4 provides an example of a switch being used in a LAN.

Figure 5-4 shows a switch being used in the LAN to interconnect the hosts. In this figure, the hub has been replaced with a switch. The change from a hub to a switch is relatively easy. The port connections are the same (RJ-45), and once the connections are changed and the device is powered on, the switch begins to make the direct data connections for multiple ports using layer 2 switching.

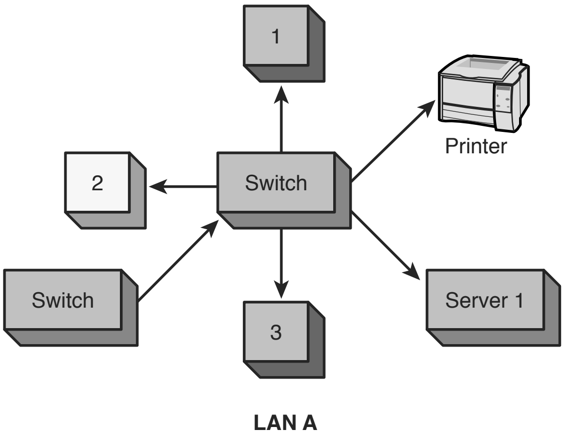


FIGURE 5-4 A switch used to interconnect hosts in a LAN.

> **Multicast**
> Messages are sent to a specific group of hosts on the network

The LAN shown in Figure 5-5 contains 14 computers and 2 printers connected to 16 ports on the switch, configured in a star topology. If the computer connected to port 1 is printing a file on the laser printer (port 12), the switch will set up a direct connection between ports 1 and 12. The computer at port 14 could also be communicating with the computer at port 7, and the computer at port 6 could be printing a file on the color printer at port 16. The use of the switch enables simultaneous direct data connections for multiple pairs of hosts connected to the network. Each switch connection provides a link with minimal collisions and therefore maximum use of the LAN's bandwidth. A link with minimal collisions is possible because only the two computers that established the link will be communicating over the channel. Recall that in the star topology each host has a direct connection to the switch. Therefore, when the link is established between the two hosts, their link is isolated from any other data traffic. However, the exception to this is when broadcast or **multicast** messages are sent in the LAN. In the case of a broadcast message, the message is sent to all devices connected to the LAN. A multicast message is sent to a specific group of hosts on the network.

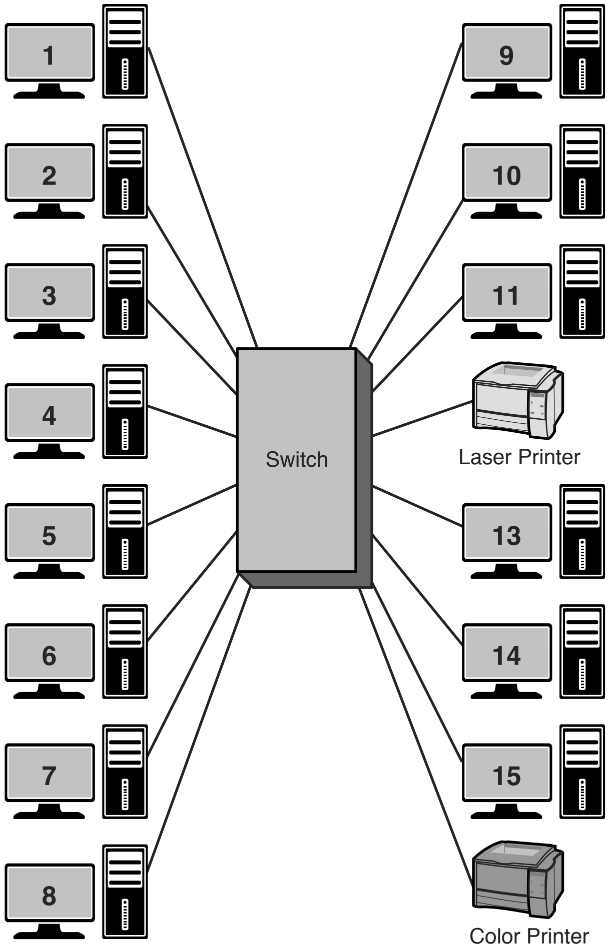


FIGURE 5-5 A switch used to interconnect the networking devices in a LAN.

Hub–Switch Comparison

An experiment was set up to test the data handling characteristics of a hub and a switch given the same input instructions. The objective of this experiment was to show that data traffic is isolated with a switch but not with a hub. For this experiment, a LAN using a hub and a LAN using a switch were assembled. The LANs are shown in Figure 5-6(a) and (b). Each LAN contains four computers connected in a star topology. The computers are marked 1–4 for reference. The IP addresses are listed for each host.

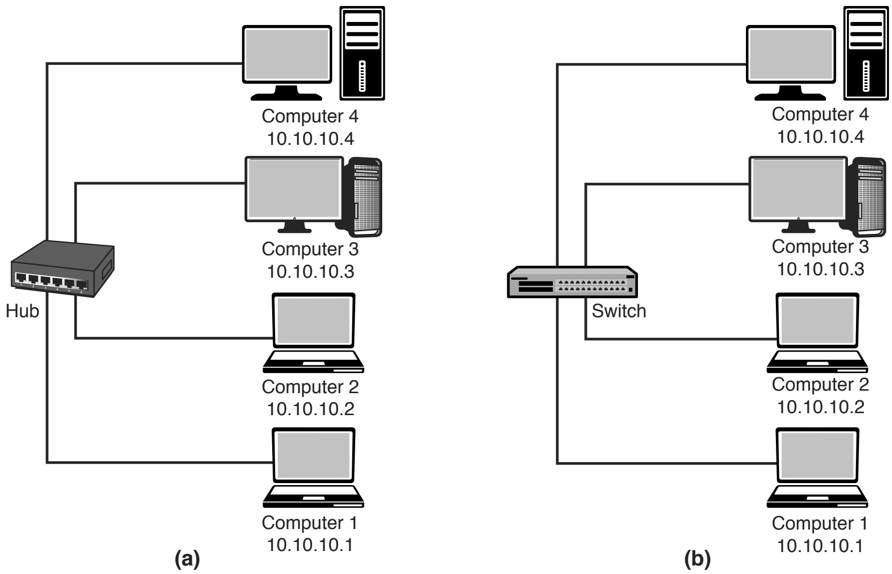


FIGURE 5-6 (a) The LAN experiment with a hub; (b) the LAN experiment with a switch.

The Hub Experimental Results

In this experiment, computer 1 pinged computer 3. Computer 2 was used to capture the LAN data traffic using a network protocol analyzer. What are the expected results? Remember, a hub is a multiport repeater, and all data traffic input to the hub is passed on to all hosts connected to its ports. See the Ping Command Review section that follows for a brief review of the use of the **ping** command.

Ping Command Review

The **ping** command is used to verify that a network connection exists between two computers. The command format for **ping** is:

```
ping [ip address] {for this example ping 10.10.10.3}
```

After a link is established between the two computers, a series of echo requests and echo replies are issued by the networking devices to test the time it takes for data to pass through the link. The protocol used by the **ping** command is the Internet Connection Message Protocol (ICMP).

The **ping** command is issued to an IP address; however, delivery of this command to the computer designated by the IP address requires that a MAC address be identified for final delivery. The computer issuing the **ping** might not know the MAC address of the computer holding the identified IP address (no entry in the ARP cache table); therefore, an ARP request is issued. An ARP request is broadcast to all computers connected in the LAN. The computer that holds the IP address replies with its MAC address, and a direct line of communications is then established.

The data traffic collected by computer 2 when computer 1 pinged computer 3 is provided in Figure 5-7. The first line of the captured data shows the ARP request asking who has the IP address 10.10.10.3. The second line of the captured data shows the reply from 10.10.10.3 with the MAC address of 00-B0-D0-25-BF-48. The next eight lines in the captured data are the series of four echo requests and replies associated with a ping request. Even though computer 2 was not being pinged or replying to the ARP request, the data traffic was still present on computer 2's hub port. The echo reply is from a Dell network interface card with the last six characters of the MAC address of 25-BF-48. The echo request is coming from a computer with 13-99-2E as the last six hex characters of its MAC address.

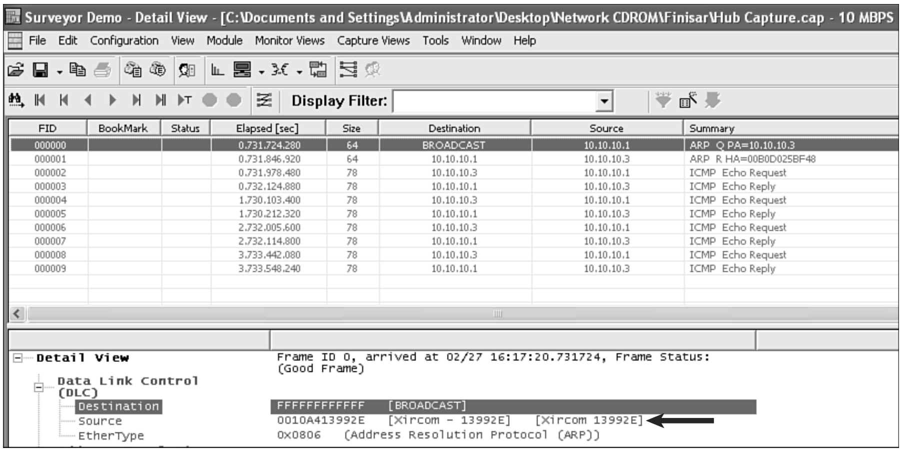


FIGURE 5-7 The captured data traffic by computer 2 for the LAN [Figure 5-6(a)] using a hub.

The Switch Experimental Results

The same experiment was repeated for the LAN shown in Figure 5-6(b), this time using a switch to interconnect the computers instead of a hub. This network consists of four computers connected in a star topology using a switch at the center of the network. The **ping** command was sent from computer 1 to computer 3, **ping 10.10.10.3**. The ARP cache for computer 1 is empty; therefore, the MAC address for computer 3 is not known by computer 1. An ARP request is issued by computer 1, and computer 3 replies. The series of echo requests and echo replies follow; however, the data traffic captured by computer 2 (Figure 5-8), shows the ARP request asking who has the IP address 10.10.10.3. This is the last of the data communications between computers 1 and 3 seen by computer 2. A direct line of communication between computers 1 and 3 is established by the switch that prevents computer 2 from seeing the data traffic from computers 1 and 3. The only data traffic seen by computer 2 in this process was the broadcast of the ARP request. This is true for any other hosts in the LAN. The results of this experiment show that the use of the switch substantially reduces data traffic in the LAN, particularly unnecessary data traffic. The experiment shows that the broadcast associated with an ARP request is seen by all computers but not the ARP replies in a LAN using a switch. This is because a direct data connection is established between the two hosts. This experiment used pings and ARPs; however, this same advantage of using a switch is true when transferring files, image downloads, file printing, and so on. The data traffic is isolated from other computers on the LAN. Remember, the switch uses MAC addresses to establish which computers are connected to its ports. The switch then extracts the destination MAC address from the Ethernet data packets to determine to which port to switch the data.

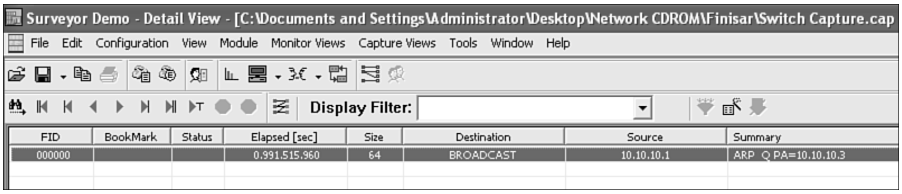


FIGURE 5-8 The data traffic captured by computer 2 for the LAN [Figure 5-6(b)] using a switch.

Managed Switches

A **managed switch** is simply a network switch that allows the network administrator to monitor, configure, and manage certain network features such as which computers are allowed to access the LAN via the switch. Access to the management features for the switch is password protected so that only the network administrators can gain entry. The following information describes some of the features of the managed interface for a Cisco Catalyst 2900 series switch established using the **Cisco Network Assistant (CNA)**. This software can be downloaded from Cisco and provides an easy way to manage the features of the Cisco switches. (*Note:* The download requires that you have set up a Cisco user account and password. The Cisco Network Assistant provides for a centralized mode for completing various network administration tasks for switches, routers, and wireless networking equipment.)

Managed Switch
Allows the network administrator to monitor, configure, and manage select network features

Cisco Network Assistant (CNA)
A management software tool from Cisco that simplifies switch configuration and troubleshooting

The start-up menu for a Cisco Catalyst 2960 switch obtained via the CNA is provided in Figure 5-9. The image is showing the current setup for the switch. The assigned IP address for the switch is 192.168.1.1, and a router and a switch are interconnected with the switch. The steps for setting the IP address for an interface on the switch are presented later in this section.

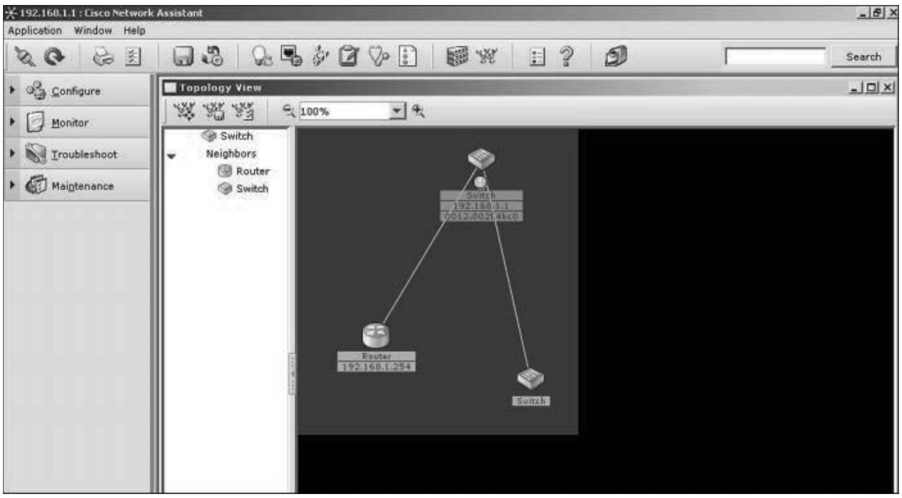


FIGURE 5-9 The start-up menu of a Cisco Catalyst switch using the Cisco Network Administrator software.

The current connections to the ports on the switch can be viewed by clicking the stacked switch icon at the top of the screen as shown in Figure 5-10. The image of the switch port connections shows ports 1, 2, and 3 are brighter, indicating that there are networking devices connected to the ports. The MAC addresses of the devices connected to the switch ports can be displayed by clicking the MAC address button under the Configure button as shown in Figure 5-11. Four MAC addresses are assigned to port 1, one MAC address is assigned to port 2, and one MAC address is assigned to port 3. Multiple networking devices can be connected to a port if the devices are first connected to another switch or hub and the output of the switch or hub is connected to one switch port. An example showing four devices connected through a hub to port 1 on the switch is shown in Figure 5-12. The output interface information for the MAC Addresses table shows the following information in Figure 5-11:

FastEthernet 0/1
FastEthernet 0/2
FastEthernet 0/3

Dynamic Assignment
MAC addresses are assigned to a port when a host is connected

Static Addressing
The MAC address has been manually assigned to a switch port

Secure Address
The switch port will automatically disable itself if a device with a different MAC address connects to the port

Notice that the Dynamic Address tab is highlighted. This indicates that this is a listing of the MAC addresses that have been assigned dynamically. **Dynamic assignment** means that the MAC address was assigned to a port when a host was connected. There is also a tab for Static Addresses. **Static addressing** indicates that the MAC address has been manually assigned to an interface, and the port assignment does not expire. The Secure tab shows what switch ports have been secured. A **secure address** means that a MAC address has been assigned to a port, and the port will automatically disable itself if a device with a different MAC address connects to the secured port.

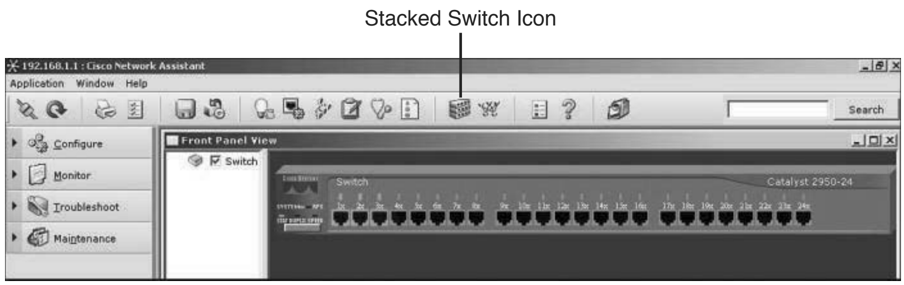


FIGURE 5-10 The highlighted ports showing the current connections and the location of the stacked switches icon.

The FastEthernet 0/1, FastEthernet 0/2, FastEthernet 0/3 notation indicates the [Interface Type Slot#/Interface#] on the switch, and FastEthernet indicates that this interface supports 100Mbps and 10Mbps data rate connections.

Aging Time
The length of time a MAC address remains assigned to a port

The "Aging Time" is listed to be 300 seconds. **Aging time** is the length of time a MAC address remains assigned to a port. The assignment of the MAC address will be removed if there is no data activity within this time. If the computer with the assigned MAC address initiates new data activity, the aging time counter is restarted, and the MAC address remains assigned to the port. The management window shows a switch setting for enabling "Aging." This switch is used to turn off the aging counter so that a MAC address assignment on a port never expires.

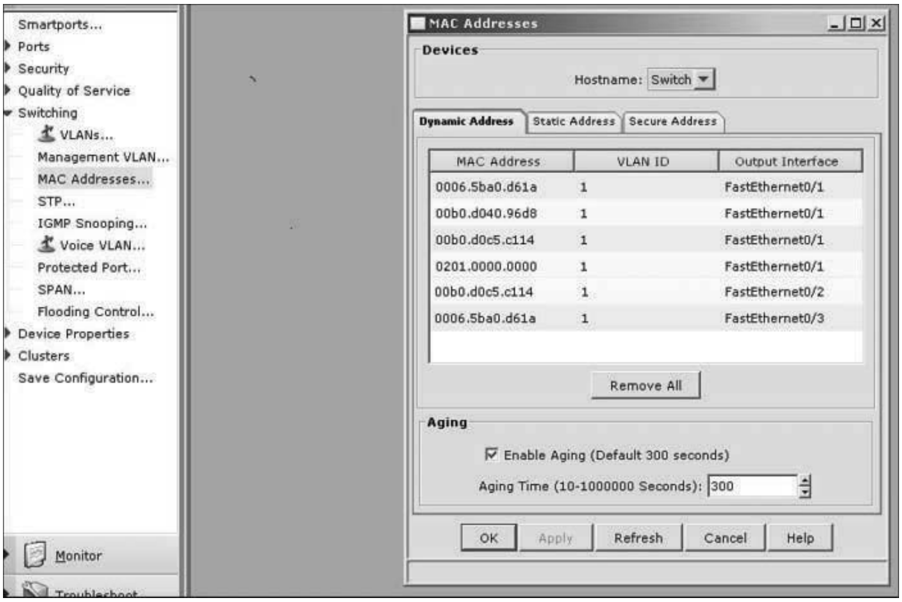


FIGURE 5-11 The menu listing the MAC addresses currently connected to the switch.

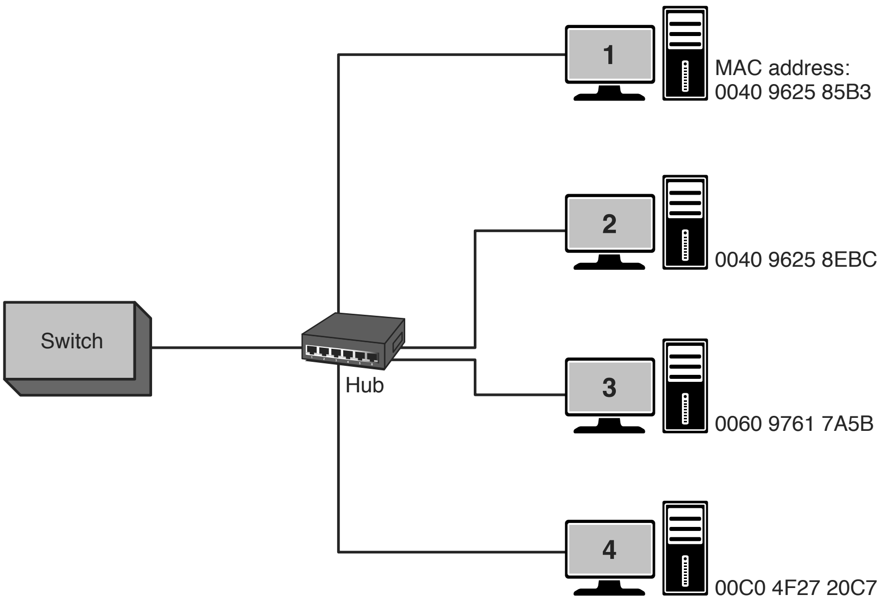


FIGURE 5-12 An example of a hub connected to a switch port, with four computers connected to the hub.

The IP address on a switch interface can be configured using the Cisco Network Assistant software by clicking **Configure > Device Properties > IP Addresses**. This opens the IP Addresses menu shown in Figure 5-13. Click the area where the IP address should be entered. This opens a text box for entering the IP address. Enter the IP address and click **OK** to save the IP address.

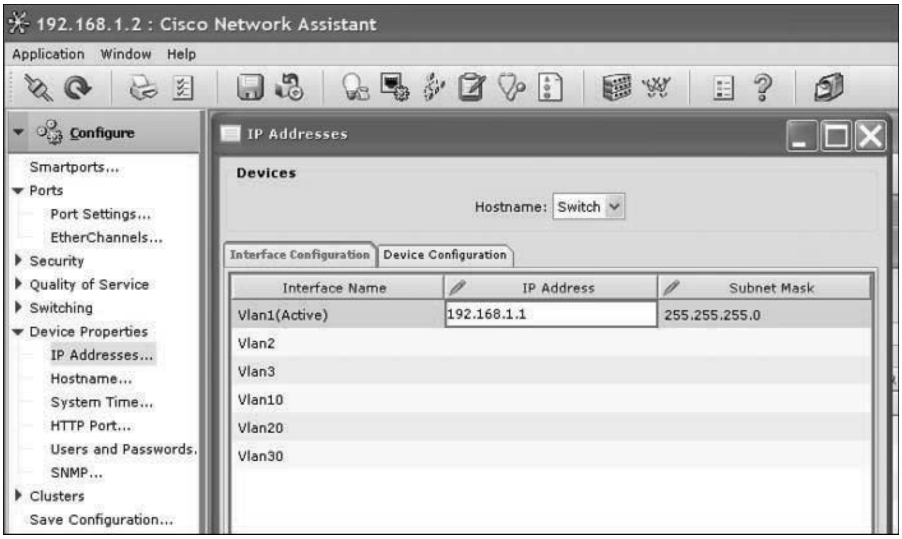


FIGURE 5-13 Configuring an IP address on an interface.

> **Isolating the Collision Domains**
> Breaking the network into segments where a segment is a portion of the network where the data traffic from one part of the network is isolated from the other networking devices

The benefits of using a network switch are many in a modern computer network. These benefits include less network congestion, faster data transfers, and excellent manageability. It has been shown that a network switch can be used to replace the network hub, and the advantage is that data traffic within a LAN is isolated. The term for this is **isolating the collision domains**, which is breaking the network into segments. A segment is a portion of the network where the data traffic from one part of the network is isolated from the other networking devices. A direct benefit of isolating collision domains is that there will be an increase in the data transfer speed and throughput. This is due to the fact that the LAN bandwidth is not being shared and chances of data collisions are minimized. As a result, the LAN will exhibit faster data transfers and latency within the LAN will be significantly reduced. Reduced latency means that the data packets will arrive at the destination more quickly.

> **Content Addressable Memory (CAM)**
> A table of MAC addresses and port mapping used by the switch to identify connected networking devices

Switches learn the MAC addresses of the connected networking by extracting the MAC address information from the headers of Ethernet data packet headers of transmitted data packets. The switch will map the extracted MAC address to the port where the data packet came in. This information is stored in **Content Addressable Memory (CAM)**. CAM is a table of MAC address and port mapping used by the switch to identify connected networking devices. The extracted MAC addresses are then used by the switch to map a direct communication between two network devices connected to its ports. The MAC address and port information remain in CAM as long as the device connected to the switch port remains active. A timestamp establishes the time when the mapping of the MAC address to a switch port is established. However, switches limit the amount of time address and port information are stored in CAM. This is called *aging time*. The mapping information will be deleted from the switch's CAM if there is no activity during this set time. This technique keeps the mapping information stored in CAM up-to-date.

What happens if the destination MAC address is not stored in CAM? In this case, the packet is transmitted out all switch ports except for the port where the packet was received. This is called **flooding**.

It has been shown that switches minimize the collision domain due to the fact that a direct switch connection is made between networking devices. However, it is important to remember that switches do not reduce the broadcast domain. In a **broadcast domain**, any network broadcast sent over the network will be seen by all networking devices in the same network. Broadcasts within a LAN will be passed by switches. Refer to the discussion of Figure 5-7 and 5-8 for an example.

Two modes used in a switch to forward frames: **store-and-forward** and **cut-through**.

- **Store-and-Forward**: In this mode, the entire frame of data is received before any decision is made regarding forwarding the data packet to its destination. There is switch latency in this mode because the destination and source MAC addresses must be extracted from the packet, and the entire packet must be received before it is sent to the destination. The term **switch latency** is the length of time a data packet takes from the time it enters a switch until it exits. An advantage of the store-and-forward mode is that the switch checks the data packet for errors before it is sent on to the destination. A disadvantage is lengthy data packets will take a longer time before they exit the switch and are sent to the destination.
- **Cut-Through**: In this mode, the data packet is forwarded to the destination as soon as the destination MAC address has been read. This minimizes the switch latency; however, no error detection is provided by the switch. There are two forms of cut-through switching—Fast-Forward and Fragment Free.
  - **Fast-Forward**: This mode offers the minimum switch latency. The received data packet is sent to the destination as soon as the destination MAC address is extracted.
  - **Fragment-Free**: In this mode, fragment collisions are filtered out by the switch. Fragment-collisions are collisions that occur within the first 64 bytes of the data packet. Recall from Chapter 1, "Introduction to Computer Networks," Table 1-1 that the minimum Ethernet data packet size is 64 bytes. The collisions create packets smaller than 64 bytes, which are discarded. Latency is measured from the time the first bit is received until it is transmitted.
- **Adaptive Cut-Through**: This is a combination of the store-and-forward mode and cut-through. The cut-through mode is used until an **error threshold** (errors in the data packets) has been exceeded. The switch mode changes from cut-through to store-and-forward after the error threshold has been exceeded.

Flooding
The term used to describe what happens when a switch doesn't have the destination MAC address stored in CAM

Broadcast Domain
Any network broadcast sent over the network will be seen by all networking devices in this domain.

Store-and-Forward
The entire frame of data is received before any decision is made regarding forwarding the data packet to its destination.

Cut-Through
The data packet is forwarded to the destination as soon as the destination MAC address has been read.

Switch Latency
The length of time a data packet takes from the time it enters a switch until it exits

Error Threshold
The point where the number of errors in the data packets has reached a threshold and the switch changes from the cut-through to the store-and-forward mode

Multilayer Switches

Multilayer Switch (MLS)
Operates at layer 2 but functions at the higher layers

Wire Speed Routing
Data packets are processed as quickly as they arrive.

Newer switch technologies are available to help further improve the performance of computer networks. The term used to describe these switches is **multilayer switches (MLS)**. An example is a layer 3 switch. Layer 3 switches still work at layer 2 but additionally work at the network layer (layer 3) of the OSI model and use IP addressing for making decisions to route a data packet in the best direction. The major difference is that the packet switching in basic routers is handled by a programmed microprocessor. The layer 3 switch uses application-specific integrated circuits (ASICs) hardware to handle the packet switching. The advantage of using hardware to handle the packet switching is a significant reduction in processing time (software versus hardware). In fact, the processing time of layer 3 switches can be as fast as the input data rate. This is called **wire speed routing**, where the data packets are processed as fast as they are arriving. Multilayer switches can also work at the upper layers of the OSI model. An example is a layer 4 switch that processes data packets at the transport layer of the OSI model.

Section 5-3 Review

This section has covered the following **Network+** Exam objectives.

1.1 Explain the functions and applications of various network devices

This section introduced the use of the network switch. A discussion on a managed switch was presented incorporating the use of the Cisco Network Assistant. Examples of dynamic MAC address assignment and aging time were also presented.

1.8 Given a scenario, implement and configure the appropriate addressing schema

The concept of multicast messaging where messages are sent to a specific group of hosts on the network was presented in this section.

1.9 Explain the basics of routing concepts and protocols

This section presented a look at latency. A direct benefit of isolating collision domains is that there will be an increase in the data transfer speed and throughput. Reduced latency means that the data packets will arrive at the destination more quickly.

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools

The use of the ping command was demonstrated in this section. This is a very important troubleshooting tool.

Test Your Knowledge

1. A layer 2 switch does which of the following? (Select all that apply.)
   a. Provides a direct connection for networking devices in a LAN
   b. Uses MAC addressing from the Data Link Layer
   c. Uses MAC addressing from the Network Layer
   d. Uses IP addressing from the Network Layer
2. The network administrator wants to verify the network connection at 10.10.20.5. Which of the following commands can be used to verify the connection? (Select all that apply.)
   a. **ping all 10.10.20.5**
   b. **ping 10.10.20.5**
   c. **ping -t 10.10.20.5**
   d. **ping -2 10.10.20.5**
3. A managed switch allows the network administrator to do what? (Select all that apply.)
   a. Monitor network features.
   b. Configure network features.
   c. Manage certain network features.
   d. All of these answers are correct.
   e. None of these answers is correct.

5-4 THE ROUTER

The concept of the use of a router in a computer network is introduced in this section. Router configuration is not introduced until Chapter 6, "TCP/IP," but this section introduces the basic hardware and interfaces available with the router.

The router is the most powerful networking device used today to interconnect LANs. The router is a layer 3 device in the OSI model, which means the router uses the **network address** (layer 3 addressing) to make routing decisions regarding forwarding data packets. Remember from Chapter 1, section 3, that the OSI model separates network responsibilities into different layers. In the OSI model, the layer 3 or network layer responsibilities include handling of the network address. The network address is also called a *logical address,* rather than being a physical address such as the MAC address. The *physical address* is the hardware or MAC address embedded into the network interface card. The **logical address** describes the IP address location of the network and the address location of the host in the network.

Network Address
Another name for the layer 3 address

Logical Address
Describes the IP address location of the network and the address location of the host in the network

Essentially, the router is configured to know how to route data packets entering or exiting the LAN. This differs from the bridge and the layer 2 switch, which use the Ethernet address for making decisions regarding forwarding data packets and only know how to forward data to hosts physically connected to their ports.

Routers are used to interconnect LANs in a campus network. Routers can be used to interconnect networks that use the same protocol (for example, Ethernet), or they can be used to interconnect LANs that are using different layer 2 technologies such as an Ethernet and token ring. Routers also make it possible to interconnect to LANs around the country and the world and interconnect to many different networking protocols.

Router Interface
The physical connection where the router connects to the network

Routers have multiple port connections for connecting to the LANs, and by definition a router must have a minimum of three ports. The common symbol used to represent a router in a networking drawing is provided in Figure 5-14. The arrows pointing in and out indicate that data enters and exits the routers through multiple ports. The router ports are *bidirectional,* meaning that data can enter and exit the same router port. Often the router ports are called the **router interface**, the physical connection where the router connects to the network.

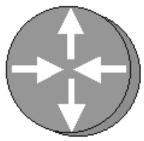


FIGURE 5-14 The network symbol for a router.

The Router Interface: Cisco 2800 Series

Figure 5-15 shows the rear panel view (interface side) of a Cisco 2800 series router.

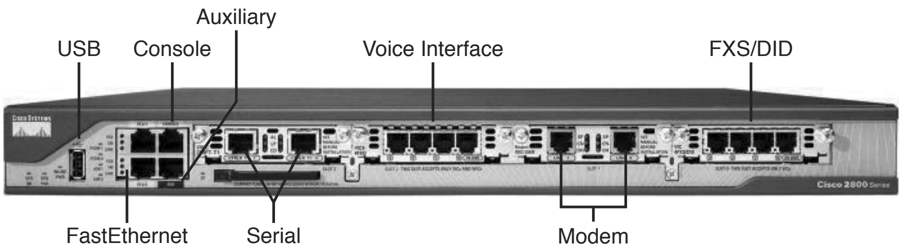


FIGURE 5-15 The rear panel view of a Cisco 2800 series router.

The following describes the function of each interface:

- **USB Interface:** The USB ports are used for storage and security support.
- **FastEthernet Ports:** FE0/0: Fast Ethernet (10/100Mbps) and FE0/1: Fast Ethernet (10/100Mbps).

- **Console Input:** This input provides an RS-232 serial communications link into the router for initial router configuration. A special cable, called a *console cable*, is used to connect the console input to the serial port on a computer. The console cable can have RJ-45 plugs on each end and requires the use of an RJ-45 to DB9 adapter for connecting to the computer's COM1 or COM2 serial port. The console cable can also have an RJ-45 connector on one end and an integrated DB9 connector on the other end.
- **Auxiliary Input:** This input is used to connect a dial-in modem into the router. The auxiliary port provides an alternative way to remotely log in to the router if the network is down. This port also uses an RJ-45 connection.
- **Serial Interface:** CTRLR T1 1 and CTRLR T1 0.

  This is a serial connection, and it has a built-in CSU/DSU. This interface is used to provide a T1 connection to the communications carrier. (*Note:* The CSU/DSU function is presented in Chapter 8, "Introduction to Switch Configuration.") This type of connection (RJ-45) replaces the older cabling using V.35 cable (shown later in Figure 5-18). There are three LEDs on this interface:
  - **AL**—alarm
  - **LP**—loop
  - **CD**—Carrier Detect
- **Voice Interface Card (VIC2-4FXO):** This interface shows four phone line connections. This router can be programmed as a small Private Branch Exchange (PBX) for use in a small office. The PBX function is presented in Chapter 10, "Internet Technologies: Out to the Internet."
- **WAN Interface Card (WIC2AM):** This interface has two RJ-11 jacks and two V.90 analog internal modems. These modems can be used to handle both incoming and outgoing modem calls. This interface is listed as modem in Figure 5-15.
- **VIC-4FXS/DID:** This interface is a four-port FXS and DID voice/fax interface card. FXS is a Foreign Exchange Interface that connects directly to a standard telephone. DID is Direct Inward Dialing and is a feature that enables callers to directly call an extension on a PBX. This interface is listed as FXS/DID in Figure 5-15.

The Router Interface—Cisco 2600 Series

Figure 5-16 shows the rear panel view (interface side) of a Cisco 2600 series router.

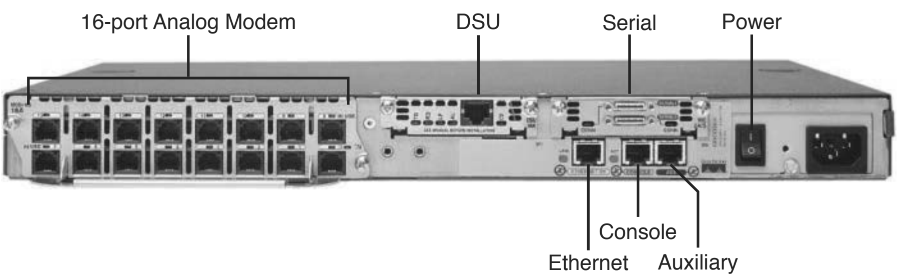


FIGURE 5-16 The rear panel view of a Cisco 2600 series router.

The following describes the function of each interface to the network:

- **Power On/Off:** Turns on/off electrical power to the router.
- **Auxiliary Input:** Used to connect a dial-in modem into the router. The auxiliary port provides an alternative way to remotely log in to the router if the network is down. This port also uses an RJ-45 connection.
- **Console Input:** Provides an RS-232 serial communications link into the router for initial router configuration. A special cable, called a *console cable*, is used to connect the console input to the serial port on a computer. The console cable uses RJ-45 plugs on each end and requires the use of an RJ-45 to DB9 adapter for connecting to the COM1 or COM2 serial port.
- **Serial Ports:** Provides a serial data communication link into and out of the router, using V.35 serial interface cables.
- **DSU Port:** This T1 controller port connection is used to make the serial connection to Telco. This module has a built-in CSU/DSU module. There are five LEDs next to the RJ-45 jack. These LEDs are for the following:
  - **TD**—Transmit Data
  - **P**—Loop
  - **D**—Receive Data
  - **D**—Carrier Detect
  - **L**—Alarm
- **Ethernet Port:** This connection provides a 10/100Mbps Ethernet data link.
- **Analog Modem Ports:** This router has a 16-port analog network module.

Media Converter
Used to adapt a layer 1 (physical layer) technology to another layer 1 technology

A **media converter** is used to convert the 15-pin AUI port to the 8-pin RJ-45 connector. Figure 5-17 shows an example of an AUI to RJ-45 media converter. Media converters are commonly used in computer networks to adapt layer 1 or physical layer technologies from one technology to another. For example:

AUI to twisted pair (RJ-45) AUI to fiber
RJ-45 to fiber

Figure 5-18 shows a Cisco 7200 series router, which provides adaptable interfaces for connecting to many physical layer technologies such as FastEthernet, gigabit Ethernet, ATM, and FDDI.

FIGURE 5-17 A CentreCom 210TS AUI to RJ-45 media converter.

FIGURE 5-18 A Cisco 7200 series router (courtesy of Cisco Systems).

Section 5-4 Review

This section has covered the following **Network+** Exam objectives.

1.1 Explain the functions and applications of various network devices

The network router, a layer 3 device, was presented in this section. The network router is the most powerful networking device used today to interconnect LANs.

1.4 Explain the characteristics and benefits of various WAN technologies

The ATM interface for a network router was presented.

5.2 Explain the basics of network theory and concepts

This section has introduced the carrier detect/sense feature on a router. This feature was present for both Cisco 2800 and 2600 series routers.

Test Your Knowledge

1. A router uses which of the following to make routing decisions regarding forwarding data packets?
    a. Router address
    b. Network address
    c. Fast link pulse
    d. None of these answers is correct.
2. A logical address is which of the following?
    a. MAC address
    b. Router interface address
    c. Network address
    d. The ARP address
3. The physical connection where the router connects to the network is called which of the following?
    a. Console input
    b. Auxiliary input
    c. Router interface
    d. USB interface

5-5 INTERCONNECTING LANS WITH THE ROUTER

This section examines how routers can be used to interconnect LANs. The concept of the gateway, routing tables, and network segments are introduced. Make sure the student understands the terminology and can identify the router hardware. These concepts will be used in Chapters 6, 7, 8, and 9.

The previous section introduced the function of a router in a network. A router routes data based on the destination network address or logical address rather than the physical address used by layer 2 devices, such as the switch and the bridge. Information exchanged with bridges and layer 2 switches requires that the MAC address for the hosts be known. Routed networks such as most enterprise and campus networks use IP addressing for managing the data movement. **Enterprise network** is a term used to describe the network used by a large company. The use of the network or logical address on computers allows the information to be sent from a LAN to a destination without requiring that the computer know the MAC address of the destination computer. Remember, delivery of data packets is based on knowing the MAC address of the destination.

Enterprise Network
Term used to describe the network used by a large company

An overview of the router interface was presented in section 5-4. The router interface provides a way to access the router for configuration either locally or remotely. Interfaces are provided for making serial connections to the router and to other devices that require a serial communications link. For example, interfaces to wide area networking devices require a serial interface. RJ-45 ports are provided on the router interface for connecting the router to a LAN. Older routers can require the use of an AUI port to establish an Ethernet connection to a UTP cable. This port provides a 10Mbps data connection to Ethernet (10Mbps) networks. The RJ-45 connection is used to connect both Ethernet (10Mbps), FastEthernet (100Mbps), Gigabit Ethernet (1000Mbps), and 10 Gigabit Ethernet (10G) to a LAN. The RJ-45 connection can also support gigabit and 10G Ethernet, but high-speed data networks can also use a fiber connection.

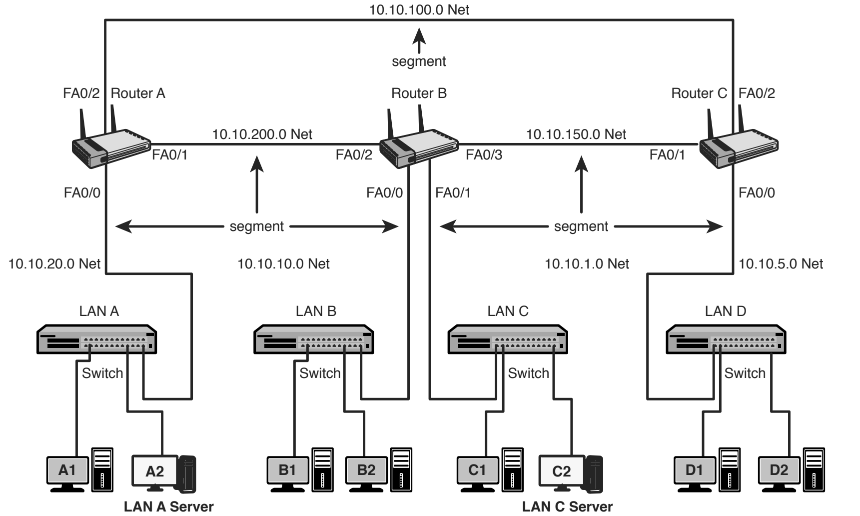
This section introduces the information needed to design, manage, and configure campus networks. An example of a small interconnected LAN is provided in Figure 5-19. This example shows four Ethernet LANs interconnected using three routers. The LANs are configured in a star topology using switches at the center of the LAN. The LANs are labeled LAN A, LAN B, LAN C, and LAN D. The routers are labeled RouterA, RouterB, and RouterC (router naming protocols are discussed in Chapter 7, "Introduction to Router Configuration"). Connection of the routers to the LANs is provided by the router's **FastEthernet port (FA0/0, FA0/1, FA0/2, . . .)**. Look for the FA label in Figure 5-19.

FastEthernet Port (FA0/0, FA0/1, FA0/2,...)
Naming of the FastEthernet ports on the router

The interconnections for the routers and the LANs are summarized as follows:

- **Router A** connects directly to the LAN A switch via FastEthernet port FA0/0. RouterA also connects directly to RouterB via the FastEthernet port FA0/1 and connects to RouterC via FastEthernet port FA0/2.
- **Router B** connects directly to the LAN B switch via FastEthernet port FA0/0. RouterB connects to the LAN C switch via FastEthernet port FA0/1. RouterB connects directly to RouterA via FastEthernet port FA0/2 and connects to RouterC via FastEthernet port FA0/3.

- **Router C** connects directly to the LAN D switch via the FastEthernet port FA0/0. Connection to RouterB is provided via Ethernet port FA0/1. RouterC connects to RouterA via FastEthernet port FA0/2.



Router A Port Addresses (LAN A)		**Router B Port Addresses (LAN B)**		**Router B Port Addresses (LAN C)**		**Router Port Addresses (LAN D)**	
FastEthernet 0/0 (Gateway Address)	10.10.20.250	FastEthernet 0/0 (Gateway Address)	10.10.10.250	FastEthernet 0/1 (Gateway Address)	10.10.1.250	FastEthernet 0/0 (Gateway Address)	10.10.5.250
FastEthernet 0/1	10.10.200.1	FastEthernet 0/2	10.10.200.2	FastEthernet 0/2	10.10.200.2	FastEthernet 0/1	10.10.150.2
FastEthernet 0/2	10.10.100.1	FastEthernet 0/3	10.10.150.1	FastEthernet 0/3	10.10.150.1	FastEthernet 0/2	10.10.100.2
LAN A Computers		**LAN B Computers**		**LAN C Computers**		**LAN D Computers**	
Computer A1	10.10.20.1	Computer A1	10.10.10.1	Computer A1	10.10.1.1	Computer A1	10.10.5.1
Computer A2	10.10.20.2	Computer A2	10.10.10.2	Computer A2	10.10.1.2	Computer A2	10.10.5.2
Subnet Mask	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***

FIGURE 5-19 A small interconnected LAN.

> **Serial Port (S0/0, S0/1, S0/2,...)**
> Naming of the serial ports on the router

The **serial ports (S0/0, S0/1, S0/2,...)** are not being used to interconnect the routers in this sample campus network. The serial interfaces are typically used to interconnect LANs that connect through a data communications carrier such as a telephone company (Telco).

The network configuration provided in Figure 5-19 enables data packets to be sent and received from any host on the network after the routers in the network have been properly configured. For example, computer A1 in LAN A could be sending data to computer D1 in LAN D. This requires that the IP address for computer D1 is known by the user sending the data from computer A1. The data from computer A1 will first travel to the switch where the data is passed to RouterA via the FA0/0 FastEthernet data port. RouterA will examine the network address of the data packet and use configured routing instructions stored in routing tables to decide where to forward the data. RouterA determines that an available path to RouterC is via the FA0/2 FastEthernet port connection. The data is then sent directly to RouterC. RouterC determines that the data packet should be forwarded to the FA0/0 port to reach computer D1 in LAN D. The data is then sent to D1. Alternatively, RouterA could have sent the data to RouterC through RouterB via Router A's FA0/1

FastEthernet port. Path selection for data packets is examined in Chapter 9, "Routing Protocols."

Delivery of the information over the network was made possible by the use of an IP address and **routing tables**. Routing tables keep track of the routes used for forwarding data to its destination. RouterA used its routing table to determine a network data path so computer A1's data could reach computer D1 in LAN D. RouterA determines that a path to the network where computer D1 is located can be obtained via RouterA's FA0/2 FastEthernet port to the FA0/2 FastEthernet port on RouterC. RouterC determines that computer D1 is on LAN D, which connects to RouterC's FA0/0 FastEthernet port. An ARP request is issued by RouterC to determine the MAC address of computer D1. The MAC address is then used for final delivery of the data to computer D1.

Routing Table
Keeps track of the routes to use for forwarding data to its destination

If RouterA determines that the network path to RouterC is down, RouterA can route the data packet to RouterC through RouterB. After RouterB receives the data packet from RouterA, it uses its routing tables to determine where to forward the data packet. RouterB determines that the data needs to be sent to RouterC, and it uses the FA0/3 FastEthernet port to forward the data.

Gateway Address

The term **gateway** is used to describe the address of the networking device that enables the hosts in a LAN to connect to networks and hosts outside the LAN. For example, for all hosts in LAN A, the gateway address will be 10.10.10.250. This address is configured on the host computer. Any IP packets with a destination outside the LAN will be sent to the gateway address.

Gateway
Describes the networking device that enables hosts in a LAN to connect to networks (and hosts) outside the LAN

Network Segments

The *network segment* defines the networking link between two LANs. There is a segment associated with each connection of an internetworking device (for example, router—hub, router—switch, router—router). For example, the IP address for the network segment connecting LAN A to the router is 10.10.20.0. All hosts connected to this segment must contain a 10.10.20.x because a subnet mask of 255.255.255.0 is being used. Subnet masking is fully explained in Chapter 6.

Routers use the information about the network segments to determine where to forward data packets. For example, the network segments that connect to RouterA include

10.10.20.0
10.10.200.0
10.10.100.0

The computers in LAN A will have a 10.10.20.x address. All the computers in this network must contain a 10.10.20.x IP address. For example, computer A1 in LAN A will have the assigned IP address of 10.10.20.1 and a gateway address of 10.10.20.250. The computers in LAN B are located in the 10.10.10.0 network. This means that all the computers in this network must contain a 10.10.10.x IP address. The *x* part of the IP address is assigned for each host. The gateway address for the hosts in LAN B is 10.10.10.250.

Section 5-5 Review

This section has covered the following **Network+** Exam objectives.

1.9 Explain the basics of routing concepts and protocols

The concept of routing tables was presented in this section. It is important to remember that the purpose of the routing table is to keep track of the routes used to forward data to its destination.

4.6 Given a scenario, troubleshoot and resolve common network issues

This section introduced the gateway address, which enables the host in a LAN to connect to hosts outside the LAN.

Test Your Knowledge

1. The router's routing tables do which of the following? (Select all that apply.)
   a. Keep track of the routes to forward data to its destination
   b. Keep track of the IP addresses to forward data to its destination
   c. Keep track of the MAC addresses to forward data to its destination
   d. None of these answers is correct.
2. The term Enterprise Network is used to describe the network used by a large company. True or False?
3. A gateway address defines which of the following?
   a. The networking links between two LANs
   b. The networking device that enables hosts in a LAN to connect to networks outside the LAN
   c. The networking device that enables hosts in a LAN to connect to networks inside the LAN
   d. All of these answers are correct

5-6 CONFIGURING THE NETWORK INTERFACE—AUTO-NEGOTIATION

This chapter has introduced how LANs are interconnected. And this section examines how interconnected networking devices negotiate an operating speed. The steps for negotiation and the concept of full- and half-duplex are all examined. A summary of the advantages and disadvantages of the auto-negotiation protocol are examined. Make sure the student understands that auto-negotiation is not for every network application.

Most modern networking internetworking technologies (for example, hubs, switches, bridges, and routers) now incorporate the **auto-negotiation** protocol. The protocol enables the Ethernet equipment to automate many of the installation steps. This includes automatically configuring the operating speeds (for example, 10/100/1000Mbps) and the selection of full- or half-duplex operation for the data link. The auto-negotiation protocol is defined in the IEEE Ethernet standard 802.3x for FastEthernet.

Auto-negotiation
Protocol used by interconnected electronic devices to negotiate a link speed

The auto-negotiation protocol uses a **fast link pulse (FLP)** to carry the information between each end of a data link. Figure 5-20 shows a data link. The data rate for the fast link pulses is 10Mbps, the same as for 10BASE-T. The link pulses were designed to operate over the limited bandwidth supported by CAT3 cabling. Therefore, even if a link is negotiated, there is no guarantee that the negotiated data rate will work over the link. Other tests on the cable link must be used to certify that the cable can carry the negotiated data link configuration (refer to Chapter 2, "Physical Layer Cabling: Twisted Pair").

Fast Link Pulse (FLP)
Carries the configuration information between each end of a data link

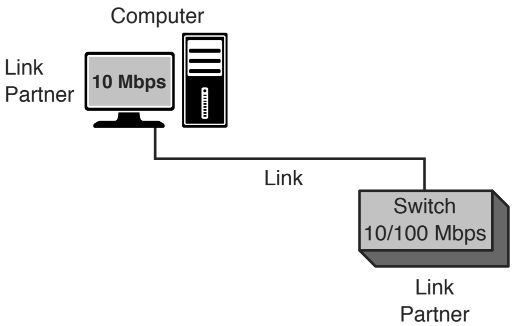


FIGURE 5-20 The two ends of a data link negotiating the operating parameters.

Auto-Negotiation Steps

Each link partner shares or advertises its data link capabilities with the other link partner. The two link partners then use the advertised capabilities to establish the fastest possible data link rate for both links. In the example of the link partners shown in Figure 5-22, computer 1 advertises that its interface supports 10Mbps. The switch advertises that it supports both 10Mbps and 100Mbps. The network interfaces on each link partner are set for auto-negotiation; therefore, the 10Mbps operating mode is selected. This is the fastest data rate that can be used in this data link. The data rate is limited by the 10Mbps capabilities of the computer's network interface.

Note

Auto-negotiation is established when an Ethernet link is established. The link information is only sent one time, when the link is established. The negotiated link configuration will remain until the link is broken or the interfaces are reconfigured.

Full-Duplex/Half-Duplex

> **Half-Duplex**
> The communications device can transmit or receive, but not at the same time

Modern network interfaces for computer networks have the capability of running the data over the links in either full- or half-duplex mode. As noted previously, *full-duplex* means that the communications device can transmit and receive at the same time. **Half-duplex** means the communications device can transmit or receive, but not at the same time.

In full-duplex operation (10/100Mbps), the media must have separate transmit and receive data paths. This is provided for in CAT6/5e/5 cable with pairs 1–2 (transmit) and pairs 3–6 (receive). Full-duplex with gigabit and 10 gigabit data rates require the use of all four wire pairs (1–2, 3–6, 4–5, 7–8). An important note is that the full-duplex mode in computer network links is only for point-to-point links. This means that there can only be two end stations on the link. The CSMA/CD protocol is turned off; therefore, there can't be another networking device competing for use of the link. An example of networking devices that can run full-duplex are computers connected to a switch. The switch can be configured to run the full-duplex mode. This also requires that each end station on the link must be configurable to run full-duplex mode.

In half-duplex operation, the link uses the CSMA/CD protocol. This means only one device talks at a time, and while the one device is talking, the other networking devices "listen" to the network traffic. Figure 5-21(a) and (b) shows examples of networks configured for full- and half-duplex mode. In full-duplex operation [Figure 5-21(a)], CSMA/CD is turned off and computers 1, 2, and the switch are transmitting and receiving at the same time. In half-duplex mode [Figure 5-21(b)], CSMA/CD is turned on, computer 1 is transmitting, and computer 2 is "listening" or receiving the data transmission.

Figure 5-22(a) and (b) provides an example of the port management features available with the Cisco switch using the Cisco Network Administrator software. The settings for the speed are shown in Figure 5-22(a). An example of setting the switch for auto, half-, and full-duplex are shown in Figure 5-22(b). The auto setting is for auto-negotiate.

Table 5-4 provides a summary of the advantages and disadvantages of the auto-negotiation protocol.

TABLE 5-4 **Summary of the Auto-negotiation Protocol**

Advantages	Disadvantages
Useful in LANs that have multiple users with multiple connection capabilities.	Not recommended for fixed data links such as the backbone in a network.
The auto-negotiation feature can maximize the data links' throughput.	A failed negotiation on a functioning link can cause a link failure.

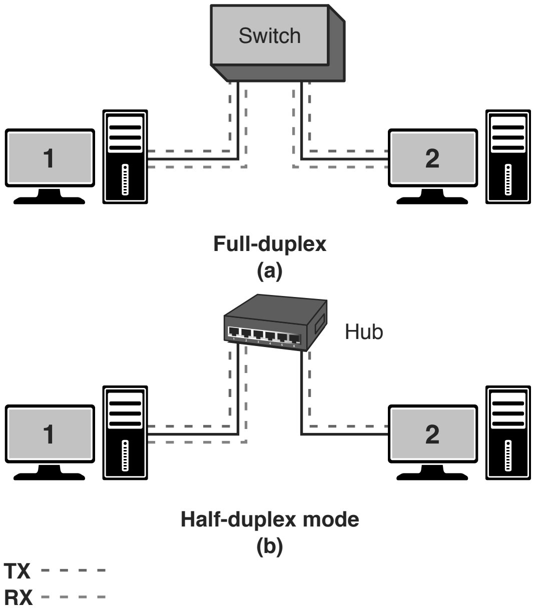


FIGURE 5-21 (a) Computer 1 transmits and receives at the same time; (b) computer 1 transmits; others listen.

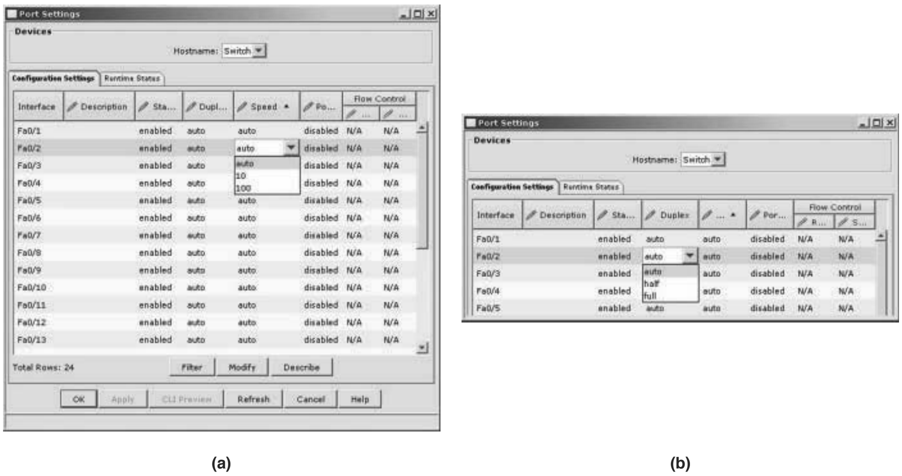


FIGURE 5-22 An example of the port management options available with a Cisco switch: (a) 100Mbps auto-negotiation; (b) 10Mbps half-/full-duplex option.

Section 5-6 Review

This section has covered the following **Network+** Exam objectives.

5.2 Explain the basics of network theory and concepts

The changes in the CSMA/CD protocol when configuring switch ports for operation in the half- and full-duplex mode was presented.

Test Your Knowledge

1. Which of the following is a disadvantage of the auto-negotiation protocol?
    a. It is only useful in LANs that have multiple connection capabilities.
    b. A failed negotiation on a functioning link can cause a link failure.
    c. It should be used only in critical network data paths.
    d. It works at 10Mbps.
2. The fast link pulse does which of the following? (Select all that apply.)
    a. Carries the configuration information between each end of a data link
    b. Is used in auto-negotiation
    c. Uses a 100Mbps data rate
    d. Uses a 1Mbps data rate
3. Which of the following is an advantage of auto-negotiation? (Select all that apply.)
    a. Is useful in LANs that have multiple users with multiple connection capabilities
    b. Can maximize the data link throughput
    c. Simplifies the backbone configuration
    d. Simplifies the LAN configuration
    e. All of the answers are correct.

SUMMARY

This chapter has established how LANs are interconnected. The need for careful documentation was addressed in this chapter. The importance of this will become more relevant as the complexity in network topics increases from chapter to chapter. Internetworking hardware such as bridges, switches, and routers were discussed and examples of using these technologies presented.

A technique for internetworking the LANs using routers has been presented. In addition, the purpose of a router and its hardware interface has been defined. The use of switches and hubs to connect to the routers has been demonstrated. The purpose of a gateway has been explained and demonstrated. The concept of a network segment has been examined.

The concepts the student should understand from this chapter are the following:

- How bridges are used to interconnect separate LANs
- How a switch is used in a network and why the switch improves network performance
- Understand and be able to identify the various connections on a the router interface
- How a router is used to interconnect LANs
- The purpose of a gateway in a computer network
- The concept of a network segment
- The concept of auto-negotiation

QUESTIONS AND PROBLEMS

Section 5-2

1. What is a *bridge*?

   A layer 2 device used to interconnect two LANs

2. Define a *segment.*

   Section of a network separated by bridges, switches, and routers

3. What information is stored in a bridge table?

   The MAC address and port locations for hosts connected to the bridge ports

4. What is an *association* on a bridge, and how is it used?

   Association indicates that the destination address is for one of the networking devices connected to one of its ports. If an association is detected, the data packet is forwarded to the port.

5. What are excessive amounts of broadcasts on a network called?

   Broadcast storm

6. Which command is used on a computer to view the contents of the ARP cache?

   arp -a

7. An empty ARP cache indicates what?

   All of the ARP entries have expired.

8. Why do entries into the bridging table have a limited lifetime?

   Each MAC address entry into the bridging table remains active as long as there is periodic data traffic activity. The entries expire so that the table only lists the MAC address for the networking devices recently active in the network.

9. Which of the following are advantages of using a bridge to interconnect LANs?

   a. Works best in low traffic areas

   b. Relatively inexpensive

   c. Can be used to route data traffic

   d. Easy to install

   e. Reduces collision domains

Section 5-3

10. The network switch operates at which layer of the OSI model?

    Layer 2: Data Link

11. Another name for a switch is

    a. multiport repeater

    b. multiport bridge

    c. multiport router

    d. multiport hub

12. How does a switch provide a link with minimal collisions?

    Only the two computers or networking devices that established the link will be communicating on the channel.

13. The link for a switch connection is isolated from other data traffic except for what type of messages?

    Broadcast and multicast

14. Explain what data traffic is sent across a network when a computer pings another computer and a hub is used to interconnect the computers.

    Line 1 ARP request

    Line 2 ARP reply

    Line 3 Echo request/Echo reply (repeats 4 times)

    …

    …

    Line 10

15. Explain what data traffic is seen by computer 3 when computer 1 pings computer 2 in a LAN. A switch is used to interconnect the computers.

    Line 1 ARP request

16. Explain the concept of *dynamic assignment* on a switch.

    The MAC address was assigned to a port when the device was connected.

17. Define *aging time* on a switch.

    The length of the time a MAC address remains assigned to a port

18. Explain how a switch learns MAC addresses, and where a switch stores the address.

    Switches learn the MAC addresses of the connected networking by extracting the MAC address information from the headers of Ethernet data packet headers of transmitted data packets. The switch will map the extracted MAC address to the port where the data packet came in. This information is stored in Content Addressable Memory (CAM).

19. What happens if a MAC address is not stored in CAM on a switch?

    The packet is transmitted out all switch ports except for the port where the packet was received. This is called flooding.

20. Which two modes are used by a switch to forward frames?

    Store-and-forward and cut-through

21. Which switch mode offers minimum latency?

    Fast-Forward: This mode offers the minimum switch latency. The received data packet is sent to the destination as soon as the destination MAC address is extracted.

22. What is error threshold, and which mode is it associated with?

    Cut-through mode is used until an error-threshold (errors in the data packets) has been exceeded. The switch mode changes from cut-through to store-and-forward after the error threshold has been exceeded.

23. Explain the difference in store-and-forward and the cut-through mode on a switch.

    In store-and-forward mode, the entire frame of data is received before any decision is made regarding forwarding the data packet to its destination. An advantage of the store-and-forward mode is that the switch checks the data packet for errors before it is sent on to the destination. A disadvantage is that lengthy data packets will take a longer time before they exit the switch and are sent to the destination.

    In cut-through mode, the data packet is forwarded to the destination as soon as the destination MAC address has been read. This minimizes the switch latency; however, no error detection is provided by the switch.

24. How does a layer 3 switch differ from a layer 2 switch?

    Layer 3 switches still work at layer 2 but additionally work at the network layer (layer 3) of the OSI model and use IP addressing for making decisions to route a data packet in the best direction. The major difference is that the packet switching in basic routers is handled by a programmed microprocessor. The layer 3 switch uses application-specific integrated circuits (ASICs) hardware to handle the packet switching. The advantage of using hardware to handle the packet switching is a significant reduction in processing time (software versus hardware).

25. What is meant by the term *wire-speed routing*?

    The data packets are processed as quickly as they arrive.

Section 5-4

26. A router uses the network address on a data packet for what purpose?

    To make routing decisions about to which router interface to forward the data.

27. What is the *logical address*?

    Describes the IP address location of the network and the address location of the host in the network.

28. The physical connection where a router connects to the network is called the

    a. router port
    b. network port
    c. network interface
    d. router interface

29. The connection to the router's console input is typically which of the following?

    a. RS-232
    b. RJ-45
    c. DB9
    d. RJ-11

30. AUI stands for

    a. Auxiliary Unit Input
    b. Attachment Unit Interconnect
    c. Auxiliary Unit Interface
    d. Attachment Unit Interface

31. The AUI port on a router connects to which networking protocol?

    a. 100BASE-T
    b. 10BASE-T
    c. Token Ring
    d. Ethernet

Section 5-5

32. Define enterprise network.

    A term used to describe the network used by a large company.

33. The router interface most commonly used to interconnect LANs in a campus network is

    a. serial
    b. console port
    c. Ethernet
    d. ATM

34. Serial interfaces on a router are typically used to

    a. interconnect routers
    b. interconnect hubs
    c. connect to communication carriers
    d. connect to auxiliary ports

35. The designation E0 indicates

    a. Ethernet port 0
    b. Ethernet input
    c. External port 0
    d. Exit port 0

36. Routing tables on a router keep track of

    a. port assignments
    b. MAC address assignments
    c. gateway addresses of LANs
    d. routes to use for forwarding data to its destination

37. The convention used for naming of the serial port 0 on a router is
    a. S0
    b. System 0
    c. Serial interface 0
    d. Serial AUI 0
38. Define the term *gateway*.

    Gateway is a term used to describe the networking device that enables hosts in a LAN to connect to networks and hosts outside the LAN.

Section 5-6

39. What is the purpose of the fast link pulse?

    It carries the configuration information between each end of a data link.
40. Define *full-duplex*.

    The communications device can transmit and receive at the same time.
41. Define *half-duplex*.

    The communication device can transmit and receive, but not at the same time.
42. Which of the following is a disadvantage of the auto-negotiation protocol?
    a. Only useful in LANs that have multiple connection capabilities.
    b. A failed negotiation on a functioning link can cause a link failure.
    c. It's recommended for use in critical network data paths.
    d. It works at 10Mbps.

CRITICAL THINKING

43. Describe how a network administrator uses the OSI model to isolate a network problem.

    The answer should discuss how the network administrator looks for problems at different layers using the **ping** command, telnet, and so on. This concept was discussed in section 5-3.
44. Why is auto-negotiation not recommended for use in critical network data paths?

    The data speeds should be fixed for critical data paths. You don't want to take the chance of the networking equipment negotiating a slower speed.
45. What would happen if the local network devices do not have local ARP cache?

    The broadcast will increase dramatically depending on the size of the network. Broadcast leads to network degradation. Also, every network device will have to process more broadcast messages and that takes up CPU process.

CERTIFICATION QUESTIONS

46. Which of the following best defines a *bridging table*?
    a. A list of MAC addresses and port locations for hosts connected to the bridge ports
    b. A list of IP addresses and port locations for hosts connected to the bridge ports
    c. A list of IP addresses and port locations for hosts connected to the hub ports
    d. A list of MAC addresses and port locations for hosts connected to the hub ports
47. Which of the following best defines *aging time*?
    a. The length of time a MAC address remains assigned to a port
    b. The length of time an IP address remains assigned to a port
    c. The length of time a MAC address remains assigned to a hub
    d. The length of time an IP address remains assigned to a hub
48. Dynamic assignment on a switch implies which of the following? (Select all that apply.)
    a. MAC addresses are assigned to a port when a host is connected.
    b. IP addresses are assigned to a port when a host is connected.
    c. MAC addresses are assigned to a switch when a host is connected.
    d. IP addresses are assigned to a switch when a host is connected.
49. Which of the following terms is used to describe that a MAC address has been manually assigned?
    a. Dynamic assignment
    b. ARP assignment
    c. DHCP assignment
    d. Static assignment
50. What is the purpose of the secure tab on a switch?
    a. The switchport will use port discovery to assign a MAC address to the port.
    b. The switchport will automatically disable itself if a device with a different MAC address connects to the port.
    c. The switchport will use a different MAC address than the one connected to the port.
    d. This enables the switch to select what networking devices have a selectable IP address.

51. What is the length of time an IP address is assigned to a switchport called?
    a. Delay time
    b. Enable time
    c. Aging time
    d. Access time
52. Which of the following is a table of MAC addresses and port mapping used by the switch to identify connected network devices?
    a. CAM
    b. ARP
    c. ARP-A
    d. ipconfig /all
53. Which of the following best defines store-and-forward relative to switch operation?
    a. The frame is stored in CAM and the forward to the source for confirmation.
    b. The frame is stored in CAM and the forward to the destination for confirmation.
    c. The header is received before forwarding it to the destination.
    d. The entire frame is received before a decision is made regarding forwarding to its destination.
54. In which switch mode is the data packet forwarded to the destination as soon as the MAC address has been read?
    a. Store-and-forward
    b. Adaptive fast-forward
    c. Cut-through
    d. Fast-forward
55. Which switch mode offers the minimum switch latency?
    a. Cut-through
    b. Fast-forward
    c. Store-and-forward
    d. Adaptive cut-through

This page intentionally left blank

INDEX

Numbers

A

B

C

D

E

F

G

H

I

J-L

M

N

O

P

Q-R

S

T

U

V

W

X

Y-Z