Introducing Routing and Switching in the Enterprise

CCNA Discovery Learning Guide

Allan Reid • Jim Lorenz • Cheryl Schmidt

Cisco | Networking Academy
Mind Wide Open

Introducing Routing and Switching in the Enterprise

CCNA Discovery Learning Guide

Part I: Concepts

Allan Reid

Jim Lorenz

Cheryl Schmidt

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Introducing Routing and Switching in the Enterprise

CCNA Discovery Learning Guide
Part I: Concepts

Allan Reid ▪ Jim Lorenz ▪ Cheryl Schmidt

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

Printed in the United States of America

Third Printing: November 2011

Library of Congress Cataloging-in-Publication Data:
Library of Congress Cataloging-in-Publication Data
Reid, Allan.
Introducing routing and switching in the enterprise / Allan Reid, Jim Lorenz, Cheryl Schmidt.
p. cm. -- (CCNA discovery learning guide)
Includes index.
ISBN-13: 978-1-58713-211-7 (pbk. w/cd)
ISBN-10: 1-58713-211-7
1. Routing (Computer network management) 2. Packet switching (Data transmission) I. Lorenz, Jim. II. Schmidt, Cheryl A., III. Cisco Systems, Inc. IV. Title. V. Series.
TK5105.543.R45 2008

004.6--dc22

2008010656

ISBN-13: 978-1-58713-211-7
ISBN-10: 1-58713-211-7

This book is part of a two-book set. Not to be sold separately.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Executive Editor
Mary Beth Ray

Managing Editor
Patrick Kanouse

Development Editor
Dayna Isley

Project Editor
Jennifer Gallant

Copy Editors
Keith Cline
Written Elegance, Inc.

Technical Editors
Tony Chen
Tom Knott
Fred Lance
Michael Duane Taylor
Tara Skibar
Marlon Vernon

Editorial Assistant
Vanessa Evans

Book and Cover Designer
Louisa Adair

Composition
Bronkella Publishing

Indexer
Heather McNeill

Proofreaders
Karen A. Gill
Leslie Joseph

Warning and Disclaimer

This book is designed to provide information about the Introducing Routing and Switching in the Enterprise CCNA Discovery course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

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

Feedback Information

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

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

We greatly appreciate your assistance.

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

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

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

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

About the Authors

Allan Reid is the curriculum lead and a CCNA/CCNP instructor at the Centennial College CATC in Toronto, Canada. Allan is a professor in the Information and Communications Engineering Technology department and an instructor and program supervisor for the School of Continuing Education at Centennial College. He has developed and taught networking courses for both private and public organizations and has been instrumental in the development and implementation of numerous certificate, diploma, and degree programs in networking. Allan is also a curriculum developer for the Cisco Networking Academy. Outside of his academic responsibilities, he has been active in the computer and networking fields for more than 25 years and is currently a principal in a company specializing in the design, management, and security of network solutions for small and medium-sized companies. Allan authored the first edition of *WAN Technologies CCNA 4 Companion Guide* (Cisco Press, ISBN: 1-58713-172-2) and *Using a Networker's Journal*, which is a supplement to *A Networker's Journal* (Cisco Press, ISBN: 1-58713-158-7). Most recently, Allan coauthored the CCNA Discovery online academy courses Networking for Home and Small Businesses and Introducing Routing and Switching in the Enterprise, with Jim Lorenz.

Jim Lorenz is an instructor and curriculum developer for the Cisco Networking Academy. Jim has coauthored several Cisco Press titles, including *Fundamentals of UNIX Companion Guide*, Second Edition (ISBN 1-58713-140-4), *Fundamentals of UNIX Lab Companion*, Second Edition (ISBN 1-58713-139-0), and the third editions of the CCNA Lab Companions. He has more than 20 years of experience in information systems, ranging from programming and database administration to network design and project management. Jim has developed and taught computer and networking courses for numerous public and private institutions. As the Cisco Academy Manager at Chandler-Gilbert Community College in Arizona, he was instrumental in starting the Information Technology Institute (ITI) and developed a number of certificates and degree programs. Most recently, Jim coauthored the CCNA Discovery online academy courses Networking for Home and Small Businesses and Introducing Routing and Switching in the Enterprise, with Allan Reid.

Cheryl Schmidt is a professor of network engineering technology at Florida Community College in Jacksonville, Florida, where she has worked for the past 19 years (13 years as a faculty member). Before joining the classroom full time, Cheryl worked in the computer/networking industry, having begun her career in electronics/computers in the U.S. Navy. Cheryl has been active in the Cisco Academy, through which she has taught CCNA, CCNP, wireless, and security classes and has been instrumental in the development and implementation of a converged networking program including VoIP and QoS classes.

About the Technical Reviewers

Tony Chen, CCNP and CCAI, manages Cisco Networking Academy for the College of DuPage in Glen Ellyn, Illinois, and teaches CCNA and CCNP classes at the college. As a manager for a regional academy, he also trains and supports local Cisco networking academies. He also manages the computer network for the Ball Foundation. The Ball Foundation's motto is to discover and develop human potential. Tony Chen has an understanding wife, Joanne, and one wonderful daughter, Kylie.

Tom Knott is the technology and communications specialist for the Kenan Institute for Engineering, Technology & Science at North Carolina State University. In that capacity, he works as tech support, manages websites, writes program content, and serves as staff photographer. Mr. Knott was a public school teacher for the previous 17 years, the last 10 teaching Cisco Academy courses at Southeast Raleigh High School, a magnet high school. He is also an author for Cisco Press and has worked on numerous curriculum projects for the Cisco Networking Academy.

Fred Lance teaches CCNA, CCNP, and security classes at NHTI in Concord, New Hampshire. After 15 years working in the networking field, he joined the IT faculty of NHTI in 1999 to implement the Cisco Networking Academy for the college. He received both his CCNA and CCNP certifications after moving into the teaching field. He resides in Andover, New Hampshire, with his wife Brenda and their three daughters, Abigail, Becca, and Emily. He has been a volunteer firefighter in Andover for 18 years and enjoys building and painting in his spare time.

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

Marlon Vernon currently teaches the CCNA and CCNP networking courses. He has been teaching for 23 years in the fields of electronics engineering and computer networking technologies both at the high school and college levels. He has served on the Cisco Advisory Council for the global networking academies for the past four years.

Michael Duane Taylor is department head of computer information sciences at the Raleigh Campus of ECPI College of Technology. He has more than seven years of experience teaching introductory networking and CCNA-level curriculum and was awarded the Instructor of the Year Award. Previously, Michael was a lab supervisor with Global Knowledge, working with router hardware configuration and repair. He holds a bachelor's degree in business administration from the University of North Carolina at Chapel Hill and a master of science degree in industrial technology/computer network management from East Carolina University. His certifications include CCNA, CCNP-router, and MCSE.

Dedications

This book is dedicated to my children: Andrew, Philip, Amanda, Christopher, and Shaun. You are my inspiration, and you make it all worthwhile. Thank you for your patience and support.

—Allan Reid

To the three most important people in my life: my wife, Mary, and my daughters, Jessica and Natasha. Thanks for your patience and support.

—Jim Lorenz

In addition to my thankfulness for the production team and my family (my husband, Karl, and my daughters, Raina and Kara), I would like to thank my students and coworkers for their continued support in my projects, classes, and ideas. It truly takes a team to have success.

—Cheryl Schmidt

Acknowledgments

From Allan, Jim, and Cheryl:

We want to thank Mary Beth Ray and Dayna Isley with Cisco Press for their help and guidance in putting this book together. We also want to thank the technical editors: Tony Chen, Tom Knott, Fred Lance, Tara Skibar, Mike Taylor, and Marlon Vernon. Their attention to detail and suggestions made a significant contribution to the accuracy and clarity of the content.

We also want to acknowledge the entire CCNA Discovery development team from Cisco Systems for their hard work and dedication to making CCNA Discovery a reality.

Contents at a Glance

Contents

Part II: Labs

Icons Used in This Book

Command Syntax Conventions

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

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

Introduction

Cisco Networking Academy is a comprehensive e-learning program that delivers information technology skills to students around the world. The Cisco CCNA Discovery curriculum consists of four courses that provide a comprehensive overview of networking, from fundamentals to advanced applications and services. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses and in enterprise and Internet service provider environments. The Introducing Routing and Switching in the Enterprise course is the third course in the curriculum.

Introducing Routing and Switching in the Enterprise, CCNA Discovery Learning Guide is the official supplemental textbook for the third course in v4.*x* of the CCNA Discovery online curriculum of the Networking Academy. As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. In addition, it contains all the interactive activities, Packet Tracer activities, and hands-on labs from the online curriculum and bonus labs.

This book emphasizes key topics, terms, and activities and provides many alternative explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then also use this *Learning Guide*'s study tools to help solidify your understanding of all the topics. In addition, the book includes the following:

- Expanded coverage of CCNA exam material
- Additional key Glossary terms
- Bonus labs
- Additional Check Your Understanding and Challenge questions and activities
- Interactive activities and Packet Tracer activities on the CD-ROM

Goal of This Book

First and foremost, by providing a fresh, complementary perspective of the online content, this book helps you learn all the required materials of the third course in the Networking Academy CCNA Discovery curriculum. As a secondary goal, individuals who do not always have Internet access can use this text as a mobile replacement for the online curriculum. In those cases, you can read the appropriate sections of this book, as directed by your instructor, and learn the topics that appear in the online curriculum. Another secondary goal of this book is to serve as your offline study material to help prepare you for the CCNA exams.

Audience for This Book

This book's main audience is anyone taking the third CCNA Discovery course of the Networking Academy curriculum. Many Networking Academies use this textbook as a required tool in the course, whereas other Networking Academies recommend the learning guides as an additional source of study and practice materials.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives**: Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Learning Guide* encourages you to think about finding the answers as you read the chapter.

- **"How-to" feature**: When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes, tips, cautions, and warnings**: These short sidebars point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries**: At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.

Readability

The authors have compiled, edited, and in some cases rewritten the material so that it has a more conversational tone that follows a consistent and accessible reading level. In addition, the following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms**: Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary**: This book contains an all-new Glossary with more than 300 computer and networking terms.

Practice

Practice makes perfect. This new *Learning Guide* offers you ample opportunities to put what you learn to practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key**: Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Check Your Understanding and Challenge Questions Answer Key," provides an answer key to all the questions and includes an explanation of each answer.
- **(*New*) Challenge questions and activities**: Additional, and more challenging, review questions and activities are presented at the end of chapters. These questions are purposefully designed to be similar to the more complex styles of questions you might see on the CCNA exam. This section might also include activities to help prepare you for the exams. Appendix A provides the answers.

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

- **Interactive activities**: These activities provide an interactive learning experience to reinforce the material presented in the chapter.

- **Labs**: Part II of this book contains all the hands-on labs from the curriculum plus additional labs for further practice. Part I includes references to the hands-on labs, as denoted by the lab icon, and Part II of the book contains each lab in full. You may perform each lab when it is referenced in the chapter or wait until you have completed the entire chapter.

A Word About Packet Tracer Software and Activities

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

Packet Tracer v4.*x* is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

A Word About the Discovery Server CD

The CCNA Discovery series of courses is designed to provide a hands-on learning approach to networking. Many of the CCNA Discovery labs are based on Internet services. Because it is not always possible to allow students access to these services on a live network, the Discovery Server has been developed to provide them.

The Discovery Server CD is a bootable CD that transforms a regular PC into a Linux server running several preconfigured services for use with Discovery labs. Your instructor can download the CD files, burn a CD, and show you how to use the server. Hands-on labs that use the Discovery Server are identified within the labs themselves.

Once booted, the server provides many services to clients, including the following:

- Domain Name Services
- Web services
- FTP
- TFTP
- Telnet

- SSH
- DHCP
- Streaming video

How This Book Is Organized

This book covers the major topics in the same sequence as the online curriculum for the CCNA Discovery Introducing Routing and Switching in the Enterprise course. The online curriculum has ten chapters for this course, so this book has ten chapters, with the same names and numbers as the online course chapters.

To make it easier to use this book as a companion to the course, the major topic headings in each chapter match, with just a few exceptions, the major sections of the online course chapters. However, the *Learning Guide* presents many topics in slightly different order inside each major heading. In addition, the book occasionally uses different examples than the course. As a result, students get more detailed explanations, a second set of examples, and different sequences of individual topics, all to aid the learning process. This new design, based on research into the needs of the Networking Academies, helps typical students lock in their understanding of all the course topics.

Chapters and Topics

Part I of this book has ten chapters, as follows:

- **Chapter 1, "Networking in the Enterprise,"** describes the goals of the enterprise network and compares enterprise LANs, WANs, intranets, and extranets. Types of enterprise applications are identified, including traffic flow patterns and prioritization. This chapter also focuses on the needs of teleworkers and the use of virtual private networks to support them.
- **Chapter 2, "Exploring the Enterprise Network Infrastructure,"** describes the network operations center (NOC), telecommunications rooms, and network documentation used in the enterprise. Requirements for supporting the enterprise edge are introduced, including external service delivery and security considerations. This chapter also provides a good review of switch and router hardware. It reinforces the basic commands necessary to configure switches and routers and verify their operation.
- **Chapter 3, "Switching in an Enterprise Network,"** focuses on the characteristics of switches and issues associated with supporting them in an enterprise environment. These include redundancy and Spanning Tree Protocol (STP). You learn to configure VLANs, trunking, and multi-switch inter-VLAN routing. The chapter also covers the VLAN Trunking Protocol (VTP), support for IP telephony, and wireless and VLAN implementation best practices.
- **Chapter 4, "Addressing in an Enterprise Network,"** compares flat and hierarchical network design with a focus on the structure and advantages of hierarchical IP addressing. This chapter provides a review of subnet masks and basic subnetting and introduces variable-length subnet masks (VLSM) and their benefits. It provides instruction on how to implement VLSM addressing in hierarchical network design. The use and importance of classless routing, classless inter-domain routing (CIDR), and route summarization are explained, along with subnetting best practices. This chapter also provides a review of private IP addressing, Network Address Translation (NAT), and Port Address Translation (PAT), with examples of implementation.

- **Chapter 5, "Routing with a Distance Vector Protocol,"** describes common network topologies and provides a review of static and dynamic routing and default routes. The chapter also provides a review of distance vector routing protocols. The advantages and disadvantages of using Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP) are discussed. Instructions are provided for the configuration and implementation of the RIPv2 and EIGRP dynamic routing protocols.
- **Chapter 6, "Routing with a Link-State Protocol,"** focuses on link-state routing protocols, specifically the Open Shortest Path First (OSPF) Protocol. OSPF characteristics are described, as are advantages and issues involved with implementing OSPF. Instructions are provided for configuring single-area OSPF. In addition, issues associated with using multiple routing protocols in a network are addressed.
- **Chapter 7, "Implementing Enterprise WAN Links,"** focuses on devices and technology options for connecting the enterprise WAN. Packet- and circuit-switching technologies are compared, as are last-mile and long-range technologies. WAN encapsulations, such as High-Level Data Link Control (HDLC) and PPP, are described. You learn how to configure PPP on a WAN link, including authentication. The chapter also provides an overview of the popular Frame Relay WAN technology.
- **Chapter 8, "Filtering Traffic Using Access Control Lists,"** emphasizes the importance of using access control lists (ACL) in network security and traffic flow control. This chapter describes the various types of Cisco IOS ACLs and how they are configured, including the use of the wildcard mask. Standard, extended, and named ACLs are compared, with suggestions for when to use them and placement in specific scenarios. Details are provided on how to create, edit, and apply various ACLs. Filtering traffic based on specific fields in the IP packet is covered. The use of ACLs with NAT and PAT and inter-VLAN routing is discussed. In addition, ACL logging (and the use of syslog servers) is introduced.
- **Chapter 9, "Troubleshooting an Enterprise Network,"** emphasizes the impact of network failure on an organization and the concept of a failure domain. This chapter describes network monitoring tools and techniques and reviews the troubleshooting process. This chapter identifies common problems associated with switching and connectivity, routing, WAN configurations and ACLs, and ways to troubleshoot these problems.
- **Chapter 10, "Putting It All Together,"** In this summary activity, you use what you have learned about the enterprise network infrastructure, switching technologies, hierarchical IP addressing, routing protocols, WAN technologies, and ACLs to build and configure a multi-switch, multirouter simulated enterprise network.

Part I: Concepts also includes the following:

- **Appendix A, "Check Your Understanding and Challenge Questions Answer Key,"** provides the answers to the Check Your Understanding questions that you find at the end of each chapter. It also includes answers for the Challenge questions and activities that conclude most chapters.
- The **Glossary** provides a compiled list of all the key terms that appear throughout this book, plus additional computer and networking terms.

Part II of this book includes the labs that correspond to each chapter. Part II also includes the following:

- **Appendix B, "Lab Equipment Interfaces and Initial Configuration Restoration,"** provides a table listing the proper interface designations for various routers. Procedures are included for erasing and restoring routers and switches to clear previous configurations. In addition, the steps necessary to restore an SDM router are provided.

About the CD-ROM

The CD-ROM included with this book provides many useful tools and information to support your education:

- **Packet Tracer Activity files**: These are files to work through the Packet Tracer activities referenced throughout the book, as indicated by the Packet Tracer activity icon.
- **Interactive activities**: The CD-ROM contains the interactive activities referenced throughout the book.
- **Taking Notes**: This section includes a TXT file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill for not only learning and studying the material, but for on-the-job success, too. Also included in this section is "A Guide to Using a Networker's Journal" PDF booklet providing important insight into the value of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.
- **IT Career Information**: This section includes a student guide to applying the toolkit approach to your career development. Learn more about entering the world of information technology as a career by reading two informational chapters excerpted from *The IT Career Builder's Toolkit*: "Communication Skills" and "Technical Skills."
- **Lifelong Learning in Networking**: As you embark on a technology career, you will notice that it is ever changing and evolving. This career path provides new and exciting opportunities to learn new technologies and their applications. Cisco Press is one of the key resources to plug into on your quest for knowledge. This section of the CD-ROM provides an orientation to the information available to you and tips on how to tap into these resources for lifelong learning.

PART 1
Concepts

This page intentionally left blank

CHAPTER 2

Exploring the Enterprise Network Infrastructure

Objectives

Upon completion of this chapter, you should be able to answer the following questions:

- What are the main types of network documentation and how are they interpreted?
- What equipment is found in the enterprise Network Operations Center?
- What is the point of presence for service delivery and how is service delivered?
- What are network security considerations and what equipment is used at the enterprise edge?
- What are some characteristics of router and switch hardware?
- What are the most common and useful router and switch CLI configuration and verification commands?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

physical topology page 22

logical topology page 22

control plane page 22

redlined page 24

as-built page 24

business continuity plan (BCP) page 24

business security plan (BSP) page 25

network maintenance plan (NMP) page 25

service-level agreement (SLA) page 25

Network Operations Center (NOC) page 26

data center page 26

server farm page 26

load balancing page 26

network attached storage (NAS) page 27

storage-area network (SAN) page 27

rack units (RU) page 27

Structured cabling page 28

electromagnetic interference (EMI) page 28

telecommunications room page 29

intermediate distribution facility (IDF) page 29

access point (AP) page 29

main distribution facility (MDF) page 29

extended star page 29

Power over Ethernet (PoE) page 31

point of presence (POP) page 31

service provider (SP) page 32

(T1/E1) page 33

punchdown block page 33

channel service unit/data service unit (CSU/DSU) page 33

customer premise equipment (CPE) page 34

form factors page 36

out-of-band page 37

in-band page 37

Port density page 49

Enterprise networks contain hundreds of sites and support thousands of users worldwide. A well-managed network allows users to work reliably. Network documentation is crucial for maintaining the required 99.999 percent uptime. All Internet traffic flows through the enterprise edge, making security considerations necessary. Routers and switches provide connectivity, security, and redundancy while controlling broadcasts and failure domains.

Describing the Current Network

The following sections describe network documentation required to support the enterprise and equipment found in the Network Operations Center as well as telecommunications room design considerations.

Enterprise Network Documentation

One of the first tasks for a new network technician is to become familiar with the current network structure. Enterprise networks can have thousands of hosts and hundreds of networking devices, all of which are interconnected by copper, fiber-optic, and wireless technologies. End-user workstations, servers, and networking devices, such as switches and routers, must all be documented. Various types of documentation show different aspects of the network.

Network infrastructure diagrams, or topology diagrams, keep track of the location, function, and status of devices. Topology diagrams represent either the physical or logical network.

A ***physical topology*** map uses icons to document the location of hosts, networking devices, and media. It is important to maintain and update physical topology maps to aid future installation and troubleshooting efforts.

A ***logical topology*** map groups hosts by network usage, regardless of physical location. Host names, addresses, group information, and applications can be recorded on the logical topology map. Connections between multiple sites might be shown but do not represent actual physical locations.

Enterprise network diagrams can also include ***control plane*** information. Control plane information describes failure domains and defines the interfaces where different network technologies intersect. Figure 2-1 shows a physical topology and Figure 2-2 shows the corresponding logical topology.

Figure 2-1 Physical Network Topology

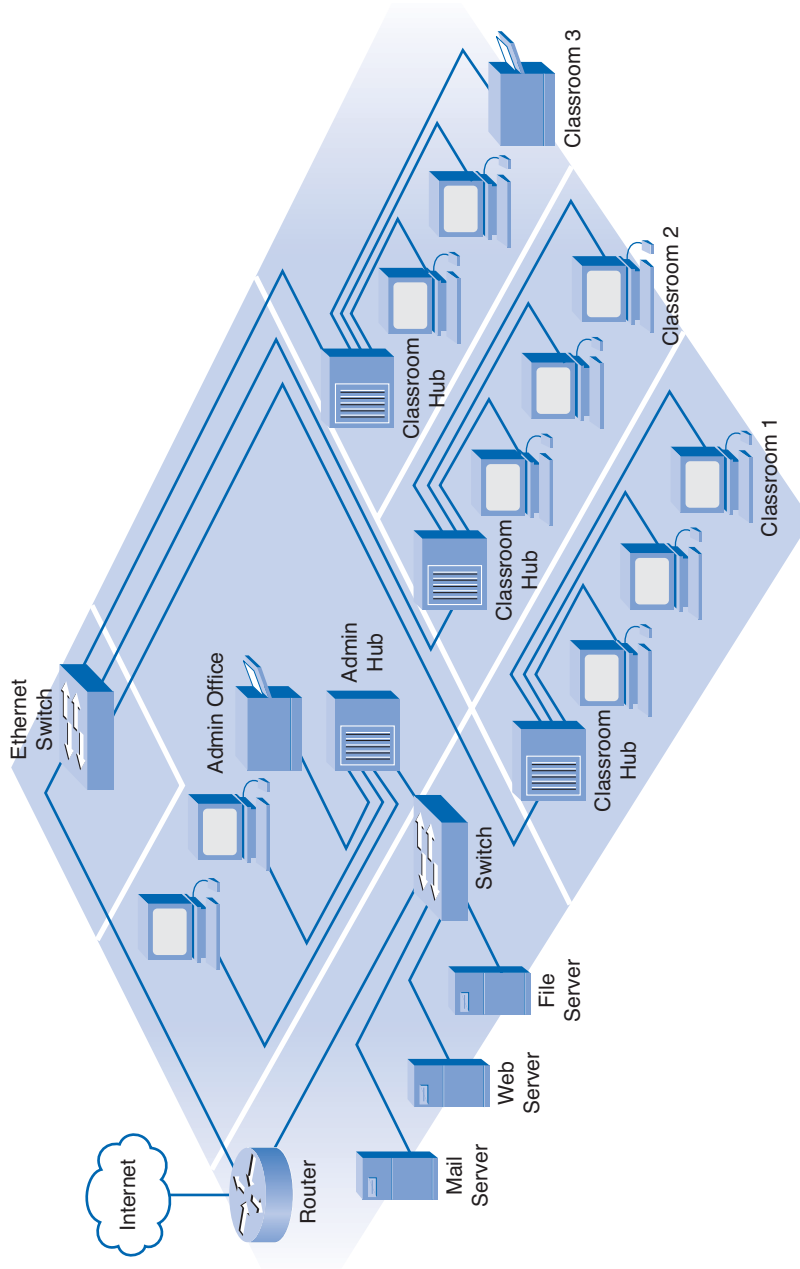
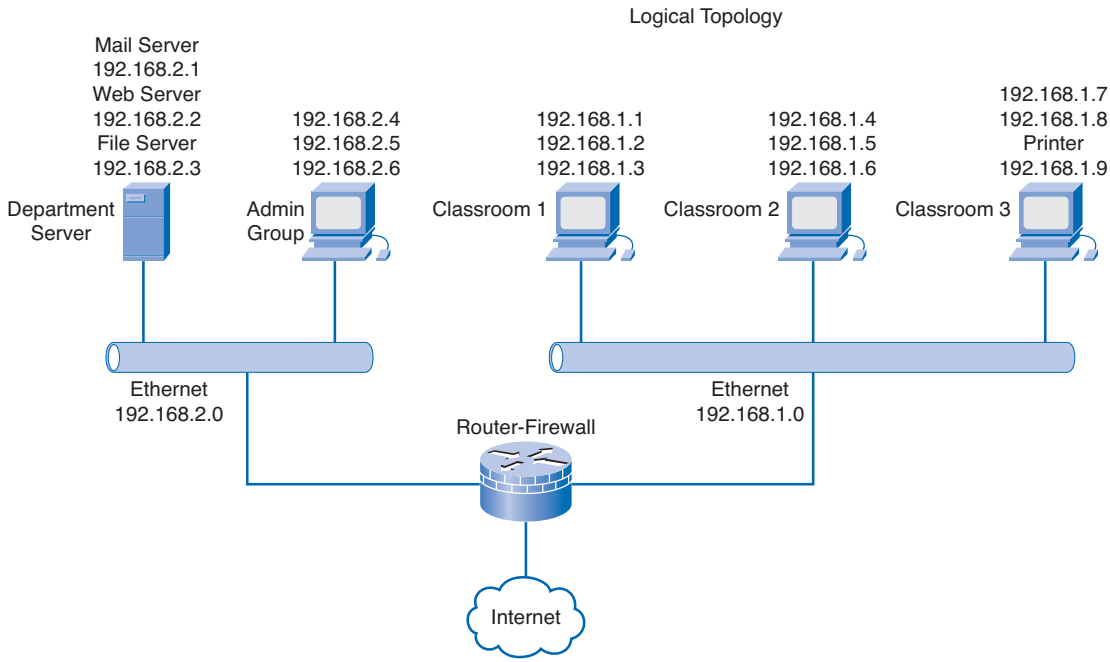


Figure 2-2 Logical Network Topology



It is crucial that network documentation remain current and accurate. Network documentation is usually accurate at the installation of a network. As the network grows or changes, however, you need to update the documentation.

Network topology maps are frequently based on original floor plans. The current floor plans might have changed since the construction of the building. Blueprints can be marked up, or ***redlined***, to show the changes. The modified diagram is known as an ***as-built***. An as-built diagram documents how a network was actually constructed, which can differ from the original plans. Always ensure that the current documentation reflects the as-built floor plan and all network topology changes.

Network diagrams are commonly created using graphical drawing software. In addition to being a drawing tool, many network diagramming tools are linked to a database. This feature allows the network support staff to develop detailed documentation by recording information about hosts and networking devices, including manufacturer, model number, purchase date, warranty period, and more. Clicking a device in the diagram opens an entry form with device data listed.

In addition to network diagrams, several other important types of documentation are used in the enterprise network, including a business continuity plan, a business security plan, a network maintenance plan, and a service-level agreement.

Business Continuity Plan

The ***business continuity plan (BCP)*** identifies the steps to be taken to continue business operation in the event of a natural or man-made disaster. The BCP helps to ensure business operations by defining procedures that must take place when a disaster strikes. IT support can include

- Off-site storage of backup data
- Alternate IT processing centers
- Redundant communication links

Business Security Plan

The ***business security plan (BSP)*** prevents unauthorized access to organizational resources and assets by defining security policies. The BSP includes physical, system, and organizational control measures. The overall security plan must include an IT portion that describes how an organization protects its network and information assets. The IT security plan can contain policies related to

- User authentication
- Permissible software
- Remote access
- Intrusion monitoring
- Incident handling

Network Maintenance Plan

The ***network maintenance plan (NMP)*** minimizes downtime by defining hardware and software maintenance procedures. The NMP ensures business continuity by keeping the network up and running efficiently. Network maintenance must be scheduled during specific time periods, usually nights and weekends, to minimize the impact on business operations. The maintenance plan can contain

- Maintenance time periods
- Scheduled downtime
- Staff on-call responsibilities
- Equipment and software to be maintained (OS, IOS, services)
- Network performance monitoring

Service-Level Agreement

A ***service-level agreement (SLA)*** ensures service parameters by defining required service provider level of performance. The SLA is a contractual agreement between the customer and a service provider or ISP, specifying items such as network availability and service response time. An SLA can include

- Connection speeds/bandwidth
- Network uptime
- Network performance monitoring
- Problem resolution response time
- On-call responsibilities

Network documentation should be kept in a centrally located area that is available by all who need access to it. Although it is common to store network documentation on network servers in digital form, hard copy versions should also be kept in filing cabinets in the event the network or server is down. Digital and hard copy versions should also be kept in a secure off-site location in the event of a disaster.

Interactive Activity 2-1: Matching Network Information to Documentation Type (2.1.1)

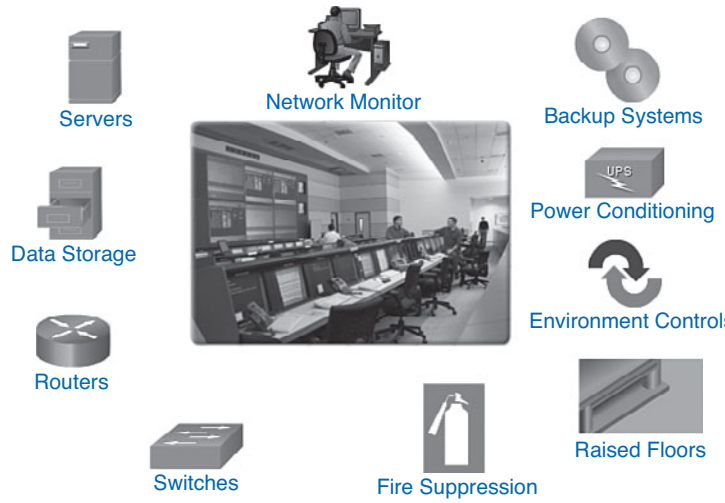
In this activity, you identify the network documentation where the information would most likely be found. Use file d3ia-2114 on the CD-ROM that accompanies this book to perform this interactive activity.

Network Operations Center (NOC)

Most enterprise networks have a ***Network Operations Center (NOC)*** that allows central management and monitoring of all network resources. The NOC is sometimes referred to as a ***data center***.

Employees in a typical enterprise NOC provide support for both local and remote locations, often managing both local- and wide-area networking issues. Larger NOCs can be multiroom areas of a building where network equipment and support staff are concentrated. Figure 2-3 shows a large NOC surrounded by the types of features and equipment found there.

Figure 2-3 Network Operations Center Components and Features



The NOC usually has

- Raised floors to allow cabling and power to run under the floor to the equipment
- High-performance UPS systems and air conditioning equipment to provide a safe operating environment for equipment
- Fire suppression systems integrated into the ceiling
- Network monitoring stations, servers, backup systems, and data storage
- Access layer switches and distribution layer routers, if it serves as a main distribution facility (MDF) for the building or campus where it is located

In addition to providing network support and management, many NOCs also provide centralized resources such as servers and data storage. Servers in the NOC are usually clustered together, creating a server farm. The ***server farm*** is frequently considered as a single resource but, in fact, provides two functions: backup and ***load balancing***. If one server fails or becomes overloaded, another server takes over.

The servers in the farm can be rack-mounted and interconnected by very high-speed switches (Gigabit Ethernet or higher). They can also be blade servers mounted in a chassis and connected by a high-speed backplane within the chassis. Figure 2-4 shows a group of rack-mounted servers.

Figure 2-4 Rack-Mounted Server Farm

Server Farm

Another important aspect of the enterprise NOC is high-speed, high-capacity data storage. This data storage, or ***network attached storage (NAS)***, groups large numbers of disk drives that are directly attached to the network and can be used by any server. An NAS device is typically attached to an Ethernet network and is assigned its own IP address. Figure 2-5 shows an example of multiple rack-mounted NAS drives.

Figure 2-5 Network Attached Storage (NAS)

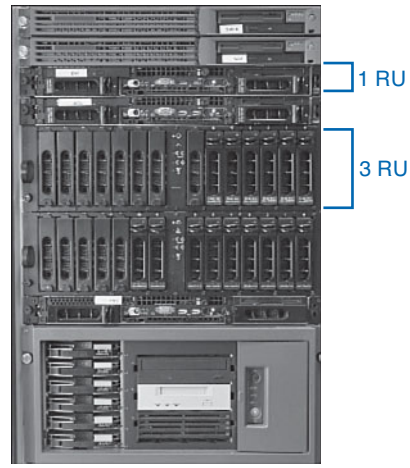
Network Attached Storage (NAS)

A more sophisticated version of NAS is a ***storage-area network (SAN)***. A SAN is a high-speed network that interconnects different types of data storage devices over a LAN or WAN.

Equipment in the enterprise NOC is usually mounted in racks. In large NOCs, racks are usually floor-to-ceiling mounted and can be attached to each other. When mounting equipment in a rack, ensure that there is adequate ventilation and access from front and back. Equipment must also be attached to a known good ground.

The most common rack width is 19 inches (48.26 cm). Most equipment is designed to fit this width. The vertical space that the equipment occupies is measured in ***rack units (RU)***. A unit equals 1.75 inches (4.4 cm). For example, a 2RU chassis is 3.5 inches (8.9 cm) high. The lower the RU number the less space a device needs; therefore, more devices can fit into the rack. Figure 2-6 shows multiple servers and disk drives in a rack configuration. Each server occupies one RU and the drives typically take two or more RUs.

Figure 2-6 Network Equipment Height Measured in RUs



Another consideration is equipment with many connections, like switches. They might need to be positioned near patch panels and close to where the cabling is gathered into cable trays.

In an enterprise NOC, thousands of cables can enter and exit the facility. ***Structured cabling*** creates an organized cabling system that is easily understood by installers, network administrators, and any other technicians who work with cables.

Cable management serves many purposes. First, it presents a neat and organized system that aids in isolating cabling problems. Second, best cabling practices protect the cables from physical damage and ***electromagnetic interference*** (***EMI***), which greatly reduces the number of problems experienced.

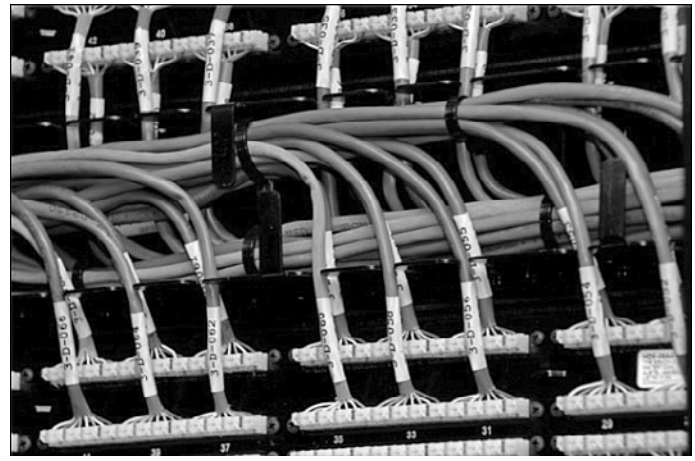
To assist in troubleshooting

- All cables should be labeled at both ends, using a standard convention that indicates source and destination.
- All cable runs should be documented on the physical network topology diagram.
- All cable runs, both copper and fiber, should be tested end to end by sending a signal down the cable and measuring loss.

Cabling standards specify a maximum distance for all cable types and network technologies. For example, the IEEE specifies that, for Fast Ethernet over unshielded twisted-pair (UTP), the cable run from switch to host cannot be greater than 100 meters (approximately 328 ft.). If the cable run is greater than the recommended length, problems could occur with data communications, especially if the terminations at the ends of the cable are poorly completed.

Documentation of the cable plan and testing are critical to network operations. Figure 2-7 shows cabling routed efficiently to the back of a patch panel. Cable bends are minimized, and each cable is clearly labeled for its destination.

Figure 2-7 Properly Routed and Labeled Cabling



Telecommunication Room Design and Considerations

The NOC is the heart of the enterprise. In practice, however, most users connect to a switch in a ***telecommunications room***, which is some distance from the NOC. The telecommunications room is also referred to as a wiring closet or ***intermediate distribution facility (IDF)***. It contains the access layer networking devices and ideally maintains environmental conditions similar to the NOC, such as air conditioning and UPS. IDFs typically contain

- Fast Ethernet switches
- Gigabit link to MDF
- Wireless access points

Users working with wired technology connect to the network through Ethernet switches or hubs. Users working with wireless technology connect through an ***access point (AP)***. Access layer devices such as switches and APs are a potential vulnerability in network security. Physical and remote access to this equipment should be limited to authorized personnel. Network personnel can also implement port security and other measures on switches, as well as various wireless security measures on APs.

Securing the telecommunications room has become even more important because of the increasing occurrence of identity theft. New privacy legislation results in severe penalties if confidential data from a network falls into the wrong hands. Modern networking devices offer capabilities to help prevent these attacks and protect data and user integrity.

Many IDFs connect to a ***main distribution facility (MDF)*** using an ***extended star*** design. The MDF is usually located in the NOC or centrally located within the building.

MDFs are typically larger than IDFs. They house high-speed switches, routers, and server farms. The central MDF switches can have enterprise servers and disk drives connected using gigabit copper links. MDFs typically contain

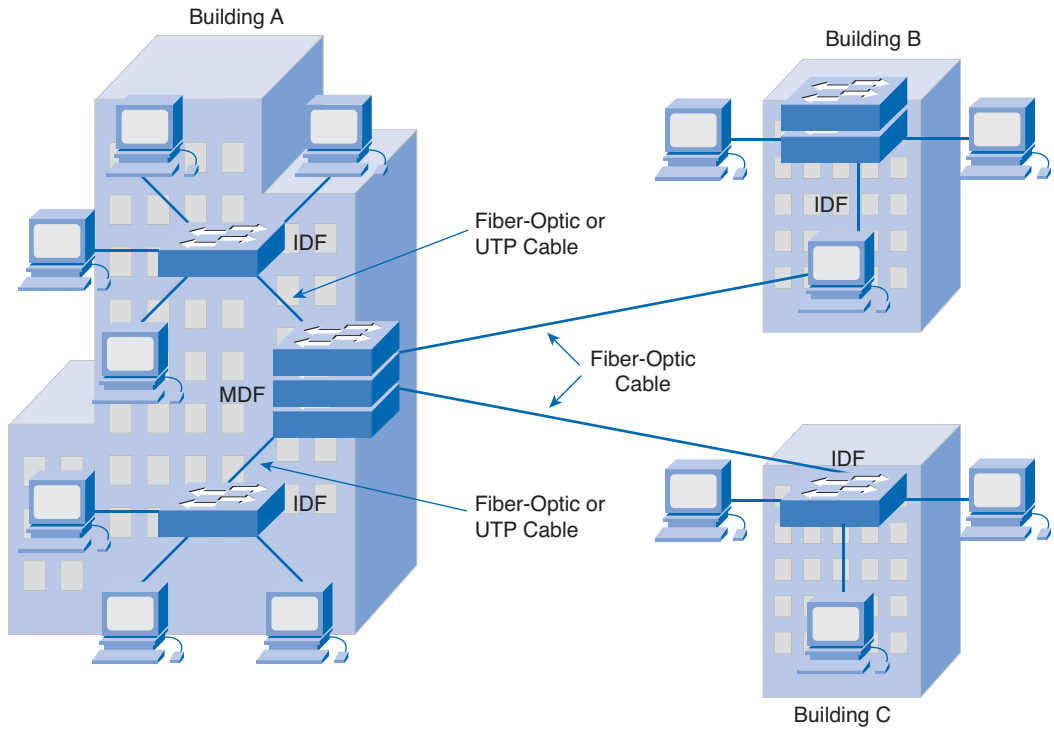
- Point of presence (POP)
- Routers
- Gigabit switches

- Gigabit links to IDFs
- Servers
- Disk storage

IDFs contain lower-speed switches, APs, and hubs. The switches in the IDFs typically have large numbers of Fast Ethernet ports for users to connect at the access layer.

The switches in the IDF usually connect to the switches in the MDF with Gigabit interfaces. This arrangement creates backbone connections, or uplinks. These backbone links, also called vertical cabling, can be copper or fiber-optic. Copper Gigabit or Fast Ethernet links are limited to a maximum of 100 meters and should use CAT5e or CAT6 UTP cable. Fiber-optic links can run much greater distances. Fiber-optic links commonly interconnect buildings, and because they do not conduct electricity, they are immune to lightning strikes, EMI, RFI, and differential grounds. Figure 2-8 illustrates a multi-building Ethernet network design with one MDF in Building A and IDFs in Buildings A, B, and C. The vertical or backbone cabling connecting the MDF and the two IDFs in Building A can be UTP or fiber depending on distance. Vertical (and horizontal) cable runs longer than 100 meters (approx. 328 ft.) should be fiber-optic.

Figure 2-8 MDFs and IDFs Connect Multiple Buildings and Users



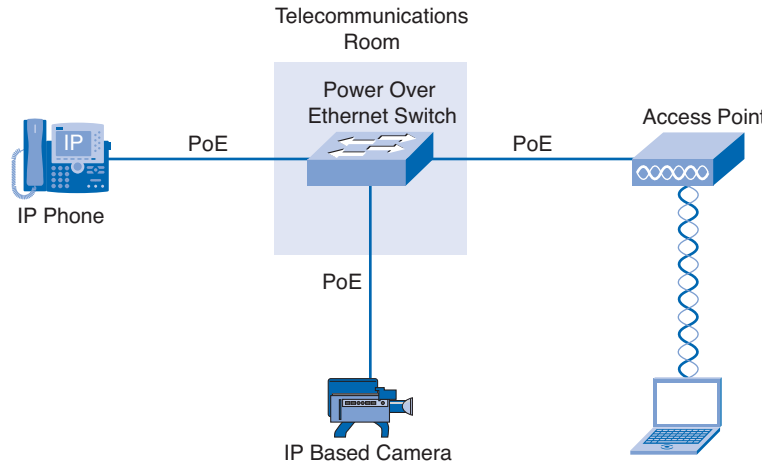
The vertical cabling between the buildings should always be fiber-optic, regardless of distance, to account for the electrical differential between buildings. Inter-building cabling can also be exposed to weather and lightning strikes, which fiber-optic can withstand more easily without damaging equipment connected to it.

In addition to providing basic network access connectivity, it is becoming more common to provide power to end-user devices directly from the Ethernet switches in the telecommunications room. These devices include IP phones, access points, and surveillance cameras.

These devices are powered using the IEEE 802.3af standard, ***Power over Ethernet (PoE)***. PoE provides power to a device over the same twisted-pair cable that carries data. This allows an IP phone, for example, to be located on a desk without the need for a separate power cord or a power outlet. To support PoE devices such as the IP phone, the connecting switch must have PoE capability.

PoE can also be provided by power injectors or PoE patch panels for those switches that do not support PoE. Panduit and other suppliers produce PoE patch panels that allow non-PoE-capable switches to participate in PoE environments. Legacy switches connect into the PoE patch panel, which then connects to the PoE-capable device. Figure 2-9 illustrate devices that can be powered by a PoE-capable switch. This allows the devices to be placed without regard to the location of power outlets.

Figure 2-9 End Devices Receive Power from a PoE Switch



Interactive Activity 2-2: Placing MDFs, IDFs, and Cabling (2.1.3)

In this activity, you place the MDFs and IDFs in an appropriate location in the campus diagram and identify appropriate cables to connect them. Use file d3ia-213 on the CD-ROM that accompanies this book to perform this interactive activity.

Supporting the Enterprise Edge

The enterprise edge is the entry and exit point to the network for external users and services. The following sections describe how external services are delivered as well as security considerations at the edge.

Service Delivery at the Point of Presence

At the outer edge of the enterprise network is the ***point of presence (POP)***, which provides an entry point for services to the enterprise network. Externally provided services coming in through the POP include Internet access, wide-area connections, and telephone services (public switched telephone network [PSTN]).

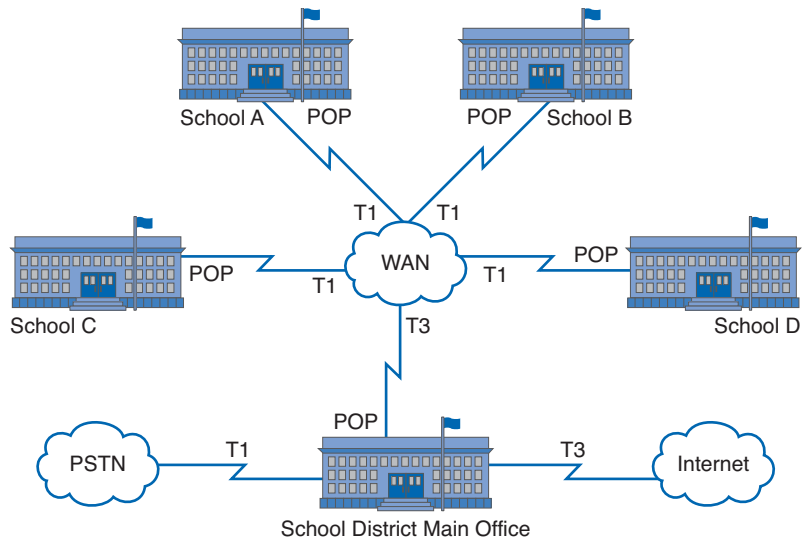
The POP contains a point of demarcation, or the demarc. The demarc provides a boundary that designates responsibility for equipment maintenance and troubleshooting between the ***service provider (SP)*** and customer. Equipment from the service provider up to the point of demarcation is the responsibility of the provider; anything past the demarc point is the responsibility of the customer.

In an enterprise, the POP provides links to outside services and sites. The POP can provide a direct link to one or more ISPs, which allows internal users the required access to the Internet. The remote sites of an enterprise are also interconnected through the POPs. The service provider establishes the wide-area links between these remote sites.

The location of the POP and the point of demarcation vary in different countries. While they are often located within the MDF of the customer, they can also be located at the SP.

Figure 2-10 shows an example of a school district with a hub-and-spoke, or star, design. The school district main office is the center of the star or hub and has the primary connections to the Internet and the PSTN. Each of the schools A, B, C, and D connect back to the district office for phone and Internet access to the outside world. The district office and each of the schools have their own POP to make the necessary WAN connections. Each school is connected to the district office with a T1 circuit with a bandwidth of 1.544 Mbps. Because all the schools share the main Internet connection at the district office, the connection to the ISP is a T3 circuit with approximately 45 Mbps bandwidth. This is a scalable design, where additional schools with T1s can connect back to the district office. This design can be applied to businesses and other organizations with multiple remote locations that connect to a central site. If additional remote sites are added to the network, the bandwidth of the Internet and PSTN connections at the central site can be upgraded to higher-speed links, if necessary.

Figure 2-10 POPs at Each Location Connect Schools to the District Office and External Services



Security Considerations at the Enterprise Edge

Large enterprises usually consist of multiple sites that interconnect. Multiple locations can have edge connections at each site connecting the enterprise to other individuals and organizations.

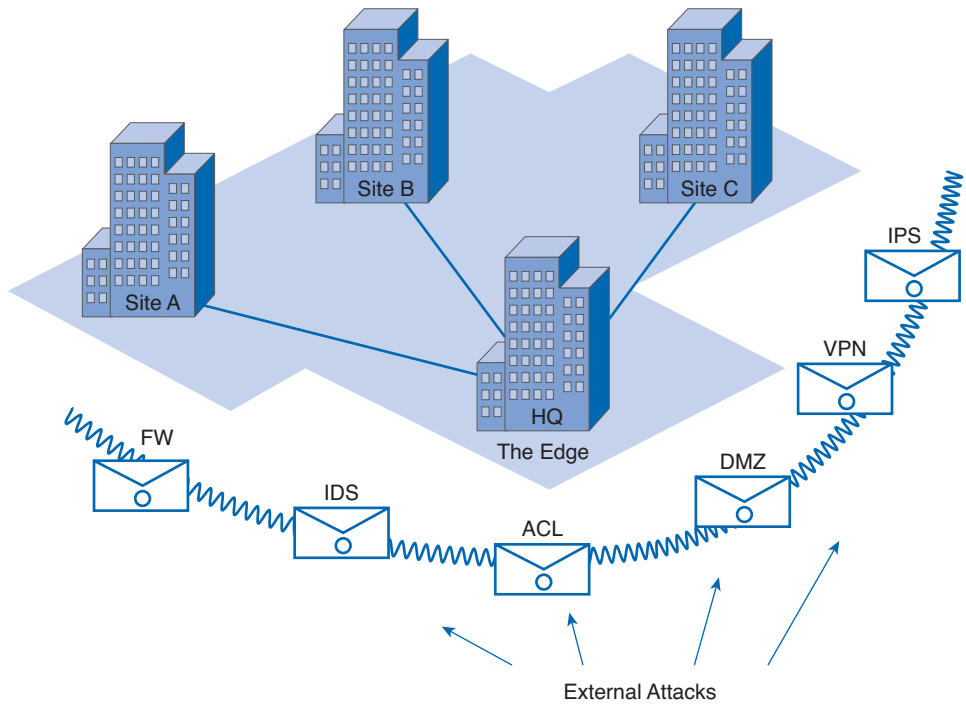
The edge is the point of entry for outside attacks and is a point of vulnerability. Attacks at the edge can affect thousands of users. For example, denial of service (DoS) attacks prevent access to resources for legitimate users inside or outside the network, affecting productivity for the entire enterprise.

All traffic into or out of the organization goes through the edge. Edge devices must be configured to defend against attacks and provide filtering based on website, IP address, traffic pattern, application, and protocol.

An organization can deploy a firewall and security appliances with an intrusion detection system (IDS) and intrusion prevention system (IPS) at the edge to protect the network. They can also set up a demilitarized zone (DMZ), an area isolated be firewalls, where web and FTP servers can be placed for external users to access.

External network administrators require access for internal maintenance and software installation. Virtual Private Networks (VPN), access control lists (ACL), user IDs, and passwords provide that access. VPNs also allow remote workers access to internal resources. Figure 2-11 depicts a network with the headquarters (HQ) as the edge, with security protection tools deployed to protect the internal network.

Figure 2-11 Security Defense Tools at the Enterprise Edge



Connecting the Enterprise Network to External Services

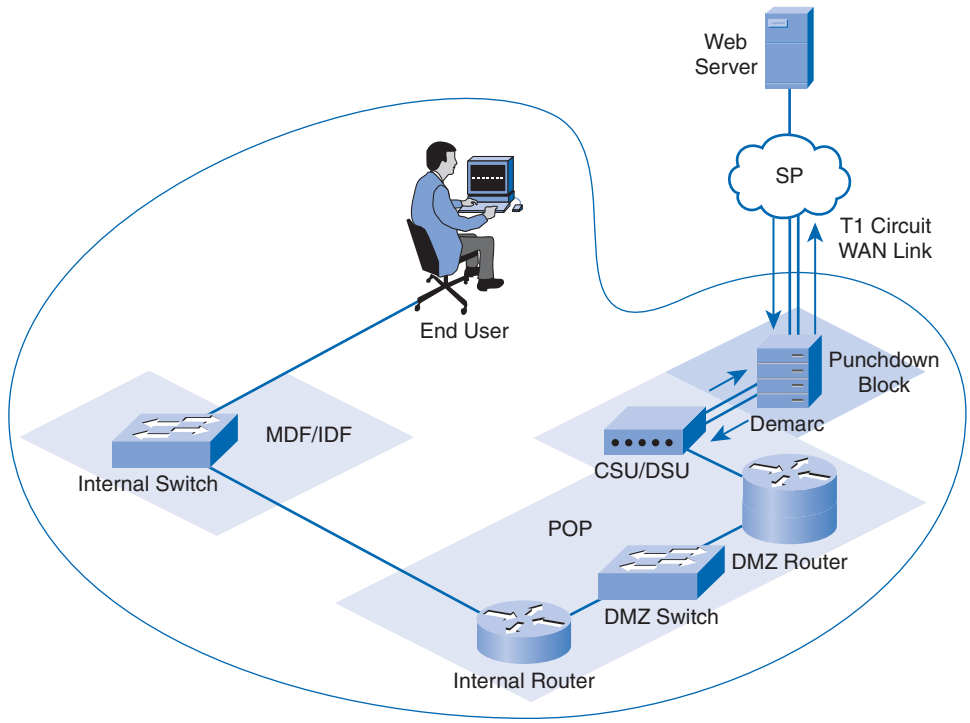
The network connection services commonly purchased by an enterprise include leased lines ***(T1/E1)***, Frame Relay, and ATM. Physical cabling brings these services to the enterprise using copper wires, as in the case of T1/E1, or fiber-optic cable for higher-speed services.

The POP must contain certain pieces of equipment to obtain whichever WAN service is required. For example, to obtain T1/E1 service, the customer might require a ***punchdown block*** to terminate the T1/E1 circuit, as well as a ***channel service unit/data service unit (CSU/DSU)*** to provide the proper

electrical interface and signaling for the service provider. This equipment can be owned and maintained by the service provider or can be owned and maintained by the customer. Regardless of ownership, all equipment located within the POP at the customer site is referred to as ***customer premise equipment (CPE)***. The CSU/DSU can be an external standalone device connected to the edge router with a cable or it can be integrated into the router.

Figure 2-12 shows an example of the equipment in the proper sequence required to bring a T1 circuit from a service provider to a customer and finally to the end user. The T1 can be provided by an SP or an ISP and can provide access to the Internet directly or to another site to form a WAN.

Figure 2-12 Connections and Devices from Service Provider to End User



Interactive Activity 2-3: Specifying Components to Bring Service to the Internal Network (2.2.3)

In this activity, you specify the components, in order, needed to connect a service from the edge to the internal network. Use file d3ia-223 on the CD-ROM that accompanies this book to perform this interactive activity.

Reviewing Routing and Switching

The following sections provide a review of router and switch hardware characteristics. They also serve as a review of router and switch commands most commonly used to display information about and configure these devices.

Router Hardware

One important device in the distribution layer of an enterprise network is a router. Without the routing process, packets could not leave the local network.

The router provides access to other private networks as well as to the Internet. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway.

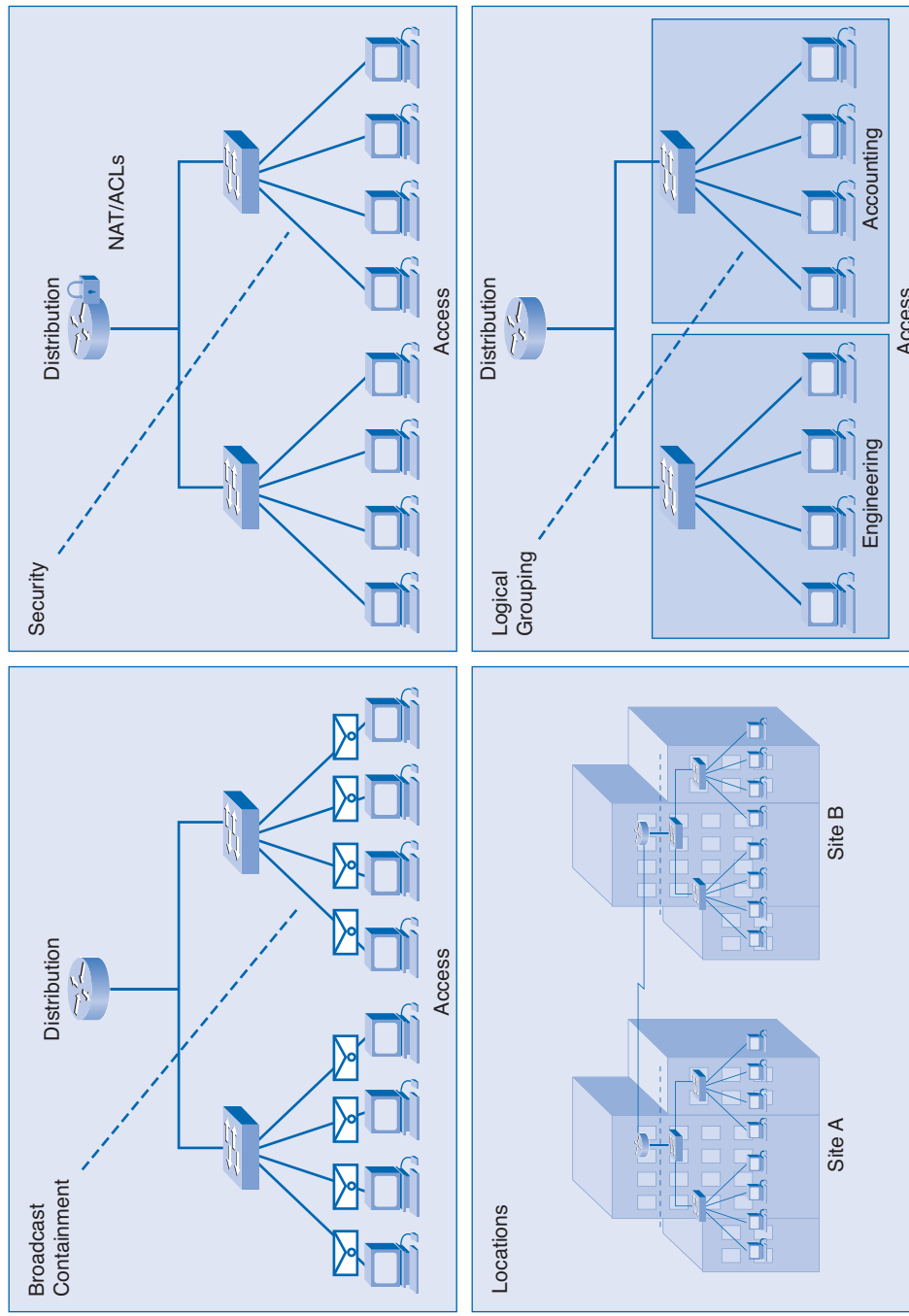
Routers play a critical role in networking by interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols. For example, a router can re-encapsulate packets from an Ethernet to a serial encapsulation.

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link goes down or traffic is congested. Routers also serve the following other beneficial functions:

- **Provide broadcast containment:** Routers in the distribution layer limit broadcasts to the local network where they need to be heard. Although broadcasts are necessary, too many hosts connected on the same local network generate excessive broadcast traffic and slow the network.
- **Connect remote locations:** Routers in the distribution layer interconnect local networks at various locations of an organization that are geographically separated.
- **Group users logically by application or department:** Routers in the distribution layer logically group users, such as departments within a company, who have common needs or for access to resources.
- **Provide enhanced security (using Network Address Translation [NAT] and ACLs):** Routers in the distribution layer separate and protect certain groups of computers where confidential information resides. Routers also hide the addresses of internal computers from the outside world to help prevent attacks and control who gets into or out of the local network.

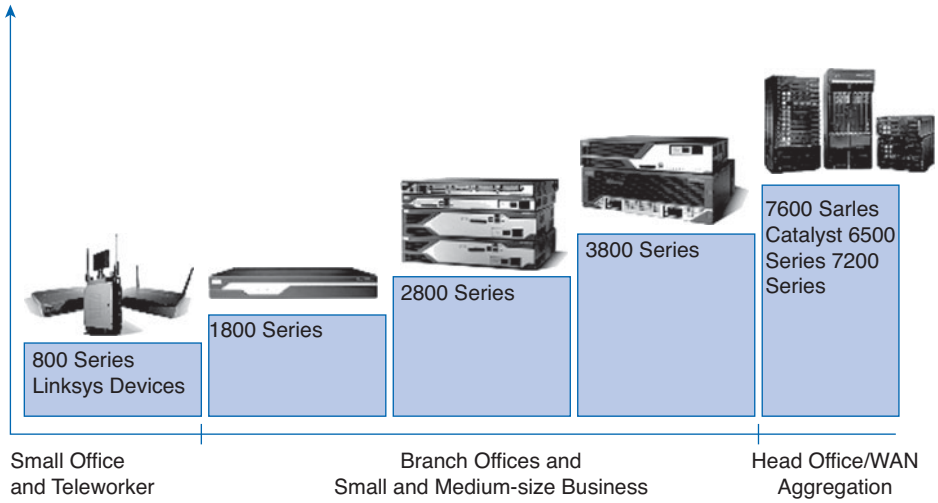
With the enterprise and the ISP, the ability to route efficiently and recover from network link failures is critical to delivering packets to their destination. Figure 2-13 depicts each of the main functions the routers can perform.

Figure 2-13 Functions of Routers



Routers come in many shapes and sizes called ***form factors***, as shown in Figure 2-14, and can support a few users or thousands of users, depending on the size and needs of the organization. Network administrators in an enterprise environment should be able to support a variety of routers and switches, from a small desktop to a rack-mounted or blade model.

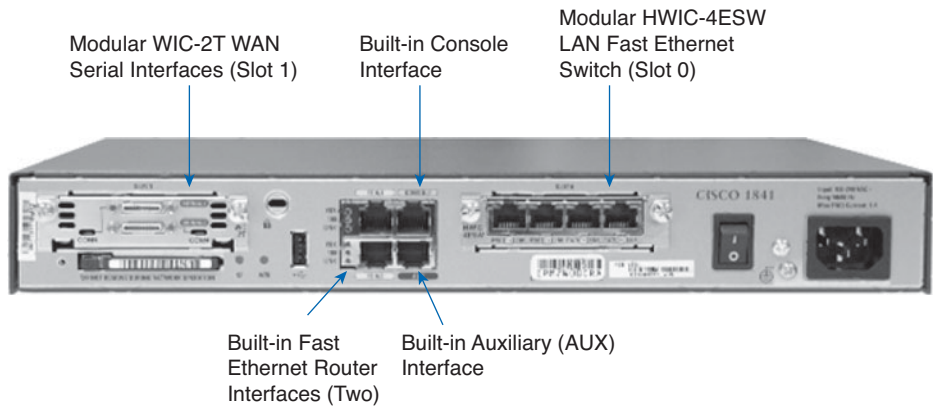
Figure 2-14 Router Classes and Form Factors



Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. As an example, a Cisco 1841 router comes with two Fast Ethernet RJ-45 interfaces built in and two slots that can accommodate many different network interface modules.

Routers come with a variety of different interfaces, such as Fast and Gigabit Ethernet, serial, and fiber-optic. Router interfaces use the controller/interface or controller/slot/interface conventions. For example, using the controller/interface convention, the first Fast Ethernet interface on a router is numbered as Fa0/0 (controller 0 and interface 0). The second is Fa0/1. The first serial interface on a router using controller/slot/interface is S0/0/0. Figure 2-15 shows the back of an 1841 ISR router with a serial interface card and an integrated 4-port Fast Ethernet switch.

Figure 2-15 Router Interfaces



Two methods exist for connecting a PC to a network device for configuration and monitoring tasks: ***out-of-band*** and ***in-band*** management.

Out-of-Band Management

Out-of-band management is used for initial configuration or when a network connection is not unavailable. If there is a problem with access to a network device through the network, it might be

necessary to use out-of-band management. For example, a WAN serial interface on a remote router might have been misconfigured so that normal network access is not possible. If the AUX port is properly configured for remote access and a dialup modem is connected, it might be possible to dial in to the modem using out-of-band management and reconfigure the router to correct the problem. Configuration using out-of-band management requires

- Direct connection to the device console port or a direct or remote connection (through dialup) to the AUX port
- Terminal emulation client

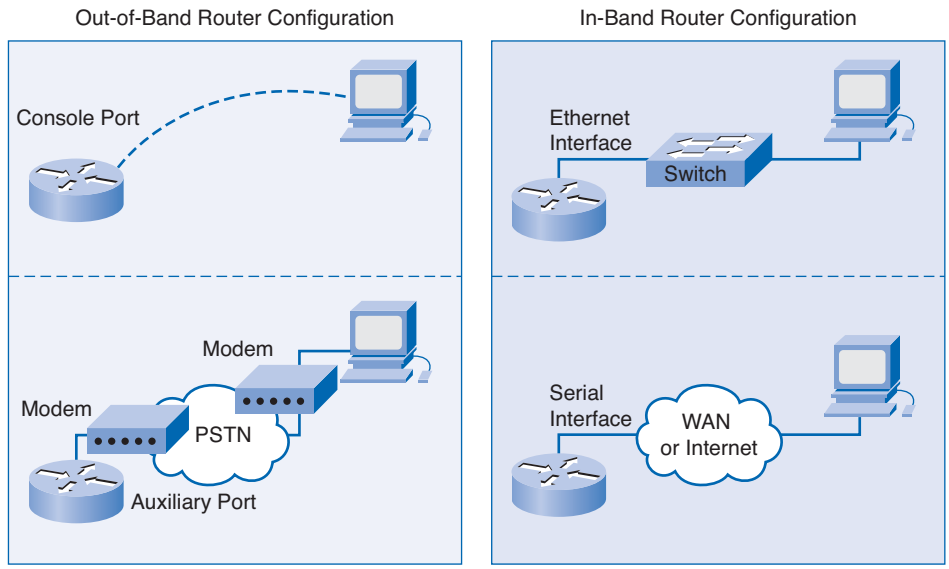
In-Band Management

In-band management is used to monitor and make configuration changes to a network device over a network connection. With in-band, the connection shares network bandwidth with other hosts on the network. Configuration using in-band management requires

- At least one network interface on the device to be connected and operational
- Valid IP configuration on interfaces involved (for an IP-based network)
- Telnet, Secure Shell (SSH), or HTTP to access a Cisco device (these protocols are primarily IP based)

Figure 2-16 shows two forms of out-of-band and two forms of in-band management.

Figure 2-16 Out-of-Band and In-Band Management Methods



Basic Router CLI show Commands

This section includes some of the most commonly used Cisco IOS commands to display and verify the operational status of the router and related network functionality. These commands are divided into several categories, as shown in Table 2-1.

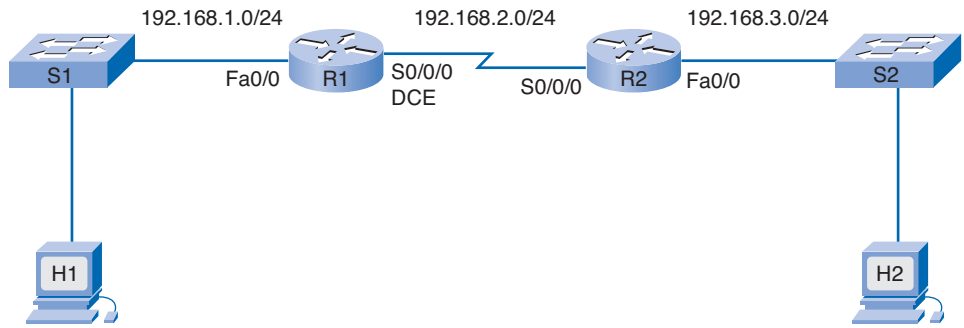
Table 2-1 lists these commands with common options used and the minimum abbreviation allowable, along with a description of their function and key information displayed.

Table 2-1 Common Router show Commands

Full Command	Abbreviation	Purpose / Information Displayed
		General Use
show running-config	**sh run**	Displays current config running in RAM. Includes host name, passwords, interface IP addresses, routing protocol activated, DHCP, and NAT configuration. Must be issued in EXEC mode.
show startup-config	**sh star**	Displays backup config in NVRAM. Can be different if running config has not been copied to backup. Must be issued in EXEC mode.
show version	**sh ve**	Displays IOS version, ROM version, router uptime system image file name, boot method, number and type of interfaces installed, and amount of RAM, NVRAM, and flash. Also shows the Configuration register.
		Routing Related
show ip protocols	**sh ip pro**	Displays information for routing protocols configured including timer settings, version numbers, update intervals, active interfaces, and networks advertised.
show ip route	**sh ip ro**	Displays routing table information including routing code, networks known, admin distance and metric, how they were learned, last update next hop, interface learned through, and any static routes (including default) configured.
		Interface Related
show interfaces (type #)	**sh int f0/0**	Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics.
show ip interface brief	**sh ip int br**	Displays all interfaces with IP address with interface status (up/down/admin down) and line protocol status (up/down).
show protocols	**sh prot**	Displays all interfaces with IP address and subnet mask (slash notation) with interface status (up/down/admin down) and line protocol status (up/down) .
		Connectivity Related
show cdp neighbors (detail)	**sh cdp ne**	Displays information on directly connected devices including device ID (host name), local interface where device is connected, capability (R=router, S=switch), platform (e.g., 2620XM), and port ID of remote device. The detail option provides the IP address of the other device as well as the IOS version.
show sessions	**sh ses**	Displays Telnet sessions (VTY) with remote hosts. Displays session number, host name, and address.
show ssh	**sh ssh**	Displays SSH server connections with remote hosts.
ping (ip / hostname)	**p**	Sends five ICMP echo requests to an IP address or host name (if DNS is available) and displays the min/max and avg time to respond.
traceroute (ip / hostname)	**tr**	Sends echo request with varying TTL. Lists routers (hops) in path and time to respond.

Figure 2-17 shows two networks (192.168.1.0/24 and 192.168.3.0/24) interconnected with a WAN link (network 192.168.2.0/24).

Figure 2-17 Multi-router and Multi-switch Network



The following examples display the **show** command output for the R1 model 1841 router in the Figure 2-17 network topology. Example 2-1 shows the **show running-config** output for R1.

Example 2-1 R1 show running-config Command Output

```
R1# show running-config

<output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
 description LAN 192.168.1.0 default gateway
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description WAN link to R2
 ip address 192.168.2.1 255.255.255.0
 encapsulation ppp
 clock rate 64000
 no fair-queue
```

```
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
!
banner motd ^CUnauthorized Access Prohibited^C
!
ip http server
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
```

Example 2-2 presents the **show version** output for R1.

Example 2-2 R1 show version Command Output

```
R1# show version

<output omitted>
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
R1 uptime is 43 minutes
System returned to ROM by reload at 22:05:12 UTC Sat Jan 5 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
6 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Example 2-3 presents the **show ip protocols** output for R1.

Example 2-3 R1 show ip protocols Command Output

```
R1# show ip protocols

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 20 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    Serial0/0/0           2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:20
  Distance: (default is 120)
```

Example 2-4 presents the **show ip route** output for R1.

Example 2-4 R1 show ip route Command Output

```
R1# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
```

Example 2-5 presents the **show interfaces** output for R1.

Example 2-5 R1 show interfaces Command Output

```
R1# show interfaces

< Some output omitted >
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     196 packets input, 31850 bytes
     Received 181 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     392 packets output, 35239 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is administratively down, line protocol is down

Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Listen, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:51:52
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     401 packets input, 27437 bytes, 0 no buffer
     Received 293 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     389 packets output, 26940 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     6 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Serial0/0/1 is administratively down, line protocol is down
```

Example 2-6 presents the **show ip interfaces brief** output for R1.

Example 2-6 R1 show ip interfaces brief Command Output

```
R1# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.1     YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/0                192.168.2.1     YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Vlan1                      unassigned      YES unset  up                    down
```

Example 2-7 presents the **show protocols** output for R1.

Example 2-7 R1 show protocols Command Output

```
R1# show protocols

Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
FastEthernet0/1/0 is up, line protocol is down
FastEthernet0/1/1 is up, line protocol is down
FastEthernet0/1/2 is up, line protocol is down
FastEthernet0/1/3 is up, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.1/24
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is up, line protocol is down
```

Example 2-8 presents the **show cdp neighbors** output for R1.

Example 2-8 R1 show cdp neighbors Command Output

```
R1# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Ser 0/0/0          137        R S I      1841      Ser 0/0/0
S1               Fas 0/0            175         S I       WS-C2960- Fas 0/1
```

Example 2-9 presents the **show cdp neighbors detail** output for R1.

Example 2-9 R1 show cdp neighbors detail Command Output

```
R1# show cdp neighbors detail

-------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.2.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/0,  Port ID (outgoing port): Serial0/0/0
Holdtime : 164 sec
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team
advertisement version: 2
VTP Management Domain: ''

-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.5
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 139 sec
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE3, RELE
ASE SOFTWARE (fc2)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 13:57 by myl
advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010221FF000000000000001D46350C80FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
```

Interactive Activity 2-4: Matching the Command to the Information Needed (2.3.2)

In this activity, you identify the command that can provide the information indicated. Use file d3ia-232 on the CD-ROM that accompanies this book to perform this interactive activity.

Basic Router Configuration Using CLI

A basic router configuration includes the host name for identification, passwords for security, and assignment of IP addresses to interfaces for connectivity. Verify and save configuration changes using the **copy running-config startup-config** command. To clear the router configuration, use the **erase startup-config** command and then the **reload** command. Table 2-2 shows common IOS commands used to configure routers. Also listed are the abbreviation, the purpose of the command, and the required mode to execute the command.

Table 2-2 Common Router Configuration Commands

Full Command / Example	Abbreviation	Purpose / Mode
	Configuration Management	
enable	**en**	Changes from user EXEC mode (>) to privileged EXEC mode (#)
configure terminal	**conf t**	Changes from privileged EXEC mode to global configuration mode
copy running-config startup-config	**cop r s**	Copies the running configuration from RAM to the startup configuration file in NVRAM
erase startup-config	**era sta**	Deletes the startup configuration file (startup-config)
reload	**rel**	Performs a software reboot
	Global Settings	
hostname R1	**ho**	Sets the device host name to R1
banner motd #XYZ#	**ban m**	Sets the banner message of the day, which is displayed at login, to XYZ
enable secret itsasecret	**ena s**	Sets the privileged mode encrypted password to itsasecret
	Line Settings	
line con 0	**lin c**	Enters line config mode for console port 0
line aux 0	**lin a**	Enters line config mode for auxiliary port 0
line vty 0 4	**lin v**	Enters line config mode for VTY lines 0 through 4
login	**login**	Allows login to a line in line config mode
password	**pas**	Sets line login password in line config mode

Full Command / Example	Abbreviation	Purpose / Mode
	Interface Settings	
interface S0/0/0	**int**	Enters interface config mode for interface Serial 0/0/0 (specifies the interface as type/number)
description XYZ	**des**	Specifies a description for the interface as XYZ (in interface config mode)
ip address 192.168.1.1 255.255.255.0	**ip add**	Specifies an IP address and subnet mask for the interface (in interface config mode)
no shutdown	**no sh**	Brings up the interface (in interface config mode). Use **shutdown** to disable the interface.
clock rate 64000	**clo r**	Sets the clock rate for a serial interface, with a DCE cable connected, to 64000 (in interface config mode)
encapsulation ppp	**enc**	Specifies the encapsulation for the interface as ppp (in interface config mode)
	Routing Settings	
router rip	**router**	Enters router config mode for the RIP routing protocol
network 172.16.0.0	**net**	Specifies network 172.16.0.0 to be advertised by RIP (in RIP router config mode)
ip route 172.16.0.0 255.255.0.0 S0/0/0	**ip route**	Specifies a static route to network 172.16.0.0 through exit interface Serial 0/0/0
ip route 0.0.0.0 0.0.0.0 192.168.2.2	**ip route**	Specifies a static default route through next-hop IP address 192.168.2.2

Example 2-10 shows the configuration commands used to configure the R1 router in Figure 2-18. Refer to Example 2-1 to see the results of the commands as displayed with the **show running-config** command. The resulting running configuration frequently has a number of commands inserted automatically by the IOS that were not entered during the configuration process.

Example 2-10 Router R1 Basic Configuration Commands

```
Router> enable
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# banner motd %Unauthorized Access Prohibited%
R1(config)# enable secret class
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line aux 0
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

```
R1(config-line)# exit
R1(config)# no ip domain-lookup

R1(config)#
R1(config)# interface FastEthernet0/0
R1(config-if)# description LAN 192.168.1.0 default gateway
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description WAN link to R2
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# encapsulation ppp
R1(config-if)# clock rate 64000
R1(config-if)# no shutdown
R1(config-if)#
R1(config-if)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
```

It is common to copy the running configuration of a device, such as the R1 router, and paste it into a text editor file for backup or use it as a starting point for modification. The text file can then be edited as necessary so that it can be used to reconfigure the router or configure another router.

Note

After a device has been configured, it is critical to copy the running configuration to the startup configuration using the **copy run start** command. Otherwise, changes will be lost if the router is restarted using the **reload** command or if it loses power.

Packet Tracer Activity

Basic Router Configuration Using CLI (2.3.3)

In this activity, you practice basic router configuration and verification commands. Use file d3-233.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

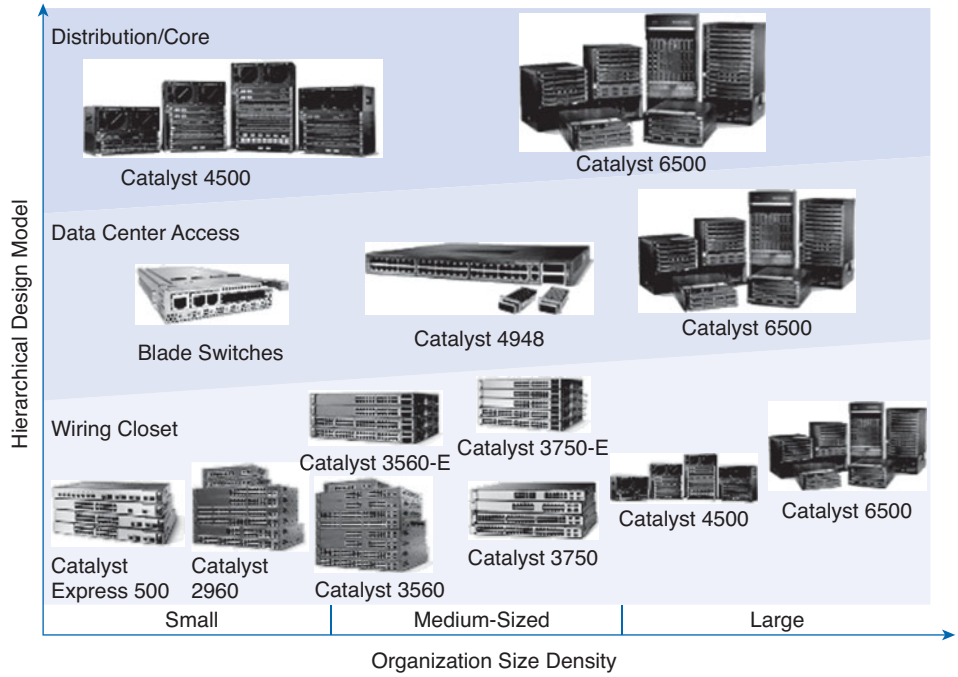
Switch Hardware

Although all three layers of the hierarchical design model contain switches and routers, the access layer generally has more switches. The main function of switches is to connect hosts such as end-user workstations, servers, IP phones, web cameras, access points, and routers. This means that there are many more switches in an organization than routers.

As shown in Figure 2-18, switches come in many form factors:

- Small standalone models sit on a desk or mount on a wall.
- Integrated routers include a switch built into the chassis that is rack mounted.
- High-end switches mount into a rack and are often a chassis-and-blade design to allow more blades to be added as the number of users increases.

Figure 2-18 Switch Classes and Form Factors



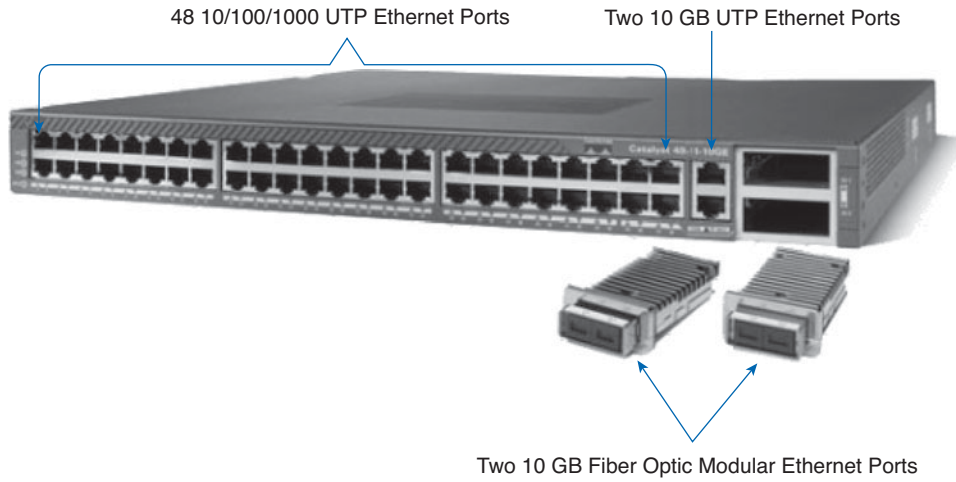
High-end enterprise and service provider switches support ports of varying speeds, from 100 MB to 10 GB.

An enterprise switch in an MDF connects other switches from IDFs using Gigabit fiber or copper cable. An IDF switch typically needs both RJ-45 Fast Ethernet ports for device connectivity and at least one Gigabit Ethernet port (copper or fiber) to uplink to the MDF switch. Some high-end switches have modular ports that can be changed if needed. For example, it might be necessary to switch from multimode fiber to single-mode fiber, which would require a different port.

Like routers, switch ports are also designated using the controller/port or controller/slot/port convention. For example, using the controller/port convention, the first Fast Ethernet port on a switch is numbered as Fa0/1 (controller 0 and port 1). The second is Fa0/2. The first port on a switch that uses controller/slot/port is Fa0/0/1. Gigabit ports are designated as Gi0/1, Gi0/2, and so on.

Port density on a switch is an important factor. In an enterprise environment where hundreds or thousands of users need switch connections, a switch with a 1RU height and 48 ports has a higher port density than a 1RU 24-port switch. Figure 2-19 shows a Cisco Catalyst 4948 switch with 48 access ports capable of operating at 10 Mbps (regular Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet). In addition, it has two built-in 10-Gbps UTP ports and two modular ports that can accept various fiber-optic Ethernet interfaces, including 10-Gbps multimode or single-mode.

Figure 2-19 Ethernet Switch Ports: Built-in and Modular



Basic Switch CLI Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status. These commands can be divided into several categories, as shown in Table 2-2.

Table 2-3 lists these commands with common options used and the minimum abbreviation allowable, along with a description of their function and key information displayed.

Table 2-3 Common Switch show Commands

Full Command	Abbreviation	Purpose / Information Displayed
	General Use	
show running-config	**sh run**	Displays current config running in RAM. Includes host name, passwords, interface IP addresses (if present), port numbers, and characteristics (duplex/speed).
show startup-config	**sh star**	Displays backup config in NVRAM. Can be different if running config has not been copied to backup.
show version	**sh ve**	Displays IOS version, ROM version, switch uptime, system image file name, boot method, number and type of interfaces installed, and amount of RAM, NVRAM, and flash. Also shows the Configuration register.
	Interface / Port Related	
show interfaces (type and number)	**sh int f0/1**	Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics.
show ip interface brief	**sh ip int br**	Displays all interfaces with IP address with interface status (up/down/admin down) and line protocol status (up/down).

Full Command	Abbreviation	Purpose / Information Displayed
	Interface / Port Related	
show port-security	**sh por**	Displays any ports where security has been activated, along with max address allowed, current count, security violation count, and action to take (normally shut-down).
show mac-address-table	**sh mac-a**	Displays all MAC addresses the switch has learned, how learned (dynamic/static), the port number, and VLAN the port is in.
	Connectivity Related	
show cdp neighbors (detail)	**sh cdp ne**	Displays information on directly connected devices, including device ID (host name), local interface where device is connected, capability (R=router, S=switch), platform (e.g., WS-2950-2), and port ID of remote device. The detail option provides the IP address of the other device as well as the IOS version.
show sessions	**sh ses**	Displays Telnet sessions (VTY) with remote hosts. Displays session number, host name, and address.
show ssh	**sh ssh**	Displays SSH server connections with remote hosts.
ping (ip / hostname)	**p**	Sends five ICMP echo requests to an IP address or host name (if DNS is available) and displays the min/max and avg time to respond.
traceroute (ip / hostname)	**tr**	Sends echo request with varying TTL. Lists routers (hops) in path and time to respond.

The same in-band and out-of-band management techniques that apply to routers also apply to switch configuration.

The following examples display **show** command output for the S1 model 2960 switch in the Figure 2-18 network topology. This switch has 24 10/100 Ethernet UTP ports and two Gigabit ports. Port Fa0/3 has a host attached and port security has been set. If the **mac-address sticky** option is used with the **switchport port-security** command, the running configuration is automatically updated when the MAC address of the host attached to that port is learned.

Example 2-11 presents the **show running-config** output for S1.

Example 2-11 S1 show running-config Command Output

```
S1# show running-config

< output omitted >
Building configuration...
Current configuration : 1373 bytes
!
version 12.2
```

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
enable secret 5 $1$9y6K$CE6oM7XmLRg6ISQPAJOk10
no ip domain-lookup
spanning-tree mode pvst
!
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000b.db04.a5cd
!
< Output for ports Fa0/4 through Fa0/21 omitted >
!
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
!
interface GigabitEthernet0/1
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
banner motd ^CUnauthorized Access Prohibited^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Example 2-12 presents the **show version** command output for S1.

Example 2-12 S1 show version Command Output

```
S1#  show version

< output omitted >
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE3, RELEASE SOFTWARE
  (fc2)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 13:57 by myl
Image text-base: 0x00003000, data-base: 0x00AA3380

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

S1 uptime is 55 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-25.SEE3/c2960-lanbase-mz.122-25.SEE3.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision D0) with 61440K/4088K bytes of memory.
Processor board ID FOC1129X56L
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1D:46:35:0C:80
Motherboard assembly number     : 73-10390-04
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC11285HJ7
Power supply serial number      : AZS11280656
Model revision number           : D0
Motherboard revision number     : A0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1129X56L
Top Assembly Part Number        : 800-27221-03
Top Assembly Revision Number    : A0
Version ID                      : V03
CLEI Code Number                : COM3L00BRB
Hardware Board Revision Number  : 0x01

Switch   Ports  Model              SW Version              SW Image
------   -----  -----              ----------              ----------
*    1   26     WS-C2960-24TT-L    12.2(25)SEE3            C2960-LANBASE-M

Configuration register is 0xF
```

Example 2-13 presents the **show interfaces** command output for S1.

Example 2-13 S1 show interfaces Command Output

```
S1# show interfaces

< output omitted >
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001d.4635.0cc0 (bia 001d.4635.0cc0)
  Internet address is 192.168.1.5/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:09, output 00:47:51, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     216 packets input, 23957 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     25 packets output, 5161 bytes, 0 underruns
     0 output errors, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001d.4635.0c81 (bia 001d.4635.0c81)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:28, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     564 packets input, 57713 bytes, 0 no buffer
     Received 197 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 195 multicast, 0 pause input
     0 input packets with dribble condition detected
     2515 packets output, 195411 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
< output omitted >
```

Example 2-14 presents the **show ip interface brief** command output for S1.

Example 2-14 S1 show ip interface brief Command Output

```
S1# show ip interface brief

< output omitted >
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.5     YES manual up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  up                    up
< Output for ports Fa0/4 through Fa0/21 omitted >
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
```

Example 2-15 presents the **show mac-address-table** output for S1.

Example 2-15 S1 show mac-address-table Command Output

```
S1# show mac-address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
< Output for some CPU ports omitted >
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    000b.db04.a5cd    DYNAMIC     Fa0/3
   1    001b.5325.256e    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 22
```

Example 2-16 presents the **show port-security** output for S1.

Example 2-16 S1 show port-security Command Output

```
S1# show port-security

Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
------------------------------------------------------------------------------
      Fa0/9          1            1               0         Shutdown
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Example 2-17 presents the **show cdp neighbors** output for S1.

Example 2-17 S1 show cdp neighbors Command Output

```
S1# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce       Holdtme    Capability    Platform   Port ID
R1                 Fas 0/1            122           R S I     1841       Fas0/0
```

A basic switch configuration includes the host name for identification, passwords for security, and assignment of IP addresses for connectivity. In-band access requires the switch to have an IP address.

Verify and save the switch configuration using the **copy running-config startup-config** command. To clear the switch configuration, use the **erase startup-config** command and then the **reload** command. You might also need to erase any VLAN information using the **delete flash:vlan.dat** command. Table 2-4 shows common IOS commands used to configure switches. Also listed is a short abbreviation, the purpose of the command, and the required mode to execute the command.

Table 2-4 Common Switch Configuration Commands

Full Command / Example	Abbreviation	Purpose / Mode
	Configuration Management	
enable	**en**	Changes from user EXEC mode (>) to privileged EXEC mode (#)
configure terminal	**conf t**	Changes from privileged EXEC mode to global configuration mode
copy running-config startup-config	**cop r s**	Copies the running configuration from RAM to the startup configuration file in NVRAM
erase startup-config	**era sta**	Deletes the startup configuration file (startup-config)
delete vlan.dat	**del**	Removes the VLAN configuration from the switch
reload	**rel**	Performs a software reboot
	Global Settings	
hostname S1	**ho**	Sets the device host name to S1
banner motd #XYZ#	**Ban m**	Sets the banner message of the day, which is displayed at login, to XYZ
enable secret itsasecret	**Ena s**	Sets the privileged mode encrypted password to itsasecret
ip default gateway	**ip def ga**	Specifies the router gateway the switch will use (in global config mode)

Full Command / Example	Abbreviation	Purpose / Mode
	Line Settings	
line con 0	**Lin c**	Enters line config mode for console port 0
line vty 0 4	**Lin v**	Enters line config mode for VTY lines 0 through 4
login	**login**	Allows login to a line in line config mode
password	**Pas**	Sets line login password in line config mode
	Interface Settings	
interface vlan 1	**Int**	Enters interface config mode for logical interface management VLAN 1 (default native VLAN)
ip address 192.168.1.1 255.255.255.0	**ip add**	Specifies an IP address and subnet mask for the interface (in VLAN interface config mode)
interface f0/1	**Int**	Enters interface config mode for physical port Fast Ethernet 0/1
speed 100	**Spe**	Sets the speed of the interface at 100 Mbps (in interface config mode)
duplex full	**Du**	Sets the duplex mode of the interface to full (in interface config mode)
switchport mode access	**switch m a**	Sets the switch port to access mode unconditionally (in interface config mode)
switchport port-security	**switch po**	Sets basic default port security on a port (in interface config mode)

Example 2-18 shows the configuration commands used to configure the S1 switch in Figure 2-18. Refer to Example 2-11 to see the results of the commands as displayed with the **show running-config** command. As with the router configuration, the resulting running configuration frequently has a number of commands inserted automatically by the IOS that were not entered during the configuration process.

Example 2-18 Switch S1 Basic Configuration Commands

```
Switch> enable
Switch# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# banner motd %Unauthorized Access Prohibited%
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 4
S1(config-line)# password cisco
```

```
S1(config-line)# login
S1(config-line)# line vty 5 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
1(config)# no ip domain-lookup
S1(config)# interface FastEthernet0/3
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# interface Vlan1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-line)# exit
S1(config)# ip default-gateway 192.168.1.1
```

Basic Switch Configuration Using CLI (2.3.5)

In this activity, you configure a switch in a switching environment. Use file d3-235.pka on the CD-ROM that accompanies this book to perform this interactive activity using Packet Tracer.

Lab 2-1: Configuring Basic Routing and Switching (2.3.5)

In this lab, you will connect and configure a multirouter network. Refer to the hands-on lab in Part II of this *Learning Guide*. You can perform this lab now or wait until the end of the chapter.

Summary

Network infrastructure diagrams document devices in a network. Network documentation includes the business continuity plan, business security plan, network maintenance plan, and service-level agreements.

The enterprise NOC manages and monitors all network resources. End users connect to the network through access layer switches and wireless APs in the IDF, and PoE provides power to devices over the same UTP cable that carries data.

The enterprise edge provides Internet access and service for users inside the organization. Edge devices provide security against attacks.

The POP at the edge provides a direct link to an SP or ISP and connects remote sites. The POP contains a demarc line of responsibility between the service provider and customer. Services are brought to the enterprise POP by copper wires or fiber-optic cable.

Distribution layer routers move packets between locations and the Internet and can control broadcasts. Routers and switches use in-band and out-of-band management.

Activities and Labs

This summary outlines the activities and labs you can perform to help reinforce important concepts described in this chapter. You can find the activity and Packet Tracer files on the CD-ROM accompanying this book. The complete hands-on labs appear in Part II.

Interactive Activities on the CD-ROM:

Interactive Activity 2-1: Matching Network Information to Documentation Type (2.1.1)

Interactive Activity 2-2: Placing MDFs, IDFs, and Cabling (2.1.3)

Interactive Activity 2-3: Specifying Components to Bring Service to the Internal Network (2.2.3)

Interactive Activity 2-4: Matching the Command to the Information Needed (2.3.2)

Packet Tracer Activities on the CD-ROM:

Basic Router Configuration Using CLI (2.3.3)

Basic Switch Configuration Using CLI (2.3.5)

Hands-on Labs in Part II of this book:

Lab 2-1: Configuring Basic Routing and Switching (2.3.5)

Check Your Understanding

Complete all the review questions listed here to check your understanding of the topics and concepts in this chapter. Appendix A, "Check Your Understanding and Challenge Questions Answer Key," lists the answers.

1. Draw a line from each term on the left to its correct description on the right. (Not all terms are used.)

Term	Description
POP	Maliciously prevents access to network resources by legitimate users
VPN	Boundary that designates responsibility for equipment maintenance and troubleshooting
DoS	Physical link to outside networks at the enterprise edge
CPE	An area of the network accessible to external users and protected by firewalls
DM	A telecommunications room to which IDFs connect
Demarc	A method of providing electrical power to Ethernet end devices
	Allows remote workers to access the internal network securely
	Equipment located at the customer facility

2. What information can you find by using the **show mac-address-table** command on a Cisco Catalyst switch?

   A. The MAC address of the console interface on the Catalyst switch
   B. The MAC addresses of the hosts connected to the switch ports
   C. The IP addresses of directly connected network devices
   D. The mapping between MAC address and IP address for network hosts

3. While troubleshooting a network problem, the network administrator issues the **show version** command on a router. What information can be found using this command?

   A. The amount of NVRAM, DRAM, and flash memory installed on the router
   B. The bandwidth, encapsulation, and I/O statistics on the interfaces
   C. Differences between the backup configuration and the current running configuration
   D. The version of the routing protocols running on the router

4. After gathering a thorough list of network applications, the traffic generated by these applications, and the priority of this traffic, a network engineer wants to integrate this information into a single document for analysis. How can this be accomplished?

   A. Create a physical topology map of the network and annotate it with the network application data.
   B. Create a logical topology map of the network and annotate it with the network application data.
   C. Create a blueprint of the facility, including network cabling and telecommunications rooms, and annotate it with the network applications data.
   D. Take a photograph of the facility, and annotate it with the network application data.

5. One evening a network administrator attempted to access a recently deployed website and received a "Page not found" error. The next day the administrator checked the web server logs and noticed that during the same hour that the site failed to load, there were hundreds of requests for the website home page. All the requests originated from the same IP address. Given this information, what might the network administrator conclude?

   A. It is normal web-surfing activity.
   B. It is likely that someone attempted a DoS attack.
   C. The link to the website does not have enough capacity and needs to be increased.
   D. The web server was turned off and was not able to service requests.

6. What type of media typically connects an MDF switch to an IDF switch in another building with an Ethernet network?

   A. Fiber-optic
   B. Coaxial cable
   C. Unshielded twisted-pair
   D. Shielded twisted-pair

7. Which of the following devices can receive power over the same twisted-pair Ethernet cable that carries data? (Choose three.)

   A. Wireless access points
   B. Monitors
   C. Web cameras
   D. IP phones
   E. Network switches
   F. Laptops

8. Indicate which type of hardware each characteristic describes by marking with an R (router) or S (switch).

   A. Defines broadcast domains
   B. Connects IP phones and access points to the network
   C. Enhances security with ACLs
   D. Interconnects networks
   E. Appears more commonly at the access layer
   F. Connects hosts to the network
   G. First Fast Ethernet interface designation is Fa0/0
   H. First Fast Ethernet interface designation is Fa0/1

9. Which of the following protocols are normally used to access a Cisco router for in-band management? (Choose two.)

   A. ARP
   B. SSH
   C. FTP
   D. SMTP
   E. Telnet

10. A network analyst is documenting the existing network at ABC-XYZ Corporation. The analyst decides to start at the core router to identify and document the Cisco network devices attached to the core. Which command executed on the core router provides the required information?

A. **show version**
B. **show ip route**
C. **show tech-support**
D. **show running-config**
E. **show cdp neighbors detail**

11. A network administrator suspects that there is a problem with the configuration of the RIP routing protocol. She investigates the interfaces and finds that all interfaces are up/up. Which of the following commands could help to identify the problem? (Choose two.)

A. **show cdp neighbors**
B. **show ip route**
C. **show sessions**
D. **show ip protocols**
E. **show version**

12. As a network technician, you are troubleshooting a router configuration. You want to get a concise display of the status of the router interfaces. You also want to verify the IP address of each interface and the subnet mask in slash format (/XX). Which command would you use?

A. **show protocols**
B. **show ip route**
C. **show running-config**
D. **show ip protocols**
E. **show ip interfaces brief**

13. What is the correct sequence of devices and connections for providing a T1 service to an organization's end user? Number each term in the proper sequence.

A. DMZ router
B. T1 circuit line
C. Internal switch
D. CSU/DSU
E. DMZ switch
F. Punchdown block
G. Internal router
H. Service provider
I. End-user PC

14. Which of the following is not a type of network protection device or technique to help security?

A. DoS
B. Firewall
C. ACL
D. IDS
E. IPS
F. DMZ
G. VPN

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in Appendix A.

1. Routers R1 and R2 are connected by a serial link. As a network administrator, you entered the following commands to configure the Serial 0/0/0 interface on Router R1. From Router R1 you are unable to ping the R2 S0/0/0 interface. What interface-related issues could be causing the problem, and what commands would you use on which routers to help isolate the problem?

```
R1(config-if)# interface Serial0/0/0
R1(config-if)# description WAN link to R2
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# encapsulation ppp
R1(config-if)# clock rate 64000
R1(config-if)# no shutdown
```

2. ISP or WAN Link Investigation Interview Activity (optional)

   In this activity, you will talk with your instructor or a network administrator at the institution where you work or other organization. Use the following form to ask a few questions to learn more about the organization's ISP service or service provider being used for a WAN connection.

   Organization: _____

   Person's name: _____

   Position/title: _____

   ISP or service provider name: _____

   Internet or WAN: _____

   Connection type/speed (DSL, cable, T1/E1, fractional T1, Frame Relay, and so on):

   _____

   CPE device (CSU/DSU, cable modem, DSL modem, and so on): _____

   If CSU/DSU, location of device (standalone or integrated into router):

   _____

   Location of POP: _____

   Is there a DMZ? _____

   Is there an SLA? _____

This page intentionally left blank

Index

NUMBERS

A

B

C

D

E

F

G - H

I

J - K - L

M

N

O

P

Q - R

S

T

U - V

W - X - Y - Z