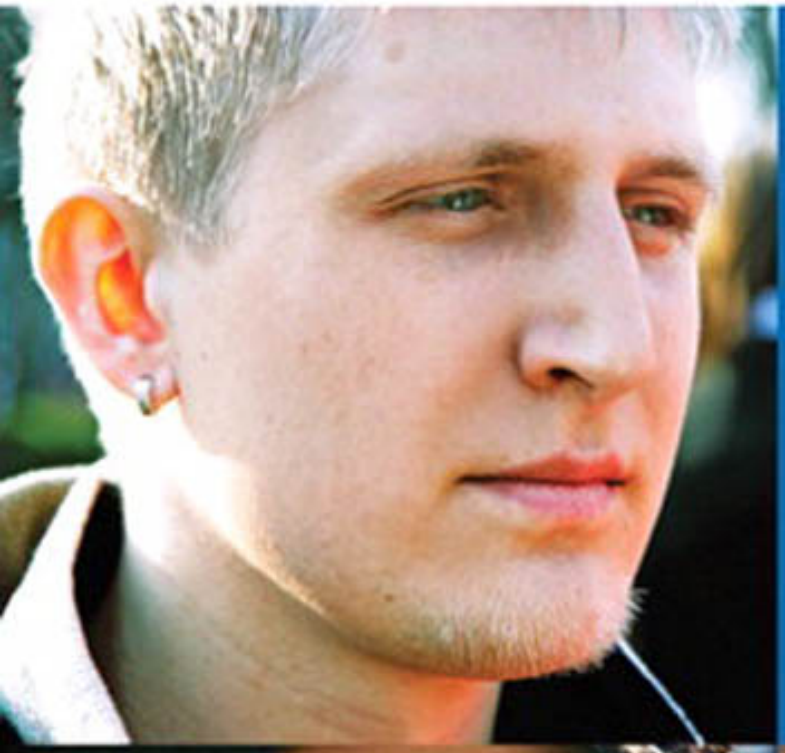


Working at a Small-to-Medium Business or ISP

CCNA Discovery Learning Guide

Allan Reid • Jim Lorenz

Cisco | Networking Academy
Mind Wide Open

Working at a Small-to-Medium Business or ISP

CCNA Discovery Learning Guide

Allan Reid

Jim Lorenz

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Working at a Small-to-Medium Business or ISP

CCNA Discovery Learning Guide

Allan Reid and Jim Lorenz

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

Printed in the United States of America

First Printing April 2008

Library of Congress Cataloging-in-Publication Data

Reid, Allan.

Working at a small-to-medium business or ISP : CCNA discovery learning guide / Allan Reid, Jim Lorenz.

p. cm.

Includes index.

ISBN 978-1-58713-210-0 (pbk. w/cd)

1. Computer networks—Textbooks. 2. Computer networks—Management—Textbooks. 3. Local area networks (Computer networks)—Textbooks. 4. Business enterprises—Computer networks—Textbooks. 5. Internet service providers—Textbooks. I. Lorenz, Jim. II. Title.

TK5105.5.R4464 2008

004.6—dc22

2008015723

ISBN-13: 978-1-58713-210-0

ISBN-10: 1-58713-210-9

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

Senior Project Editor
Tonya Simpson

Copy Editor
Gayle Johnson

Technical Editors
Bernadette O'Brien, Elaine Horn, William Shurbert, Glenn Wright

Editorial Assistant
Vanessa Evans

Book Designer
Louisa Adair

Composition
Louisa Adair

Indexer
Tim Wright

Proofreader
Molly Proue

Warning and Disclaimer

This book is designed to provide information about the *Working at a Small-to-Medium Business or ISP CCNA Discovery* course. Every effort has been made to make this book as complete and 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 of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about 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 be 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. He is a professor in the Information and Communications Engineering Technology department and is 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 developing and implementing numerous certificate, diploma, and degree programs in networking. Allan also is a curriculum developer for the Cisco Networking Academy. Outside his academic responsibilities, he has been active in the computer and networking fields for more than 25 years. Currently he is 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, he 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. He 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.

About the Technical Reviewers

Bernadette O'Brien has been teaching in the Cisco Networking Academy in Schenectady, New York since 1998. Schenectady High School is a Regional Academy for CCNA and is a CATC for Sponsored Curriculum, which Bernadette coordinates. Bernadette received her BS degree from SUNY Buffalo and her MS degree in curriculum and instruction from SUNY Albany. She is also CCNA and CCAI certified. Bernadette and her husband and two children live in a Victorian village very near the Adirondack Mountains in upstate New York. They enjoy rehabbing their 120-year-old Victorian house, skiing, and hiking.

Elaine Horn, CCAI, has been teaching in the Cisco Networking Academy since 1998 at TRECA (http://www.treca.org) in Marion, Ohio. TRECA is a CATC for CCNA, a regional academy for Sponsored and Emerging Technologies Curriculum, and a local academy for CCNA. She is currently teaching and supporting academies in Ohio, Kentucky, and Michigan. Elaine received her BS degree in education and an MA in mathematics education from The Ohio State University. She has also coordinated the Skills Ohio Internetworking Competition and worked with Cisco Press as a technical editor for Academy-related materials.

Bill Shurbert is a professor of information technology at New Hampshire Technical Institute in Concord, New Hampshire. He holds a bachelor's degree in technical management from Southern New Hampshire University. He enjoys teaching the Cisco CCNA, Wireless, and IT Essentials classes. In his off time, you can find Bill and Joanne, his wife of more than 25 years, sailing the waters of Lake Winnipesaukee.

Glenn Wright, CCNA, CCAI, is the codirector of the Cisco Academy Training Center (CATC) in Fort Worth, Texas. He has a bachelor's degree in business education from the University of North Texas and 22 years of experience in computer education. He has been involved in many aspects of the Cisco Networking Academy since 1999. He serves the Academy as an instructor and supports the Regional Academies in Texas, Louisiana, Oklahoma, Arkansas, North Carolina, South Carolina, Virginia, and Tennessee. Glenn has also worked with the Academy Quality Assurance Team, reviewing and editing Academy curriculum and assessment. He has developed and edited Packet Tracer activities for the *Discovery* curriculum. He has also worked with Cisco Press as a technical editor for Academy-related materials.

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*

Acknowledgments

We want to thank Mary Beth Ray, Dayna Isley, and Drew Cupp with Cisco Press for their help and guidance in putting this book together. We also want to thank the technical editors, Bernadette O'Brien, Elaine Horn, Bill Shurbert, and Glenn Wright. Their attention to detail and suggestions made a significant contribution to the accuracy and clarity of the content.

We would also like 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 the user enters (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

The Cisco Networking Academy is a comprehensive e-learning program that 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, as well as enterprise and Internet service provider environments. The *Working at a Small-to-Medium Business or ISP* course is the second course in the curriculum.

This book is the official supplemental textbook for the second course in v4.1 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 as well as bonus activities.

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 book's study tools to help solidify your understanding of all the topics. In addition, this book includes the following:

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

Goals of This Book

First and foremost, by providing a fresh, complementary perspective on the online content, this book helps you learn all the required materials of the second 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 CCENT and CCNA exams.

Audience for This Book

This book's main audience is anyone taking the second *CCNA Discovery* course of the Networking Academy curriculum. Many Networking Academies use this textbook as a required tool in the course. Other Networking Academies recommend the *Learning Guides* as an additional source of study and practice materials.

Book Features

This book's educational features 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. 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, this icon helps you easily find this feature as you skim through the book.
- **Notes, tips, cautions, and warnings:** These are short sidebars that point out interesting facts, time-saving 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 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 it 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 260 computer and networking terms.

Practice

Practice makes perfect. This new *Learning Guide* offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction 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 answers for all the questions and explains each answer.
- **(New) Challenge questions and activities:** Additional—and more challenging—review questions and activities are presented at the end of the 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 perform with the Cisco Packet Tracer tool. Packet Tracer allows you to create a network, 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; the 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:** 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 you see its reference in the chapter, or you can wait until you have completed the chapter.

A Word About the 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. You can spend as much time as you like completing standard lab exercises using Packet Tracer, and you have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows you 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 to access 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 *CCNA Discovery* labs. Your instructor can download the CD files, burn a CD, and show you how to use the server. Hands-on labs that make use of the Discovery server are identified within the labs themselves.

After it is booted, the server provides many services to clients:

- Domain Name System
- 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 Working at a Small-to-Medium Business or ISP* course. The online curriculum has nine chapters for this course, so this book has 10 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 a slightly different order under each major heading. Additionally, the book occasionally uses different examples than the course. As a result, you 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 10 chapters:

- **Chapter 1, "The Internet and Its Uses,"** discusses the Internet—how it is evolving and how businesses and individuals make use of it. The importance of the ISP and standards in the continuing growth of the Internet is emphasized. This chapter focuses on the Internet infrastructure, including POPs, IXPs, and the types of devices ISPs use to provide services.
- **Chapter 2, "Help Desk,"** introduces the help desk and the various roles of help desk and installation technicians. It also describes the levels of support provided by these personnel. This chapter reviews the seven layers of the OSI model as they relate to help desk support and their use in troubleshooting network issues. Common tools and diagnostic procedures used by help desk technicians are examined, as well as on-site procedures used to resolve issues.
- **Chapter 3, "Planning a Network Upgrade,"** emphasizes the importance of proper planning when performing a network upgrade, including the use of a site survey, and it describes the steps involved in performing one. An overview of structured cabling is provided, along with the factors you must consider when upgrading LAN and internetworking devices.
- **Chapter 4, "Planning the Addressing Structure,"** describes how IP addressing is implemented in the LAN and compares classful and classless networks and subnets. This chapter explains the process for subnetting a network to allow for efficient use of available IP addresses. In addition, it describes how Network Address Translation (NAT) and Port Address Translation (PAT) are used in modern-day networks.
- **Chapter 5, "Configuring Network Devices,"** introduces the ISR and the methods available for configuring an ISR using both in-band and out-of-band techniques. This chapter introduces SDM and IOS commands and discusses how each is used to configure a Cisco device. The purpose and relationship of the device startup configuration and the running configuration are explained. In addition, Cisco Discovery Protocol (CDP) is introduced. Finally, the types of WAN connections available are discussed and compared in terms of cost and speed.

- **Chapter 6, "Routing,"** describes the purpose and function of dynamic routing and compares the characteristics of different types of routes. The main interior gateway protocols and their key features are introduced, as is the configuration process for RIPv2 dynamic routing, using Cisco IOS. In addition, exterior gateway routing protocols, such as BGP, are introduced, as are the steps required to configure BGP.
- **Chapter 7, "ISP Services,"** builds on network services introduced in the first *CCNA Discovery* course. It describes them in greater detail as they relate to those provided by an ISP. It describes the most common application layer protocols, such as HTTP, FTP, SMTP, IMAP, and POP3, as well as secure versions where they exist. This chapter also compares the UDP and TCP protocols and the types of traffic for which they are best suited. It also provides additional information on the Domain Name System (DNS) and how it functions.
- **Chapter 8, "ISP Responsibility,"** describes ISP security policies and procedures and the tools used in implementing security at the ISP. This chapter describes the monitoring and managing of the ISP, as well as the responsibilities of the ISP with regard to maintenance and recovery.
- **Chapter 9, "Troubleshooting,"** provides a review of Chapters 1 through 8, with a focus on identifying and correcting network problems using the OSI model as a basis. This chapter also provides guidance in preparing for the CCENT certification exam.
- In **Chapter 10, "Putting It All Together,"** you use what you have learned about computer hardware and software, wired and wireless networking components, protocols and applications, and techniques for securing a network to plan and implement a technical solution for a small business.

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

This book 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.
- **Appendix B, "Router Boot and Password Recovery Labs,"** provides several additional labs to help you learn how to control the router bootup process and troubleshoot configuration register boot problems. Password recovery procedures are also included.
- **Appendix C, "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.
- The **glossary** provides a compiled list of all the key terms that appear throughout this book, plus additional computer and networking terms.

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 files allow you 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.

- **CCENT Study Guides:** Referenced throughout Chapter 9, "Troubleshooting," the six Study Guides and one Preparation Guide provide you with a method to prepare to obtain your CCENT certification by organizing your review of the topics covered on the ICND1 exam.
- **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 not only for learning and studying the material but also for on-the-job success. Also included in this section is "A Guide to Using a Networker's Journal." It's a PDF booklet providing important insights into the value of using a professional journal, how to organize a journal, and some best practices for 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*: "Defining Yourself: Aptitudes and Desires" and "Making Yourself Indispensable."
- **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 gives you tips on how to tap into these resources for lifelong learning.

This page intentionally left blank

PART I

Concepts

This page intentionally left blank

CHAPTER 3

Planning a Network Upgrade

Objectives

After completing this chapter, you should be able to answer the following questions:

- Why is proper planning necessary when you perform a network upgrade?
- What is a site survey, and why is it necessary?
- What steps are involved in performing a site survey?
- What is structured cabling?
- What factors must you consider when upgrading LAN and internetworking devices?

Key Terms

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

site survey 50

SWOT 55

failure domain 64

Cisco IOS 65

Integrated Services Router (ISR) 65

Fault tolerance 68

As businesses grow and evolve, they may outgrow their existing network and require a network upgrade. To help ensure a smooth transition, a careful look at both the current network and the new network requirements is necessary. This will help determine what new equipment and configurations are necessary to ensure that the new network fully supports both the current and future needs of the company or organization.

Part II of this book includes the corresponding labs for this chapter.

Common Issues

When a small company grows rapidly, the original network that supported the company often cannot keep pace with the expansion. Employees at the company may not realize how important it is to properly plan for network upgrades. In many cases, the business may just add various network hardware devices, of varying quality, from different manufacturers, and different network connection technologies, to connect new users. Often this causes a degradation in the quality of the network as each new user or device is added. If this continues, at some point the network is unable to properly support the types and level of network traffic that the users generate. Only when the network starts to fail do most small businesses look for help to redesign the network. An ISP or managed service provider may be called in to provide advice and to install and maintain the network upgrade.

Before a network upgrade can be properly designed, an onsite technician is dispatched to perform a site survey to document the existing network structure. It is also necessary to investigate and document the physical layout of the premises to determine where new equipment can be installed.

Site Survey

A ***site survey*** can give the network designer a substantial amount of information and create a proper starting point for the project. It shows what is already on site and indicates what is needed. A sales representative may accompany the technician to the site to interview the customer as well. A proper site survey gathers as much information as possible about the current business and its projected growth. This information is gathered from different people in an attempt to accurately forecast the current and future network requirements. Table 3-1 lists the information sought in a site survey.

Table 3-1 Site Survey Information

Category	Information Sought
Number of users and types of equipment	How many network users, printers, and servers will the network support? To determine the number of network users the network must support, be sure to consider how many users will be added over the next 12 months, and how many network printers and network servers the network has to accommodate.
Projected growth	What is the expected growth in the company or organization? Will the company be hiring new employees who must be provided with access to network resources? Will a new branch office be opened that will require connectivity? A network is a long-term investment. Planning for future growth now can save a great deal of time, money, and frustration in the future.

Category	Information Sought
Current Internet connectivity	How does your business connect to the Internet? Does the ISP provide the equipment, or do you own it? Often with a high-speed Internet connection such as DSL or cable, the service provider owns the equipment needed to connect to the Internet (for example, a DSL router or cable modem). If the connectivity is upgraded, the equipment that provides the connectivity may also need to be upgraded or replaced.
Application requirements	What applications does the network need to support? Do you require services for applications such as IP telephony or videoconferencing? It is important to identify the needs of particular applications, especially voice and video. These applications may require additional network device configuration and new ISP services to support the necessary quality.
Existing network infrastructure and physical layout	How many networking devices are installed in your network? What functions do they perform? Understanding the existing number and types of networking equipment that are currently installed is critical to being able to plan for the upgrade. It is also necessary to document any configurations that are loaded on the existing devices.
New services required	Will any new services be required either now or in the future? Will the company be implementing VoIP or videoconferencing technology? Many services require special equipment or configurations to optimize their performance. Equipment and configurations must take into account the possibility of new services to protect the investment and optimize performance.
Security and privacy considerations	Do you currently have a firewall in place to protect your network? When a private network connects to the Internet, it opens physical links to more than 50,000 unknown networks and all their unknown users. Although this connectivity offers exciting opportunities for information sharing, it also creates threats to information not meant for sharing. Integrated Services Routers (ISR) incorporate firewall features along with other functionality.
Wireless requirements	Would you like a wired, wireless, or wired plus wireless local-area network (LAN)? How big is the area that the wireless LAN (WLAN) must cover? It is possible to connect computers, printers, and other devices to the network using a traditional wired network (10/100 switched Ethernet), a wireless-only network (802.11x), or a combination of wired and wireless networking. Each wireless access point that connects the wireless desktop and wireless laptop computers to the network has a given range. To estimate the number of access points that are required, you must know the required coverage area and the physical characteristics of the location that the wireless network must cover.

continues

Table 3-1 Site Survey Information *continued*

Category	Information Sought
Reliability and uptime expectations	What is the real cost of downtime in the company or organization? How long an outage can the company tolerate before suffering serious financial or customer losses? Maintaining nearly 100% uptime requires complete redundancy in all equipment and services and is extremely expensive to implement. Networks must be designed to reflect the real need for uptime and system reliability. This level can be determined only through intensive investigation and discussions with all the business stakeholders.
Budget constraints	What is the budget for the network installation or upgrade? System performance, reliability, and scalability are all expensive to achieve. The project budget normally is the deciding factor as to what can and cannot be done. A complete cost-benefit analysis must be completed to determine which features and services are the most critical and which could be put off to a later date.

It is a good idea to obtain a floor plan if possible. If a floor plan is not available, you can draw a diagram indicating the size and locations of all rooms. An inventory of existing network hardware and software is also useful to provide a baseline of requirements.

You should be prepared for anything when doing the site survey. Networks do not always meet local electrical, building, or safety codes or adhere to standards. Sometimes networks grow haphazardly over time and end up being a mixture of technologies and protocols. When doing a site survey, be careful not to offend the customer by expressing an opinion about the quality of the existing installed network.

When the technician visits the customer premises, he or she should do a thorough overview of the network and computer setup. There may be some obvious issues, such as unlabeled cables, poor physical security for network devices, lack of emergency power, or lack of an uninterruptible power supply (UPS) for critical devices. These conditions should be noted on the technician's report, as well as the other requirements gathered from the survey and the customer interview. These deficiencies in the current network should be addressed in the proposal for a network upgrade.

When the site survey is complete, it is important that the technician review the results with the customer to ensure that nothing is missed and that the report has no errors. A summary of the questions asked and the information gathered can greatly simplify the review process. If the information is accurate, the report provides an excellent basis for the new network design.

Physical and Logical Topologies

Both the physical and logical topologies of the existing network need to be documented. A technician gathers the information during the site survey to create both a physical and logical topology map of the network. A physical topology, as shown in Figure 3-1, is the actual physical location of cables, computers, and other peripherals. A logical topology, as shown in Figure 3-2, documents the path that data takes through a network and the location where network functions, such as routing, occur.

Figure 3-1 Physical Topology

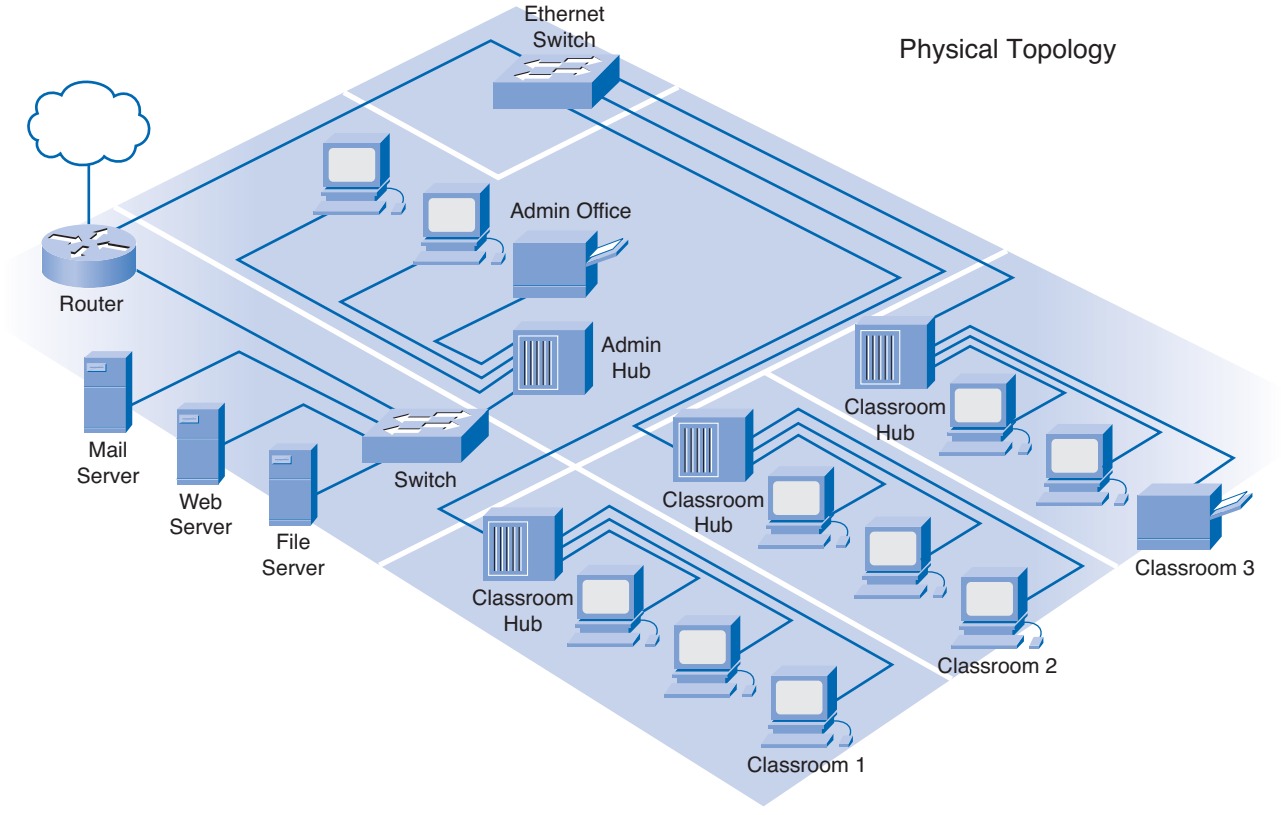
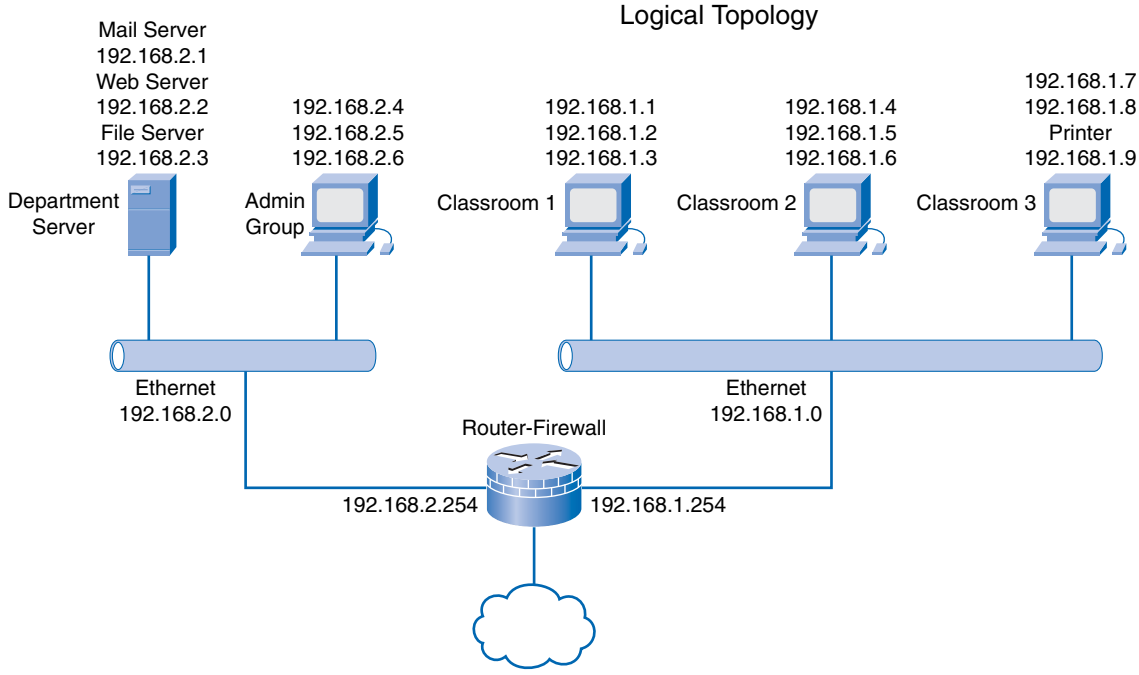


Figure 3-2 Logical Topology

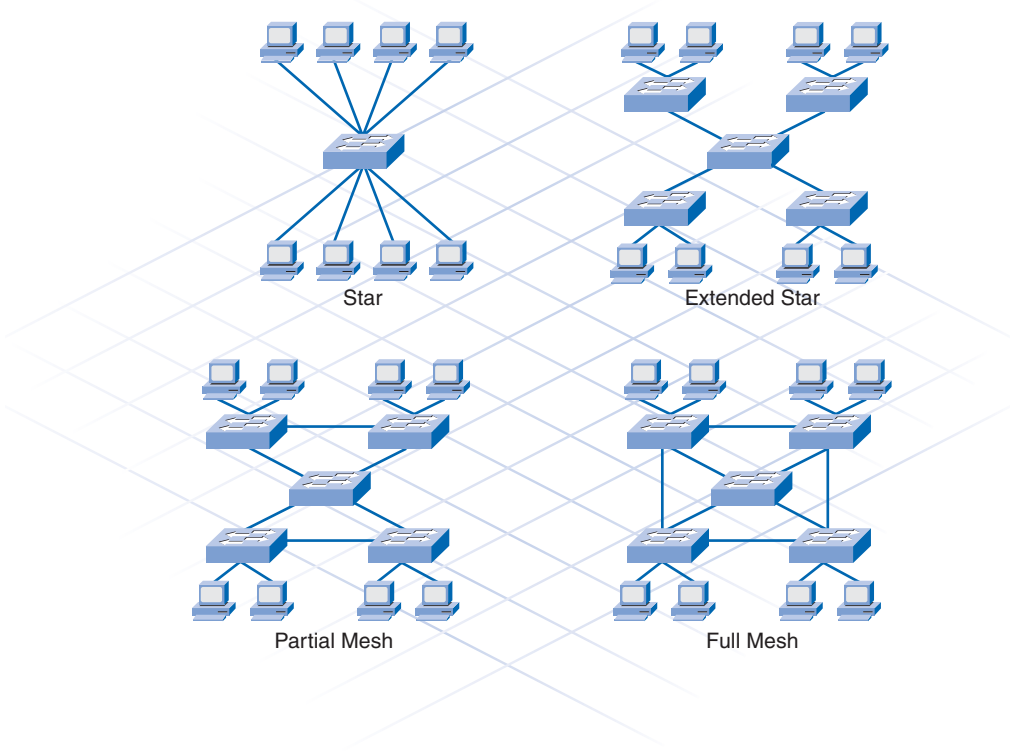


In a wired network, the physical topology map consists of the wiring closet, as well as the wiring to the individual end-user stations. In a wireless network, the physical topology consists of the wiring closet and any access points that may be installed. Because there are no wires, the physical topology contains the wireless signal coverage area.

The logical topology generally is the same for both a wired and wireless network. It includes the naming and Layer 3 addressing of end stations, router gateways, and other network devices, regardless of the physical location. It indicates the location of routing, network address translation, and firewall filtering.

Developing a logical topology requires understanding of the relationship between the devices and the network, regardless of the physical cabling layout. Several topological arrangements are possible. Examples include star, extended star, partial mesh, and full mesh topologies, as shown in Figure 3-3.

Figure 3-3 Common Topologies



Star Topologies

In a star topology, each device is connected via a single connection to a central point, which is typically a switch or a wireless access point. The advantage of a star topology is that if a single connecting device fails, only that device is affected. However, if the central device, such as the switch, fails, then all connecting devices lose connectivity.

An extended star is created when the central device in one star is connected to a central device of another star, such as when multiple switches are interconnected, or daisy-chained together.

Mesh Topologies

Most core layers in a network are wired in either a full mesh or a partial mesh topology. In a full mesh topology, every device has a connection to every other device. Although full mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly.

A partial mesh topology is used for larger installations. In a partial mesh topology, each device is connected to at least two other devices. This arrangement creates sufficient redundancy, without the complexity of a full mesh.

Implementing redundant links through partial or full mesh topologies ensures that network devices can find alternative paths to send data in the event of a failure.

Network Requirements Documentation

Along with creating the topology maps for the existing network, it is necessary to obtain additional information about the hosts and networking devices that are currently installed in the network. Record this information on a brief inventory sheet. In addition to currently installed equipment, document any planned growth that the company anticipates in the near future. This information helps the network designer determine what new equipment is required and the best way to structure the network to support the anticipated growth.

The inventory sheet of all the devices installed on the network includes the following:

- Device name
- Date of purchase
- Warranty information
- Location
- Brand and model
- Operating system
- Logical addressing information
- Connection information
- Security information

Packet Tracer Activity

Creating Network Diagrams (3.1.3)

In this activity, you create a logical diagram and inventory list for a network. Use file d2-313 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Planning the Network Upgrade

Extensive planning should go into a network upgrade. As with any project, a need is first identified, and then a plan outlines the upgrade process from beginning to end. A good project plan helps identify any strengths, weaknesses, opportunities, and threats. This is called a ***SWOT*** analysis. The plan should clearly define the tasks and the order in which tasks are completed.

Some common examples of good planning include

- Sports teams following game plans
- Builders following blueprints
- Ceremonies or meetings following agendas

Network Upgrades

A network that is a patchwork of devices strung together using a mixture of technologies and protocols usually indicates poor or no initial planning. These types of networks are susceptible to downtime and are extremely difficult to maintain and troubleshoot. Unfortunately, this type of network is often encountered as small businesses experience rapid, unexpected growth. Even larger organizations often experience unplanned growth in their networks when they acquire or merge with other organizations. Organizations that experience a controlled rate of growth can properly plan their network to avoid problems and give their users an acceptable level of service.

The planning of a network upgrade begins after the initial site survey and report are complete. It consists of five distinct phases:

- Phase 1: Requirements gathering
- Phase 2: Selection and design
- Phase 3: Implementation
- Phase 4: Operation
- Phase 5: Review and evaluation

The next sections describe each phase in greater detail.

Phase 1: Requirements Gathering

After all the information has been gathered from the customer and the site visit, the design team at the ISP analyzes the information to determine network requirements and then generates an analysis report. If insufficient information is available to properly determine the best network upgrade path to follow, this team may request additional information.

Phase 2: Selection and Design

When the analysis report is complete, devices and cabling are selected. The design team creates multiple designs and shares them with other members on the project. This allows team members to view the LAN from a documentation perspective and evaluate trade-offs in performance and cost. It is during this step that any weaknesses of the design can be identified and addressed. Also during this phase, prototypes are created and tested. A successful prototype is a good indicator of how the new network will operate.

Phase 3: Implementation

If the first two steps are done correctly, the implementation phase may be performed without incident. If tasks were overlooked in the earlier phases, they must be corrected during implementation. A good implementation schedule must allow time for unexpected events and also schedules events to keep disruption of the customer's business to a minimum. Staying in constant communication with the customer during the installation is critical to the project's success.

Phase 4: Operation

When the network implementation phase is complete, the network moves into a production environment. In this environment, the network is considered live and performs all the tasks it has been designed to accomplish. If all steps up to this point have been properly completed, very few unexpected incidents should occur when the network moves into the operation phase.

Phase 5: Review and Evaluation

After the network is operational, the design and implementation must be reviewed and evaluated against the original design objectives. This is usually done by members of the design team with assistance from the network staff. This evaluation includes costs, performance, and appropriateness for the environment. For this process, the following items are recommended:

- Compare the user experience with the goals in the documentation, and evaluate whether the design is right for the job.
- Compare the projected designs and costs with the actual deployment. This ensures that future projects will benefit from the lessons learned on this project.
- Monitor the operation, and record changes. This ensures that the system is always fully documented and accountable.

It is important that, at each phase, careful planning and review occur to ensure that the project goes smoothly and the installation is successful. Onsite technicians are often included in all phases of the upgrade, including planning. This allows them to gain a better understanding of the expectations and limitations of the network upgrade and to give the end users a much-improved level of service.

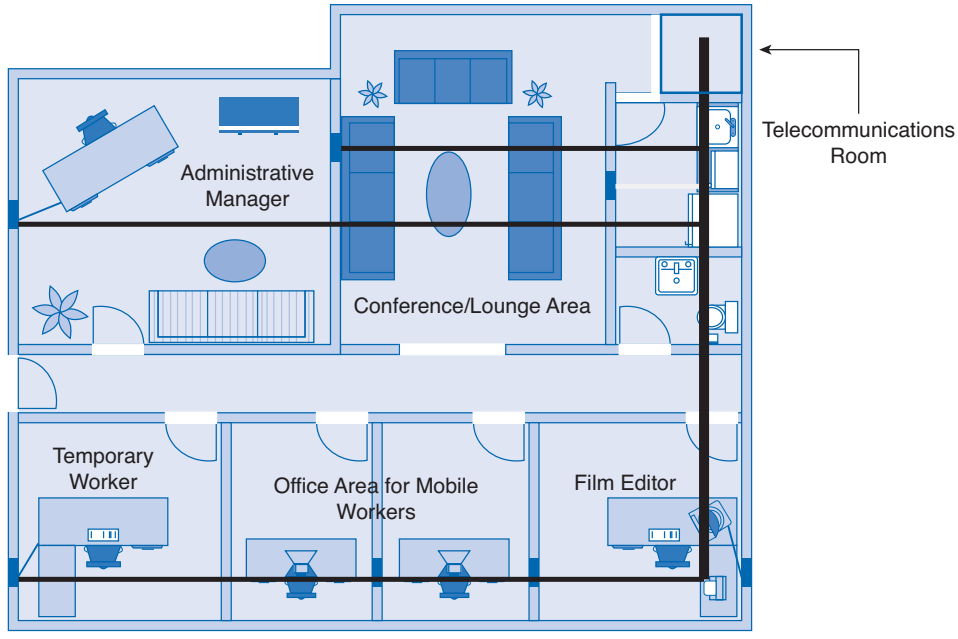
Activity 3-1: Network Planning Phases (3.2.1)

In this activity, you determine at which phase of the network planning process certain events occur. Use file d2ia-321 on the CD-ROM that accompanies this book to perform this interactive activity.

Physical Environment

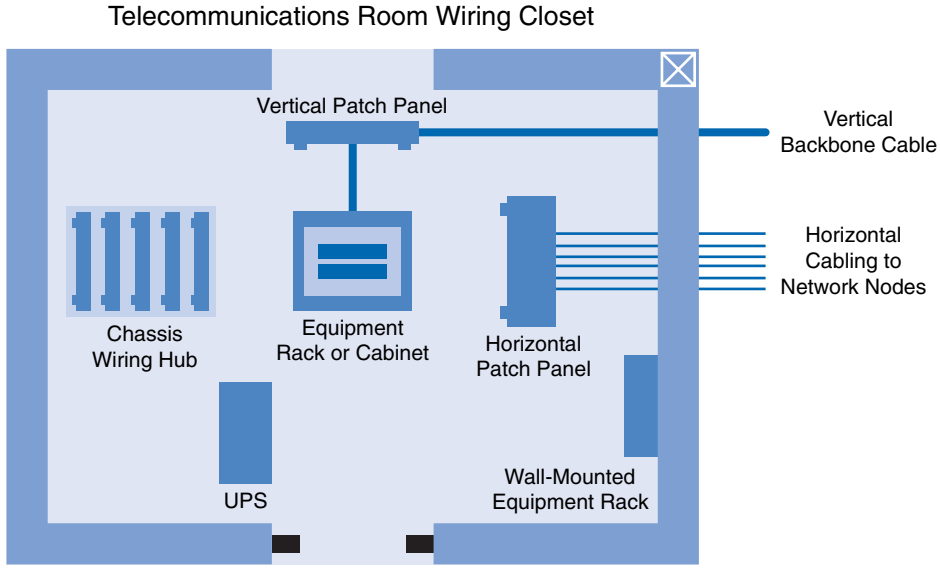
Before selecting equipment and determining the design of the new network, the network designer must examine the existing network facilities and cabling. This is part of the initial site survey. The facilities include the physical environment, the telecommunication room, and the existing network wiring. A telecommunications room or wiring closet in a small, single-floor network is usually called the main distribution facility (MDF). Figure 3-4 shows a small office environment with a single MDF.

Figure 3-4 Main Distribution Facility



The MDF typically contains many of the network devices, such as switches or hubs, routers, access points, and so on. It is where all the network cable is concentrated in a single point. Many times, the MDF also contains the ISP's point of presence (POP), where the network connects to the Internet through a telecommunications service provider. Figure 3-5 shows the layout of a typical MDF. If additional wiring closets are required, these are called intermediate distribution facilities (IDF). IDFs typically are smaller than the MDF and connect to the MDF with backbone cabling.

Figure 3-5 Typical MDF Layout



Tip

ISO standards refer to MDFs and IDFs using different terminology. MDFs and IDFs are sometimes called wiring closets. Because normally one MDF distributes telecommunication services to all areas of the building, MDFs are also called *building distributors*. Most environments have one or more IDFs on each floor of a building, so the ISO calls IDFs *floor distributors*.

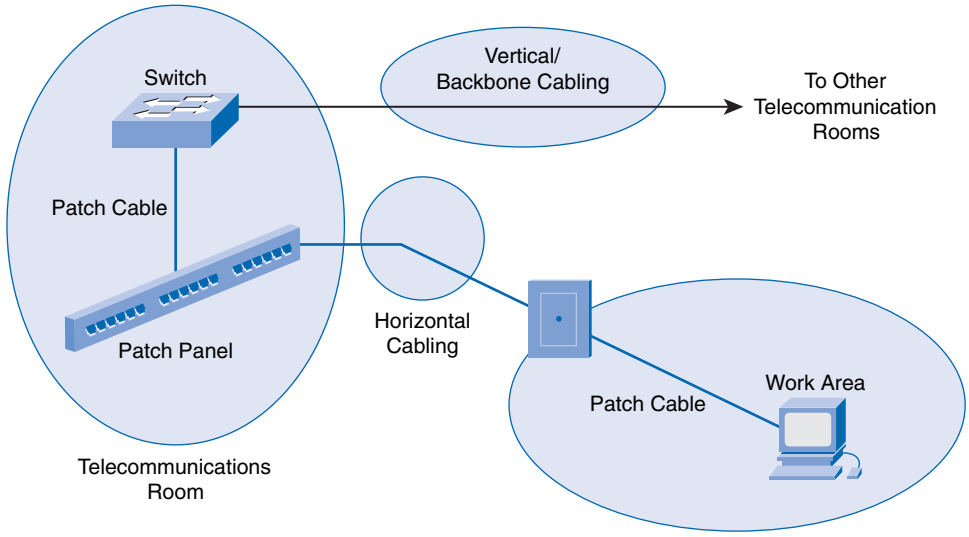
Many small businesses have no telecommunications room or closet. Network equipment may be located on a desk or other furniture, and wires could be just lying on the floor. This arrangement should be avoided. Network equipment must always be secure to protect data. Loose or improperly installed cables are prone to damage and also present a tripping hazard to employees. As a network grows, it is important to consider the telecommunications room as critical to the network's security and reliability.

Cabling Considerations

When the existing cabling is not up to specification for the new equipment, you must plan for and install new cable. The condition of the existing cabling can quickly be determined by a physical inspection of the network during the site visit. This inspection should reveal the type of cable installed as well as any issues, such as improper termination, that could degrade network performance. When planning the installation of network cabling, you must consider different physical areas, as shown in Figure 3-6:

- User work areas
- Telecommunications rooms
- Backbone area (vertical backbone cabling)
- Distribution area (horizontal cabling)

Figure 3-6 Cabling Areas



You have many different types of network cables to choose from; some are more common than others. Each type of cable is best suited to specific applications and environments. The most common type of LAN cable is unshielded twisted-pair (UTP). This cable is easy to install, is fairly inexpensive, and has a high bandwidth capability. For long backbone runs or runs between buildings, fiber-optic cable normally is installed. Coaxial cable is not typically used in LANs, but it is widely used in cable modem provider networks. Table 3-2 describes some of the more common types of network cables.

Table 3-2 Common Network Cables

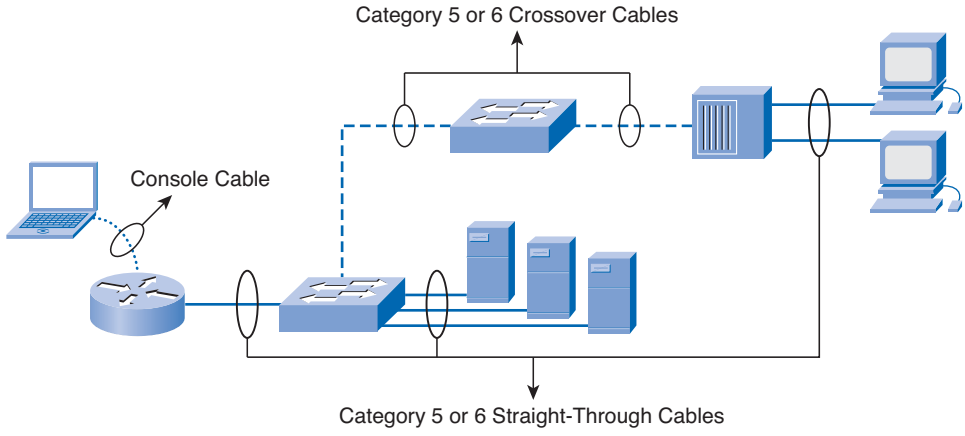
Cable Type	Characteristics
Shielded twisted-pair (STP)	Usually Category 5, 5e, or 6 cable that has a foil shielding to protect from outside electromagnetic interference (EMI). The distance limitation is approximately 328 feet (100 meters).
Unshielded twisted-pair (UTP)	Usually Category 5, 5e, or 6 cable. It does not provide extra shielding from EMI, but it is inexpensive. Cable runs should avoid electrically noisy areas. The distance limitation is approximately 328 feet (100 meters).
Coaxial	Has a solid copper core with several protective layers, including polyvinyl chloride (PVC), braided wire shielding, and a plastic covering. The distance limitation of several miles (kilometers) depends on the purpose of the connection.
Fiber-optic cable	A medium that is not susceptible to EMI and that can transmit data faster and farther than copper. Depending on the type of fiber optics, distance limitations can be several miles (kilometers).

Several organizations provide LAN cabling specifications. The Telecommunications Industry Association (TIA) and the Electronic Industries Association (EIA) worked together to provide the TIA/EIA cable specifications for LANs. Two of the most common TIA/EIA cable specifications are the 568-A and 568-B standards. Both of these standards typically use the same Category 5 or 6 cable, but with a different termination color code.

Three different types of UTP cables are commonly encountered in the network environment:

- Straight-through cables have the same pinout on both ends. They normally are used to connect dissimilar devices, such as a switch and a computer or a switch and a router.
- Crossover cables have the transmit pins on one end connected to the receive pins on the other end. This type of cable is used to connect like devices, such as two computers, two switches, or two routers. Crossover cables can also be used to connect a computer directly to a router interface.
- A console cable or a rollover cable has the pinouts on each end reversed. Normally it is used to connect the serial port of a computer to the console port of a router or switch to perform the initial configuration. Figure 3-7 shows typical uses of these cables.

Figure 3-7 Typical Uses of Cables



Another type of cable that is common in networks is a serial cable. A serial cable typically is used to connect the router to an Internet connection. This Internet connection may be to the phone company, the cable company, or a private ISP.

Structured Cable

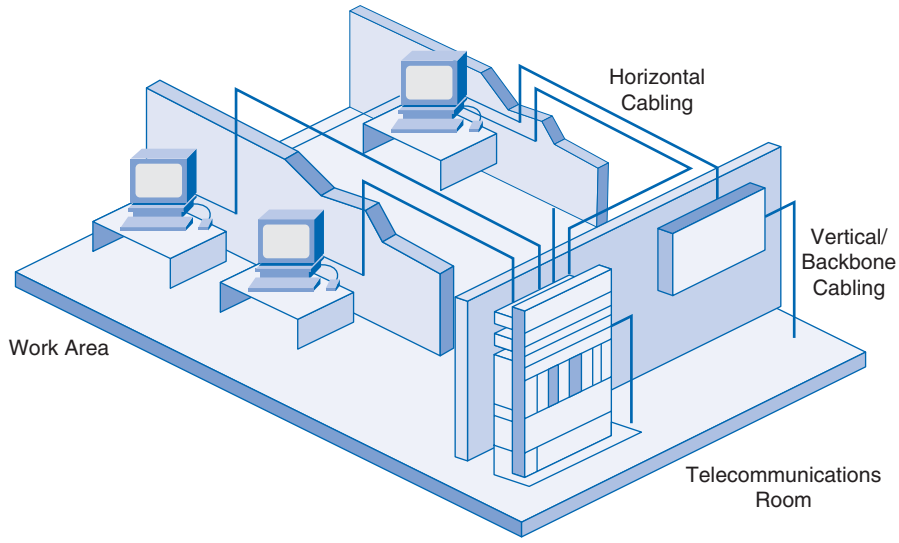
When designing a structured cabling project, the first step is to obtain an accurate floor plan. The floor plan allows the technician to identify possible wiring closet locations, cable runs, and which electrical areas to avoid.

After the technician has identified and confirmed the locations of network devices, it is time to draw the network on the floor plan. Some of the more important items to document include the following:

- **Patch cable:** A short cable from the computer to the wall plate in the user work area.
- **Horizontal cable:** A cable from the wall plate to the IDF in the distribution area.
- **Vertical cable:** A cable from the IDF to the MDF in the organization's backbone area.
- **Backbone cable:** The part of a network that handles the major traffic.
- **Location of wiring closet:** An area to concentrate the end-user cable to the hub or switch.
- **Cable management system:** A series of trays and straps used to guide and protect cable runs.
- **Cable labeling system:** A proper labeling system or scheme that identifies cables.
- **Electrical considerations:** The premises should have adequate outlets to support the electrical requirements of the network equipment.

Figure 3-8 shows a telecommunications room and work area with both horizontal and vertical cabling.

Figure 3-8 Horizontal and Vertical Cabling



Lab 3-1: Evaluating a Cabling Upgrade Plan (3.2.4)

In this lab, you propose a cable upgrade plan to accommodate extra floor space acquired by a company. Refer to the hands-on lab in Part II of this book. You may perform this lab now or wait until the end of the chapter.

Purchasing and Maintaining Equipment

As the ISP team plans the network upgrade, issues arise related to purchasing new equipment, as well as maintaining new and existing equipment. Generally you have two options for the new equipment: managed service or in-house solutions. With a managed service solution, the equipment is obtained from the ISP through a lease or some other agreement. The ISP is responsible for updating and maintaining the equipment. With an in-house solution, the customer purchases the equipment and is responsible for updates, warranties, and maintaining the equipment.

Purchasing Equipment

When you purchase equipment, cost is always a major factor. A cost analysis of the purchase options must be conducted to provide a sound basis for the final purchase decision. Normally the customer conducts the cost analysis, but this may be done in conjunction with the ISP. Many other factors should be considered in addition to cost. Table 3-3 describes some of the factors you must consider when you're trying to decide if a managed or in-house solution is more appropriate.

Table 3-3 Managed Service or In-house Solution

	In-House	Managed Service
Considerations	Requires many decisions: Type of equipment Equipment location IT organization staffing Network design Maintenance requirements	Initial evaluation and choice of service provider Requirements definition Ongoing evaluation of service provider
Costs	Equipment purchasing or leasing IT organization staffing Training costs Multiple vendor costs and building Hardware repairs and upgrades Software release upgrades Telephone line changes Redundancy and reliability requirements	Single, predictable, monthly recurring bill Minimal up-front costs
Control and responsibility	You have most of the control and responsibility for managing and maintaining your network system	Delegate the level of network management to a qualified service provider based on your needs Keep your core business processes in-house Maintain control of the work flow in your organization Set service-level agreements (SLA) with a service provider
Reliability	You are responsible for keeping your network system available to employees, customers, and partners at all times	Service provider can guarantee availability up to 99.999% A 24-hour help desk is available for remote-access users Service provider management is transparent to the end users
End-user experience	Users are unaware of whether the network is managed by the companyor an external partner	Users are unaware of whether the network is managed by the company or an external partner

If the customer chooses the managed service, the SLA outlines the lease costs as well as other service costs. If the equipment is purchased outright, the customer should be aware of cost, warranty coverage, compatibility with existing equipment, and update and maintenance issues, all of which have an associated cost. This cost must be analyzed to determine the cost-effectiveness of any planned solution.

Selecting Network Devices

After the customer requirements have been analyzed, the design staff recommends the appropriate network devices to connect and support the new network functionality. Modern networks use a variety of devices for connectivity. Each device has certain capabilities to control the flow of data across a network. A general rule is that the higher the device is in the OSI model, the more intelligent it is. This means that a higher-level device can better analyze the data traffic and forward it based on information not available at lower layers. For example, a Layer 1 hub can only forward data out all ports, a Layer 2 switch can filter the data and only send it out the port connected to the destination based on MAC address, and a Layer 3 router can decide which traffic to forward or block based on the logical address.

As switches and routers evolve, the distinction between them becomes blurred. One simple distinction remains: LAN switches provide connectivity within an organization's LAN, whereas routers are needed to interconnect local networks or to form a wide-area network (WAN) environment.

In addition to switches and routers, other connectivity options are available for LANs. Wireless access points allow computers and other devices, such as handheld Internet Protocol (IP) phones, to wirelessly connect to the network or share broadband connectivity. Firewalls guard against network threats and provide application security, network control and containment, and secure connectivity technologies. ISRs combine the functionality of switches, routers, access points, and firewalls in the same networking device.

Selecting LAN Devices

Although both a hub and a switch can provide connectivity at the access layer of a network, switches should be chosen for connecting devices to a LAN. Switches generally are more expensive than hubs, but the enhanced performance makes them cost-effective. A hub generally is chosen as a networking device within a very small LAN, within a LAN that requires low throughput requirements, or when finances are limited. A hub may also be installed in a network when all network traffic is to be monitored. Hubs forward all traffic out all ports, whereas switches microsegment the network. Connecting a network-monitoring device to a hub allows the monitoring device to see all network traffic on that segment. Some switches do provide the ability to monitor all network traffic through a special port, but this is not a universal feature.

When selecting a switch for a particular LAN, network designers need to consider a number of factors, including the following:

- Speed and types of ports/interfaces
- Expandability
- Manageability
- Cost

Speed and Types of Ports/Interfaces

Choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without your having to replace the central devices. It is a good idea to purchase the fastest ports available within the budgeted funds. A bit of extra money spent now can save a great deal of time and expense later, when it is time to upgrade the network again.

The same can be stated about the number and types of network ports. Network designers must carefully consider how many UTP and fiber ports are needed. It is important to estimate how many additional ports will be required to support network expansion in the future.

Expandability

Networking devices come in both fixed and modular physical configurations. Fixed configurations have a specific number and type of ports or interfaces and cannot be expanded. Modular devices have expansion slots that provide the flexibility to add new modules as requirements evolve. Most modular devices come with a basic number of fixed ports as well as expansion slots.

A typical use of an expansion slot is to add fiber-optic modules to a device that was originally configured with a number of fixed UTP ports. Modular switches can be a cost-effective approach to scaling LANs.

Manageability

A managed switch provides control over individual ports or over the switch as a whole. Typical controls include the ability to monitor operation and change the settings for a device. A managed device can be monitored for performance and security and typically provides enhancements to the monitoring and security features. For example, with a managed switch, ports can be turned on or off as required to control access. In addition, administrators can control which computers or devices are allowed to connect to a port.

Cost

The cost of a switch is determined by its capacity and features. The switch capacity includes the number and types of ports available and the overall throughput. Other factors that impact the cost are the switch's network management capabilities, embedded security technologies, and optional advanced switching technologies.

Using a simple cost-per-port calculation, it may appear initially that the best option is to deploy one large switch at a central location. However, this apparent cost savings may be offset by the expense from the longer cable lengths required to connect every device on the LAN to one central switch. Compare this option with the cost of deploying a number of smaller switches connected by a few long cables to a central switch.

Deploying a number of smaller devices instead of a single large device also has the benefit of reducing the size of the ***failure domain.*** A failure domain is the area of the network affected when a piece of networking equipment malfunctions or fails.

Packet Tracer ☐ **Activity**

Exploring Different LAN Switch Options (3.3.3)

In this activity, you determine which types of interfaces are required to connect a new company switch to a router, Linksys wireless router, and hosts. Use file d2-333 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Selecting Internetworking Devices

After the LAN switches have been selected, it is time to determine which router is appropriate for the customer. A router is a Layer 3 device. It performs all tasks of devices in lower layers and selects the best route to the destination network based on Layer 3 information. Routers are the primary devices used to interconnect networks. Each port on a router connects to a different network and routes packets between the networks. Routers can break up broadcast domains and collision domains.

You must consider a number of factors when selecting a router. It is necessary to match the router's characteristics to the network's requirements. Factors for choosing a router include

- The type of connectivity required
- Features available
- Cost

Connectivity

Routers are used to interconnect networks that use different technologies. They can have both LAN and WAN interfaces. The router's LAN interfaces connect to the LAN medium. This medium typically is UTP cabling, but modules can be added to the router to allow the use of fiber-optic cable and other types of media. Depending on the series or model of router, there can be multiple interface types for connecting LAN and WAN cabling. It is important to anticipate an organization's future connectivity requirements and purchase a router that will serve the organization well into the future.

Features

It is necessary to match the router's characteristics to the network's requirements. After analysis, the business may need a router with specific features in addition to basic routing. Many routers provide features such as the following:

- Security
- Quality of service (QoS)
- Voice over IP (VoIP)
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Wireless access
- Virtual private network (VPN)
- Intrusion detection

Most of these services are contained in the ***Cisco IOS*** that manages the router hardware and resources. Although normally these are software features, the hardware must be able to support the IOS required.

Cost

When you select internetwork devices, budget is an important consideration. Routers can be expensive. Additional modules, such as fiber optics, can increase the costs. To keep costs as low as possible, the medium used to connect to the router should be supported without the purchase of additional modules.

An ***Integrated Services Router (ISR)*** is a relatively new technology that combines multiple services into one device. Before the ISR, multiple devices were required to meet the needs of data, wired and wireless, voice and video, firewall, and VPN technologies. The ISR was designed with multiple services to accommodate the demands of small to medium-sized businesses and branch offices of large organizations. An ISR is designed for ease of use. It can quickly and easily enable end-to-end protection for users, applications, network endpoints, and wireless LANs. The cost of an ISR normally is less than if the individual devices are purchased separately.

Packet Tracer Activity

Exploring Internetworking Devices (3.3.4)

In this activity, you determine and install the correct modules in the 1841 ISR to provide network connectivity. In addition, you select the correct cables to connect various network devices to the 1841 ISR. Use file d2-334 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Network Equipment Upgrades

Many small networks were initially built using a low-end integrated router to connect wireless and wired users. This type of device is designed to support small networks, usually consisting of a few wired hosts and possibly four or five wireless devices. When a small business outgrows the capabilities of its existing network devices, it must upgrade to more-capable devices. The devices used in this course and book are the Cisco 1841 ISR and the Cisco 2960 switch, as shown in Figure 3-9.

Figure 3-9 Cisco 1841 ISR and 2960 Switch

Cisco 1841 ISR

Cisco 2960 Switch

The Cisco 1841 ISR is designed to be a branch office or medium-sized business router. As an entry-level multiservice router, it offers a number of different connectivity options. It is modular in design and can deliver multiple security services.

The Cisco Catalyst 2960 series Intelligent Ethernet switches are a family of fixed-configuration, standalone devices that provide Fast Ethernet and Gigabit Ethernet connectivity to the desktop. These switches can provide the high speeds and high-density switching capabilities that the smaller ISRs with integrated switching cannot. They are therefore a good option when upgrading networks built with either hubs or small ISR devices.

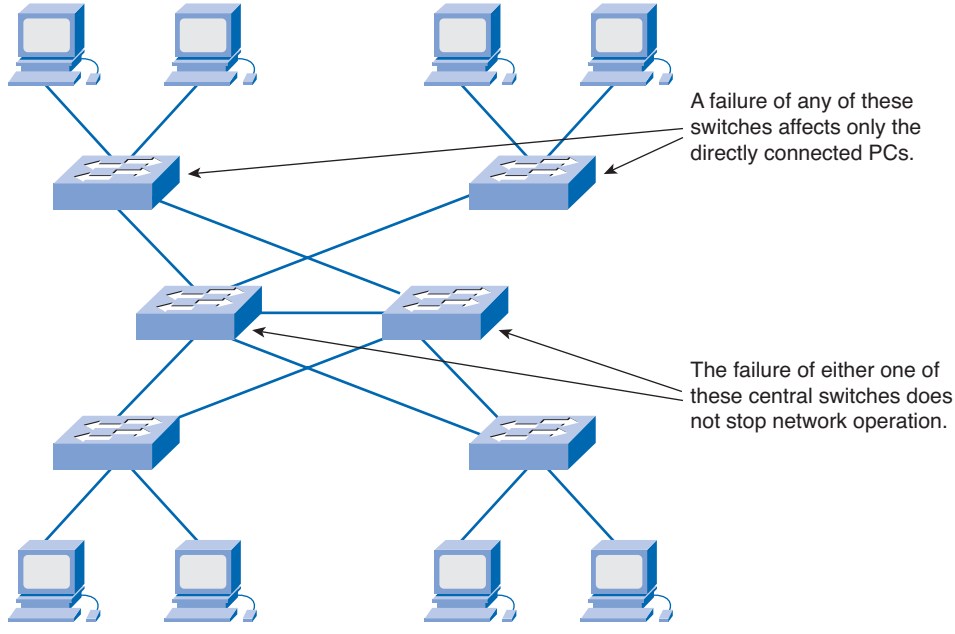
The Catalyst 2960 family of switches, shown in Figure 3-10, provides entry-level, enterprise-class, fixed-configuration switching that is optimized for access layer deployments. They provide both Fast Ethernet and Gigabit Ethernet to the desktop and are ideal for entry-level enterprise, mid-market, and branch-office environments. These compact switches often are deployed outside the wiring closet.

Figure 3-10 Cisco Catalyst 2960 Family of Switches

Reliability and Availability

Purchasing network devices and the installation of cabling for a network upgrade is only the beginning. Networks must be both reliable and available. Reliability is usually achieved by adding redundant components to the network, such as two routers instead of one. In this case, alternative data paths are created, so if one router experiences problems, the data can take an alternative route to arrive at the destination. For better reliability, all devices and connections should have complete redundancy. Unfortunately, this is extremely expensive in most environments. Therefore, the network design team must determine the level of redundancy to incorporate to achieve the necessary reliability. Figure 3-11 shows redundancy in a switched network.

Figure 3-11 Redundancy in a Switched Network



Availability is the amount of time the network is ready and able to deliver the necessary services. Any increase in reliability improves availability. Ensuring a higher level of availability requires not only redundancy but also equipment and software that have been engineered to provide this level of service. As an example of availability, telephone systems require "five 9s" of uptime. This means that the telephone system must be available 99.999% of the time. Telephone systems cannot be down, or unavailable, more than .001% of the time.

Fault tolerance systems typically are used to improve network reliability. Fault tolerance systems include devices such as UPSs, multiple AC power supplies, hot-swappable devices, and multiple interface cards. When one device fails, the redundant or backup system takes over to ensure minimal loss of reliability.

IP Addressing Plan

Planning for the network installation must include planning the logical addressing. Changing the Layer 3 IP addressing is a major issue when upgrading a network. If the network's structure is changed in the upgrade, the IP address scheme and network information may need to be altered to reflect the new structure.

When developing the addressing scheme, you must consider every device that requires an IP address, now and in the future. Some devices require addresses to carry out their functionality, and others only require an IP address to allow them to be accessed and configured across the network. Hosts and network devices that require an IP address include

- User computers
- Administrator computers
- Servers
- Other end devices such as printers, IP phones, and IP cameras
- Router LAN interfaces
- Router WAN (serial) interfaces
- Standalone switches
- Wireless access points

For example, if a new router is introduced to the network, new local networks, or subnets, are created. These new subnets need to have the proper IP address and subnet mask calculated. Sometimes, this means having to assign a totally new addressing scheme to the entire network.

After all the planning and design phases are complete, the upgrade proceeds to the implementation phase, in which the actual network installation begins.

Summary

Networks often experience unexpected growth and develop in a disorganized manner. When this happens, network performance degrades slowly with each new device added. At some point, the network no longer can support the traffic being generated by the users, so a network upgrade is required.

Whether the network upgrade is forced or planned, the upgrade process must be conducted in an organized manner. The upgrade plan must consider the strengths and weaknesses of and opportunities and threats posed by the network installation.

A network upgrade has five phases:

- Requirements gathering
- Equipment selection and network design
- Implementation
- Operation
- Review and evaluation

Documentation must include the physical and logical topology of the existing network, along with a complete inventory sheet of all equipment. This includes the location and layout of any telecommunications rooms as well as existing network wiring. Customer network requirements are gathered through surveys and interviews.

Cabling has four physical areas to consider: work areas, distribution area, telecommunications room, and backbone. Structured cabling projects deal with the placement of cables, the location of wiring closets, cable management, and electrical considerations.

When new equipment is used in a network upgrade, you have two purchase options: managed service and in-house. Both of these present many advantages and have serious limitations. The choice depends on the current business strengths and weaknesses.

Cost and expandability are two of the most important considerations when upgrading network devices. Generally, a device that functions at a higher OSI layer is considered a more intelligent device.

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 Activity on the CD:

Interactive Activity 3-1: Network Planning Phases (3.2.1)

Packet Tracer Activities on the CD:

Creating Network Diagrams (3.1.3)

Exploring Different LAN Switch Options (3.3.3)

Exploring Internetworking Devices (3.3.4)

Hands-on Lab in Part II of this book:

Lab 3-1: Evaluating a Cabling Upgrade Plan (3.2.4)

Check Your Understanding

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

1. What is the purpose of a site survey? (Select all that apply.)

   A. To determine what network resources are currently in place.
   B. To accurately forecast the current and future network requirements.
   C. To repair any malfunctioning network equipment.
   D. To ensure that all purchased networking equipment is still properly installed and functioning.

2. What should a site survey technician do if he or she finds nonstandard network installations during the survey process?

   A. Report the condition to management to make sure that the previous contractor does not get rehired.
   B. Inform management that they are in violation of standards and must pay you to correct the situation, or you will have to report them.
   C. Ignore the situation, and proceed with the survey.
   D. Report the condition to management, pointing out that this often happens when networks grow unexpectedly.

3. What should be done as a first step after the technician completes the site survey?

   A. Use the information contained in the site survey documents to determine the customer's network requirements.
   B. Review the site survey with the customer to make sure that nothing has been missed and everything is accurate.
   C. Use the information contained in the site survey documents to determine how long the planned network upgrade will take.
   D. Ask the technician to summarize the site survey documentation, summarizing only the important facts.

4. What should be contained on a logical topology diagram? (Select all that apply.)

   A. Location of all networking devices
   B. Physical location of cabling runs
   C. IP address information of all devices
   D. Device names
   E. Location of wiring closets

5. What information should you record about devices when performing a network inventory? (Select all that apply.)

A. Device name, brand, and model
B. Physical location
C. Operating system
D. Logical addressing information
E. Connection information
F. Security information

6. What is the correct sequence of steps when performing a network upgrade?

1. Review and evaluation
2. Implementation
3. Operation
4. Requirements gathering
5. Selection and design

A. 1, 2, 3, 4, 5
B. 4, 5, 1, 2, 3
C. 4, 5, 2, 3, 1
D. 4, 1, 5, 3, 2
E. 1, 4, 5, 2, 3

7. What is the name of the location where all network cable is concentrated in a single point?

A. IDF
B. ISP
C. IXP
D. MDF
E. MFD

8. What type of cable typically is used to connect a workstation network interface card (NIC) to the wall outlet?

A. STP
B. UTP
C. Coaxial
D. Fiber-optic

9. Which of the following direct connections normally would require a crossover cable? (Select all that apply.)

A. A PC connected to another PC
B. A PC connected to a switch
C. A PC connected to a router
D. A switch connected to a router
E. A router connected to another router

10. What factors should you consider when selecting an internetworking device?

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. A small company is trying to decide if it should install and manage its own network solution or if it should invest in a managed solution from its local ISP. The company currently is having financial difficulties and does not have an internal IT department. What suggestion would you make, and why?
2. You have asked two new network technicians to recommend a switch for a new department within the company. The department will have 27 users and four networked printers. All devices currently connect at 100 Mbps. The first technician recommends a switch that has 48 10/100-Mbps ports. The second technician recommends a slightly more expensive switch that has 48 10/100/1000-Mbps ports and two fiber-optic uplink ports. Which technician has made the better recommendation, and why?

Index

Symbols

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