

LAN Switching and Wireless

CCNA Exploration Companion Guide

Wayne Lewis, Ph.D.

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

LAN Switching and Wireless CCNA Exploration Companion Guide

Wayne Lewis, Ph.D.

Copyright© 2008 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing April 2008

Library of Congress Cataloging-in-Publication Data

Lewis, Wayne, Ph.D.

LAN switching and wireless : CCNA exploration companion guide / Wayne

Lewis. -- 1st ed.

p. cm.

ISBN 978-1-58713-207-0 (hardcover w/cd)

1. Telecommunication--Switching systems--Examinations--Study guides.
2. Wireless LANs--Examinations--Study guides.
3. Telecommunications engineers--Certification--Examinations--Study guides. I. Cisco Networking Academy Program. II. Cisco Systems, Inc. III. Title.

TK5103.8.L493 2008

004.6'8--dc22

2008011633

ISBN-13: 978-1-58713-207-0

ISBN-10: 1-58713-207-9

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.



Warning and Disclaimer

This book is designed to provide information about LAN Switching and Wireless of the Cisco Network Academy CCNA Exploration curriculum. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Production Manager

Patrick Kanouse

Development Editor

Andrew Cupp

Senior Project Editor

San Dee Phillips

Copy Editor

Barbara Hacha

Technical Editors

Martin S. Anderson

Samuel Bolaños

George Wong

Editorial Assistant

Vanessa Evans

Book and Cover Designer

Louisa Adair

Composition

TnT Design, Inc.

Indexer

Publishing Works

Proofreader

Mike Henry

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

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

Trademark Acknowledgments

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

Corporate and Government Sales

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

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

Feedback Information

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

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

We greatly appreciate your assistance.



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

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

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

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

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc., and Access Registrar, Aironet, BPX, Catalyst, CCDA, CGDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Introduction

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

LAN Switching and Wireless, CCNA Exploration Companion Guide is the official supplement textbook to be used with v4 of the CCNA Exploration LAN Switching and Wireless online curriculum of the Networking Academy.

This book goes beyond earlier editions of the Cisco Press Companion Guides by providing many alternative explanations and examples as compared with the course. You can use the online curriculum as normal and use this companion guide to help solidify your understanding of all the topics through the alternative examples.

The basis for this book, as well as the online curriculum, is to provide the reader with a thorough understanding of LAN switching and wireless technologies beyond that necessary for the CCNA certification exam. The commands and web-based GUI utilities for configuring LAN switching and wireless are not very difficult. The challenge is to understand the operation of these technologies and protocols and their role in the network.

The objective of this book is to explain LAN switching and wireless technologies. Every concept is methodically explained with no assumptions made of the reader's knowledge of LAN switching or wireless technologies. The only exceptions are if a concept is beyond the scope of this course or is covered in CCNP, and then it is noted within the text.

Readers are encouraged to peruse the resources managed by Wayne Lewis at cisco.honolulu.hawaii.edu. Please e-mail Wayne Lewis at waynel@hawaii.edu for more information about CCNP and network security instructor training and for access to more resources for this course and other CCNP, IP telephony, QoS, and network security courses.

Goal of This Book

First and foremost, by providing a fresh, complementary perspective on the content, this book is intended to help you learn all the required materials of the LAN Switching and Wireless course in the Networking Academy CCNA Exploration curriculum. As a secondary goal, the text is intended as a mobile replacement for the online curriculum for individuals who do not always have Internet access. In those cases, you can instead read the appropriate sections of the book, as directed by your instructor, and learn the same material that is covered in the online curriculum. Another secondary goal is to serve as your offline study material to prepare for the CCNA exam.

Audience for This Book

This book's main audience is anyone taking the CCNA Exploration LAN Switching and Wireless course of the Cisco Networking Academy curriculum. Many Academies use this textbook as a required tool in the course, and other Academies recommend the Companion 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 Companion 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, this book 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 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 author has compiled, edited, and in most cases rewritten the material so that it has a more conversational tone that follows a consistent and accessible college-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 inside 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 150 terms.

Practice

Practice makes perfect. This new Companion 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. The Appendix, “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. The Appendix 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 allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in this book’s CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

Packet Tracer
□ Activity

Labs and Study Guide

The supplementary book *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* (ISBN: 1-58713-202-8) by Cisco Press contains all the labs from the curriculum plus additional challenge labs and study guide material. The end of each chapter of this Companion Guide indicates with icons what labs, activities, and Packet Tracer activities are available in the Labs and Study Guide.



- **Lab references:** This icon notes the hands-on labs created for this chapter in the online curriculum. Within the *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* you will find additional study guide material created by the author of that book.
- **(NEW) Packet Tracer Companion activities:** Many of the Hands-on Labs include Packet Tracer Companion Activities where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in the *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* for Hands-on Labs that have a Packet Tracer Companion.

Packet Tracer
□ Companion



- **(NEW) Packet Tracer Skills Integration Challenge activities:** These activities require you to pull together several skills learned from the chapter to successfully complete one comprehensive exercise. Look for this icon in the *LAN Switching and Wireless*, *CCNA Exploration Labs and Study Guide* for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

A Word About Packet Tracer

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

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

The course includes essentially three types of Packet Tracer activities. This book uses an icon system to indicate which type of Packet Tracer activity is available. The icons are intended to give you a sense of the purpose of the activity and the amount of time you need to allot to complete it. The three types of Packet Tracer activities follow:



- **Packet Tracer Activity:** This icon identifies straightforward exercises interspersed throughout the chapters where you can practice or visualize a specific topic. The activity files for these exercises are available on this book’s CD-ROM. These activities take less time to complete than the Packet Tracer Companion and Challenge activities.



- **Packet Tracer Companion:** This icon identifies exercises that correspond to the hands-on labs of the course. You can use Packet Tracer to complete a simulation of the hands-on lab or complete a similar “lab.” The Companion Guide points these out at the end of each chapter, but look for this icon and the associated exercise file in *LAN Switching and Wireless*, *CCNA Exploration Labs and Study Guide* for hands-on labs that have a Packet Tracer Companion.



- **Packet Tracer Skills Integration Challenge:** This icon identifies activities that require you to pull together several skills learned from the chapter to successfully complete one comprehensive exercise. The Companion Guide points these out at the end of each chapter, but look for this icon and the associated exercise file in *LAN Switching and Wireless*, *CCNA Exploration Labs and Study Guide* for instructions on how to perform a Packet Tracer Skills Integration Challenge.

How This Book Is Organized

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

For people reading this book without being in the CCNA Exploration LAN Switching and Wireless class, or just using this book for self-study, the sequence of topics in each chapter provides a logical sequence for learning the material presented.

Each chapter has a reference topology that is used to maintain a common framework from which to build upon the LAN switching and wireless concepts. The single topology per chapter allows for better continuity and easier understanding of switching commands, operations, and outputs, as well as web-based GUI utility mastery.

- **Chapter 1, “LAN Design,”** provides an overview of the switched LAN architecture for small- and medium-sized businesses. The concept of converged network services within hierarchical networking is emphasized. You also learn how to select the appropriate switch to implement at each hierarchical layer in the switched LAN topology.
- **Chapter 2, “Basic Switch Concepts and Configuration,”** reviews and reinforces the underlying concepts included within the IEEE 802.3 LAN standard and introduces the role of an Ethernet switch within a LAN. The basic configuration of switches to support voice, video, and data transmission is introduced, as well as basic network management options and rudimentary security measures.
- **Chapter 3, “VLANs,”** provides an introduction to types of VLANs, port membership within VLANs, and VLAN trunking. VLANs are the logical basis upon which switched LANs are built. Configuring, verifying, and troubleshooting VLANs are discussed.
- **Chapter 4, “VTP,”** examines the VLAN trunking protocol. VTP automates many of the VLAN configuration options in a switched LAN, but requires a good conceptual understanding of how the Layer 2 protocol operates. The underlying operation of VTP and VTP pruning are explored, followed by detailed guidance on VTP configuration.
- **Chapter 5, “STP,”** provides a detailed analysis of the original IEEE 802.1D spanning-tree protocol (STP) and the improved IEEE 802.1w rapid spanning-tree protocol (RSTP). The operation of STP is complex and requires a careful, measured approach, which is provided herein. Compared to the underlying operation of STP, the configuration of 802.1D and 802.1w is relatively straightforward. Both 802.1D and 802.1w result in a logical, loop-free, Layer 2 topology with physical redundancy.
- **Chapter 6, “Inter-VLAN Routing,”** explores three methods of inter-VLAN routing: one router interface per VLAN, router-on-a-stick, and multilayer switching. The configuration of the first two methods on access layer switches is detailed. Verification and troubleshooting inter-VLAN routing scenarios round out the chapter.

- **Chapter 7, “Basic Wireless Concepts and Configuration,”** provides a quick introduction to all the important elements necessary to understand wireless technologies and standards. A web-based GUI is used to configure wireless routers in constructing the LAN/WLAN reference topology for the chapter. Common troubleshooting issues specific to wireless LANs are explored.
- The **Appendix, “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.

About the CD-ROM

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

Packet Tracer
□ Activity

- **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.
- **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 for on-the-job success as well. 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.

About the Cisco Press Website for This Book

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

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

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

LAN Design

Objectives

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

- How does a hierarchical network support the voice, video, and data needs of a small- or medium-sized business?
- What are the functions of each of the three layers of the hierarchical network design model?
- What are common examples of the effect of voice and video over IP on network design?
- What devices are recommended at each layer of the hierarchical design model?
- How are Cisco Catalyst switch product lines best positioned in the hierarchical design model?

Key Terms

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

access layer page 2

distribution layer page 3

core layer page 3

scalability page 4

redundancy page 4

performance page 4

security page 4

manageability page 4

maintainability page 4

voice over IP (VoIP) page 10

convergence page 10

quality of service (QoS) page 10

private branch exchange (PBX) page 11

enterprise network page 24

Power over Ethernet (PoE) page 26

multilayer switch page 27

For small- and medium-sized businesses, digital communication with data, voice, and video is critical to performing day-to-day business functions. Consequently, a properly designed LAN is a fundamental requirement for doing business. You must understand what a well-designed LAN is and be able to select appropriate devices to support the network specifications of a small- or medium-sized business.

In this chapter, you begin exploring the switched LAN architecture and some of the principles that are used to design a hierarchical network. You learn about converged networks. You also learn how to select the correct switch for a hierarchical network and which Cisco switches are best suited for each hierarchical layer of the network.

Switched LAN Architecture

When building a switched LAN architecture that satisfies the needs of a small- or medium-sized business, your plan is more likely to be successful if a hierarchical design model is used. Compared to other network designs, a hierarchical network is easier to manage and expand, and problems are solved more quickly.

Hierarchical network design involves dividing the network into discrete layers. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, the network design becomes modular, which facilitates scalability and performance.

The typical hierarchical design model is broken into three layers:

- Access
- Distribution
- Core

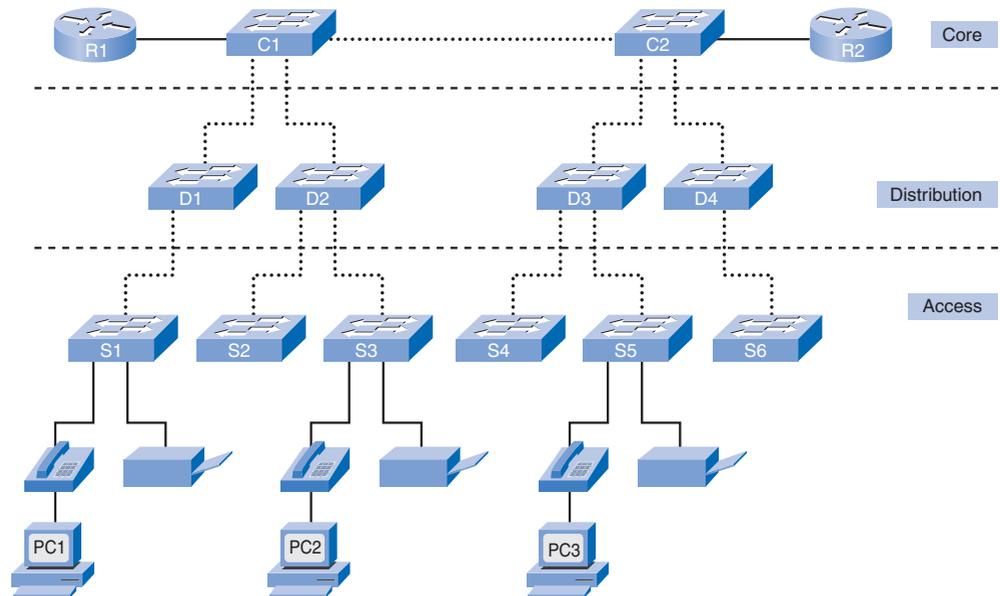
An example of a three-layer hierarchical network design is displayed in Figure 1-1.

The Hierarchical Network Model

This section describes the access, distribution, and core layers in more detail. Following the introduction of the three-layer model, we explore the hierarchical model in medium-sized businesses. Finally, we delve into the benefits of hierarchical network design.

Access Layer

The *access layer* interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points. The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.

Figure 1-1 The Hierarchical Network Model

Distribution Layer

The *distribution layer* aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer. VLANs allow you to segment the traffic on a switch into separate subnetworks. For example, in a university you might separate traffic according to faculty, students, and guests. Distribution layer switches are typically high-performance devices that have high availability and redundancy to ensure reliability. You will learn more about VLANs, broadcast domains, and inter-VLAN routing later in this book.

Core Layer

The *core layer* of the hierarchical design is the high-speed backbone of the internetwork. The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Note

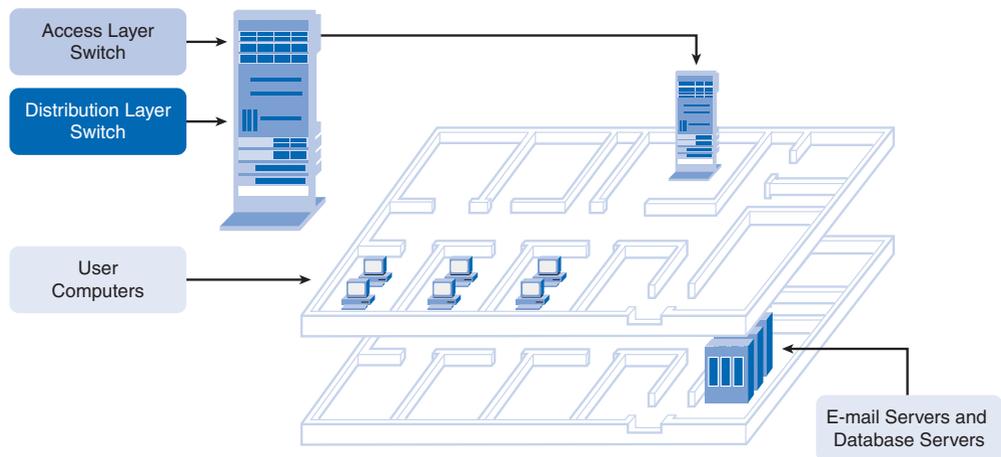
In small networks, it is not unusual to implement a collapsed core model, where the distribution layer and core layer are combined into one layer.

A Hierarchical Network in a Medium-Sized Business

Now look at the hierarchical network model applied to a business. In Figure 1-1, the access, distribution, and core layers are separated into a well-defined hierarchy. This logical representation makes it easy to see which switches perform which function. It is much harder to see these hierarchical layers when the network is installed in a business.

Figure 1-2 shows two floors of a building. The user computers and network devices that need network access are on one floor. The resources, such as e-mail servers and database servers, are located on another floor. To ensure that each floor has access to the network, access layer and distribution switches are installed in the wiring closets of each floor and connected to each of the devices needing network access. The figure shows a small rack of switches. The access layer switch and distribution layer switch are stacked on top of each other in the wiring closet.

Figure 1-2 A Hierarchical Network in a Medium-Sized Business



Although the core and other distribution layer switches are not shown, you can see how the physical layout of a network differs from the logical layout of Figure 1-1.

Benefits of a Hierarchical Network

Many benefits are associated with hierarchical network designs:

- *Scalability*
- *Security*
- *Redundancy*
- *Manageability*
- *Performance*
- *Maintainability*

Detailed descriptions of each of these benefits follow.

Scalability

Hierarchical networks scale very well. The modularity of the design allows you to replicate design elements as the network grows. Because each instance of the module is consistent, expansion is easy to plan and implement. For example, if your design model consists of two distribution layer switches for every 10 access layer switches, you can continue to add access layer switches until you have 10 access layer switches cross-connected to the two distribution layer switches before you need to add additional distribution layer switches to the network topology. Also, as you add more distribution layer switches to accommodate the load from the access layer switches, you can add additional core layer switches to handle the additional load on the core.

Redundancy

As a network grows, availability becomes more important. You can dramatically increase availability through easy redundant implementations with hierarchical networks. Access layer switches are connected to two different distribution layer switches to ensure path redundancy. If one of the distribution layer switches fails, the access layer switch can switch to the other distribution layer switch. Additionally, distribution layer switches are connected to two or more core layer switches to ensure path availability if a core switch fails. The only layer where redundancy is limited is at the access layer. Typically, end node devices, such as PCs, printers, and IP phones, do not have the capability to connect to multiple access layer switches for redundancy. If an access layer switch fails, just the devices connected to that one switch would be affected by the outage. The rest of the network would continue to function unaffected.

Performance

Communication performance is enhanced by avoiding the transmission of data through low-performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases. The distribution layer then uses its high-performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination. Because the core and distribution layers perform their operations at very high speeds, no contention for network bandwidth occurs. As a result, properly designed hierarchical networks can achieve near wire speed between all devices.

Security

Security is improved and easier to manage. Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network. You also have the flexibility to use more advanced security policies at the distribution layer. You may apply access control policies that define which communication protocols are deployed on your network and where they are permitted to go. For example, if you want to limit the use of HTTP to a specific user community connected at the access

layer, you could apply a policy that blocks HTTP traffic at the distribution layer. Restricting traffic based on higher layer protocols, such as IP and HTTP, requires that your switches are able to process policies at that layer. Some access layer switches support Layer 3 functionality, but it is usually the job of the distribution layer switches to process Layer 3 data because they can process it much more efficiently.

Manageability

Manageability is relatively simple on a hierarchical network. Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. Therefore, if you need to change the functionality of an access layer switch, you could repeat that change across all access layer switches in the network because they presumably perform the same functions at their layer. Deployment of new switches is also simplified because switch configurations can be copied between devices with very few modifications. Consistency between the switches at each layer allows for rapid recovery and simplified troubleshooting. In some special situations, configuration inconsistencies could exist between devices, so you should ensure that configurations are well documented so that you can compare them before deployment.

Maintainability

Because hierarchical networks are modular in nature and scale very easily, they are easy to maintain. With other network topology designs, maintainability becomes increasingly complicated as the network grows. Also, in some network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier. Adding switches to one layer does not necessarily mean there will not be a bottleneck or other limitation at another layer. For a full mesh network topology to achieve maximum performance, all switches need to be high-performance switches because each switch needs to be capable of performing all the functions on the network. In the hierarchical model, switch functions are different at each layer. You can save money by using less-expensive access layer switches at the lowest layer, and spend more on the distribution and core layer switches to achieve high performance on the network.

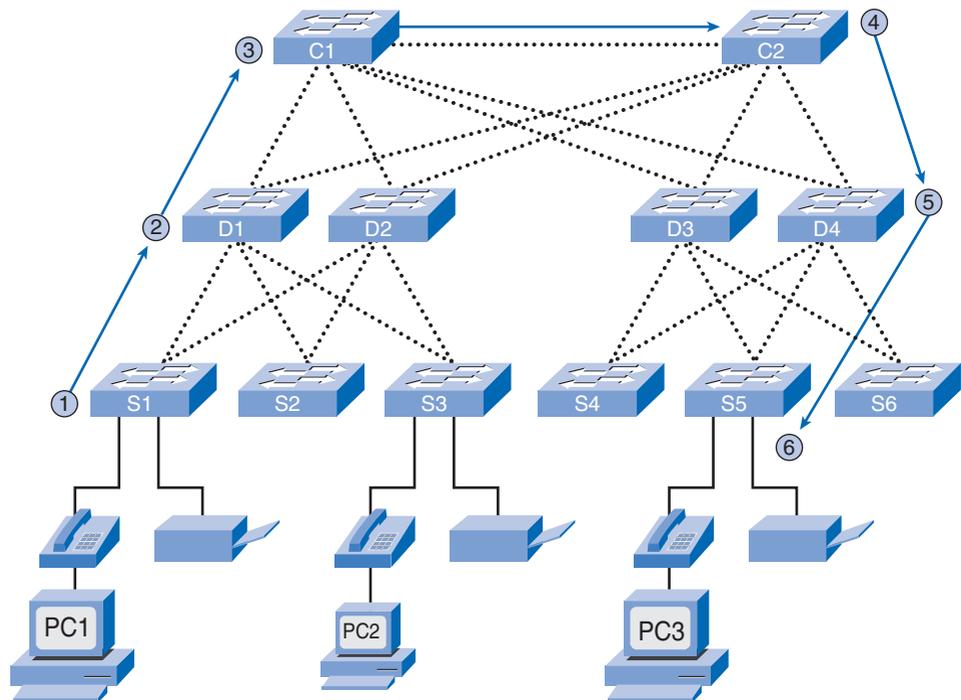
Principles of Hierarchical Network Design

Just because a network seems to have a hierarchical design does not mean that the network is well designed. These simple guidelines will help you differentiate between well-designed and poorly designed hierarchical networks. This section is not intended to provide you with all the skills and knowledge you need to design a hierarchical network, but it offers you an opportunity to begin to practice your skills by transforming a flat network topology into a hierarchical network topology.

Network Diameter

When designing a hierarchical network topology, the first thing to consider is network diameter, as depicted in Figure 1-3. Diameter is traditionally a measure of distance, but in the case of networking, we are using the term to measure the number of devices. Network diameter is the number of devices that a packet has to cross before it reaches its destination. Keeping the network diameter low ensures low and predictable latency between devices.

Figure 1-3 Network Diameter



In Figure 1-3, PC1 communicates with PC3. Up to six interconnected switches could be between PC1 and PC3. In this case, the network diameter is six. Each switch in the path introduces some degree of latency. Network device latency is the time spent by a device as it processes a packet or frame. Each switch has to determine the destination MAC address of the frame, check its MAC address table, and forward the frame out the appropriate port. Even though that entire process happens in a fraction of a second, the time adds up when the frame has to cross many switches.

In the three-layer hierarchical model, Layer 2 segmentation at the distribution layer practically eliminates network diameter as an issue. In a hierarchical network, network diameter is always going to be a predictable number of hops between the source and destination devices.

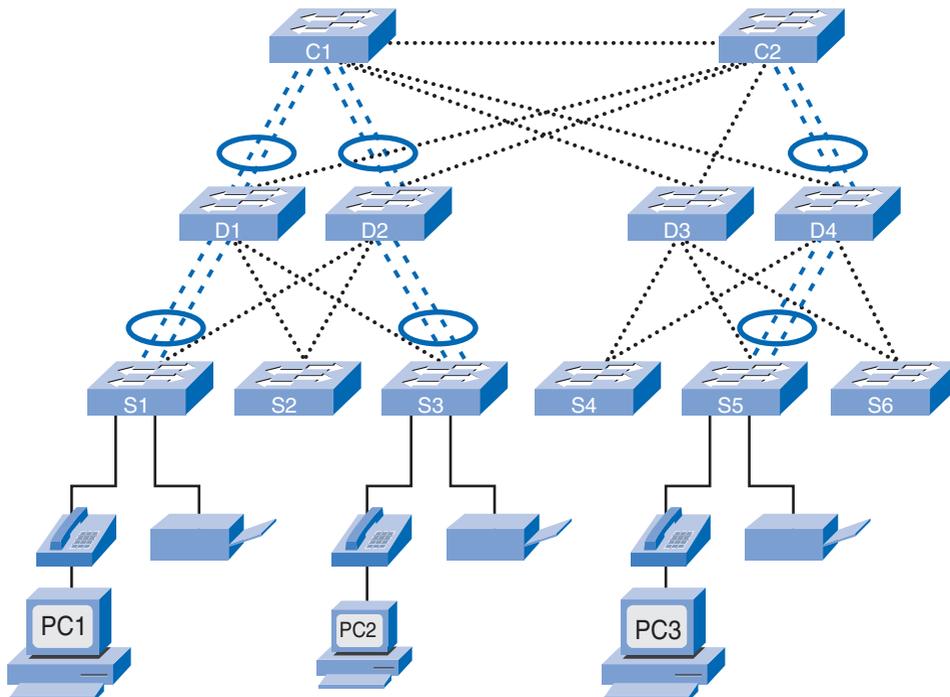
Bandwidth Aggregation

Each layer in the hierarchical network model is a possible candidate for bandwidth aggregation. Bandwidth aggregation is the combining of two or more connections to create a logically singular higher bandwidth connection. After bandwidth requirements of the network are known, links between specific switches can be aggregated, which is called link aggregation. Link aggregation allows multiple switch port links to be combined so as to achieve higher throughput between switches. Cisco has a proprietary link aggregation technology called EtherChannel, which allows multiple Ethernet links to be consolidated. A discussion of EtherChannel is beyond the scope of this book. To learn more, visit

www.cisco.com/en/US/tech/tk389/tk213/tsd_technology_support_protocol_home.html.

In Figure 1-4, computers PC1 and PC3 require a significant amount of bandwidth because they are frequently used for streaming video. The network manager has determined that the access layer switches S1, S3, and S5 require increased bandwidth. Following up the hierarchy, these access layer switches connect to the distribution switches D1, D2, and D4. The distribution switches connect to core layer switches C1 and C2. Notice how specific links on specific ports in each switch are aggregated. In this way, increased bandwidth is provided for in a targeted, specific part of the network. As is customary, aggregated links are indicated in this figure by two dotted lines with an oval tying them together. The path PC1-S1-D1-C1-C2-D4-S5-PC3 enjoys the enhanced bandwidth resulting from aggregating links.

Figure 1-4 Bandwidth Aggregation



Redundancy

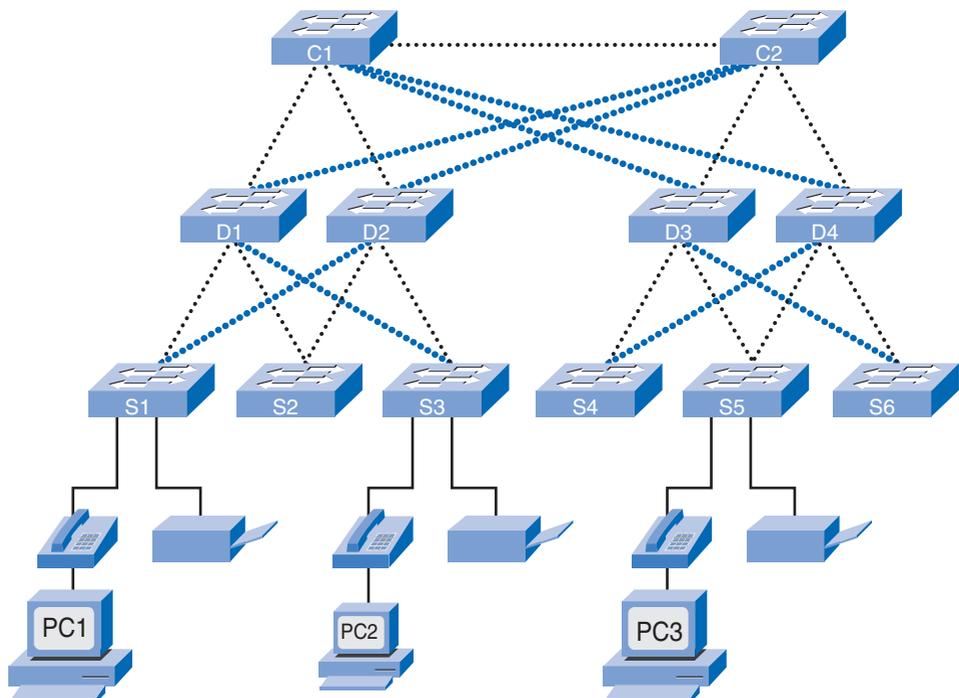
Redundancy is one part of creating a highly available network. Redundancy can be provided in a number of ways. For example, you can double up the network connections between devices, or you can double the devices themselves. This chapter explores how to employ redundant network paths between switches. A discussion on doubling up network devices and employing special network protocols to ensure high availability is beyond the scope of this book. For an interesting discussion on high availability, visit

www.cisco.com/en/US/products/ps6550/products_ios_technology_home.html.

Implementing redundant links can be expensive. Imagine if every switch in each layer of the network hierarchy had a connection to every switch at the next layer. It is unlikely that you will be able to implement redundancy at the access layer because of the cost and limited features in the end devices, but you can build redundancy into the distribution and core layers of the network.

In Figure 1-5, redundant links are shown at the distribution layer and core layer. At the distribution layer are four distribution layer switches; two distribution layer switches is the minimum required to support redundancy at this layer. The access layer switches, S1, S3, S4, and S6, are cross-connected to the distribution layer switches. The bolder dotted lines here indicate the secondary redundant uplinks. This protects your network if one of the distribution switches fails. In case of a failure, the access layer switch adjusts its transmission path and forwards the traffic through the other distribution switch.

Figure 1-5 Redundancy



Some network failure scenarios can never be prevented—for example, if the power goes out in the entire city, or the entire building is demolished because of an earthquake.

Redundancy does not attempt to address these types of disasters. To learn more about how a business can continue to work and recover from a disaster, visit

www.cisco.com/en/US/netsol/ns516/networking_solutions_package.html.

Imagine that a new network design is required. Design requirements, such as the level of performance or redundancy necessary, are determined by the business goals of the organization. After the design requirements are documented, the designer can begin selecting the equipment and infrastructure to implement the design.

When you start the equipment selection at the access layer, you can ensure that you accommodate all network devices needing access to the network. After you have all end devices accounted for, you have a better idea of how many access layer switches you need. The number of access layer switches, and the estimated traffic that each generates, helps you to determine how many distribution layer switches are required to achieve the performance and redundancy needed for the network. After you have determined the number of distribution layer switches, you can identify how many core switches are required to maintain the performance of the network.

A thorough discussion on how to determine which switch to select based on traffic flow analysis and how many core switches are required to maintain performance is beyond the scope of this book. For a good introduction to network design, an excellent reference is *Top-Down Network Design*, by Priscilla Oppenheimer, available at ciscopress.com.

What Is a Converged Network?

Small- and medium-sized businesses are embracing the idea of running voice and video services on their data networks. Let us look at how *voice over IP (VoIP)* and video over IP affect a hierarchical network.

Legacy Equipment

Convergence is the process of combining voice and video communications on a data network. Converged networks have existed for a while now, but were feasible only in large enterprise organizations because of the network infrastructure requirements and complex management that was involved to make them work seamlessly. High network costs were associated with convergence because more expensive switch hardware was required to support the additional bandwidth requirements. Converged networks also required extensive management in relation to *quality of service (QoS)*, because voice and video data traffic needed to be classified and prioritized on the network. Few individuals had the expertise in voice, video, and data networks to make convergence feasible and functional. In addition, legacy equipment hinders the process. Figure 1-6 shows legacy telephone company switches and a legacy wiring closet. Also, many offices still use analog phones, so they still have

existing analog telephone wiring closets. Because analog phones have not yet been replaced, you will see equipment that has to support both legacy *private branch exchange (PBX)* telephone systems and IP-based phones. This sort of equipment will slowly be migrated to modern IP-based phone switches. IP phones replace analog phones and IP PBXs, such as Cisco CallManager, replace PBXs.

Figure 1-6 Legacy Equipment



Large Telephone Switches



Small PBX Systems



Wiring Closet Infrastructure

Advanced Technology

Converging voice, video, and data networks has become more popular recently in the small- to medium-sized business market because of advancements in technology. Convergence is now easier to implement and manage, and less expensive to purchase. Figure 1-7 shows a high-end IP phone and switch combination suitable for a medium-sized business of 250 to 400 employees. The figure also shows a Cisco Catalyst Express 500 switch and a Cisco 7906G phone suitable for small- to medium-sized businesses. This VoIP technology used to be affordable only to enterprises and governments.

Moving to a converged network can be a difficult decision if the business already invested in separate voice, video, and data networks. It is difficult to abandon an investment that still works, but there are several advantages to converging voice, video, and data on a single network infrastructure.

Figure 1-7 VoIP Equipment

Catalyst 6500 and IP Phone



Cisco 7906G Phone



Catalyst Express 500 Switches

One benefit of a converged network is that there is just one network to manage. With separate voice, video, and data networks, changes to the network have to be coordinated across networks. Also, additional costs result from using three sets of network cabling. Using a single network means you have to manage just one wired infrastructure.

Other benefits are lower implementation and management costs. It is less expensive to implement a single network infrastructure than three distinct network infrastructures. Managing a single network is also less expensive. Traditionally, if a business has a separate voice and data network, it has one group of people managing the voice network and another group managing the data network. With a converged network, you have one group managing both the voice and data networks.

New Options

Converged networks give you options that had not existed previously. You can now tie voice and video communications directly into an employee's personal computer system, as shown in Figure 1-8.

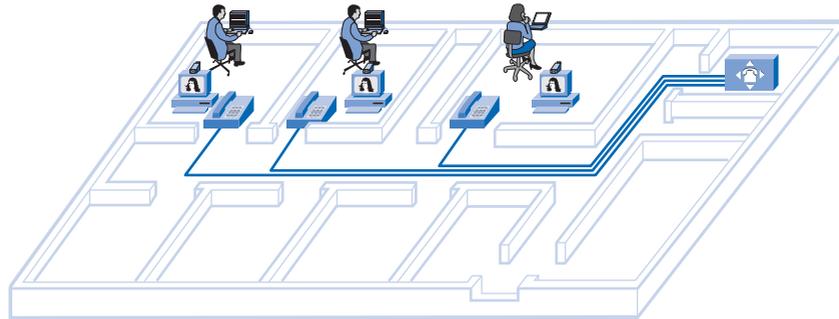
Figure 1-8 Advanced Voice and Video Communications

There is no need for an expensive handset phone or videoconferencing equipment. You can accomplish the same function using special software integrated with a personal computer. Softphones, such as the Cisco Unified Personal Communicator for PC or Mac, offer a lot of flexibility for businesses. The person in the top left of Figure 1-8 is using a softphone on the computer. When software is used in place of a physical phone, a business can quickly convert to converged networks because there is no capital expense in purchasing IP phones and the switches needed to power the phones. With the addition of inexpensive webcams, videoconferencing can be added to a softphone. These are just a few examples provided by a broader communications solution portfolio that redefine business processes today.

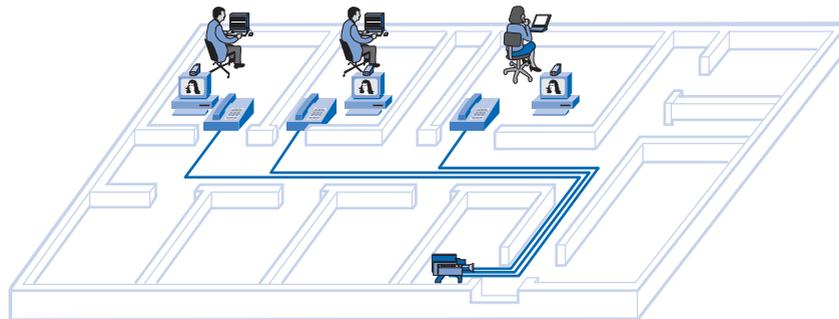
Separate Voice, Video, and Data Networks

The new options for software and hardware for the purpose of integrating voice, video, and data, force the issue of redesigning existing networks to support these devices. It is no longer feasible to separate out the voice, video, and data networks.

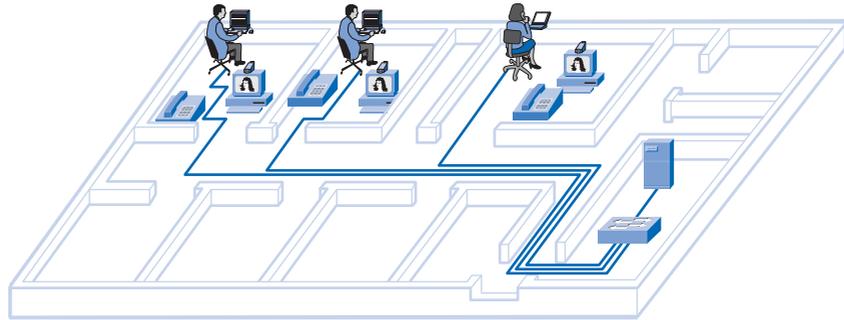
As you see in Figure 1-9, a legacy voice network contains isolated phone lines running to a PBX switch to allow phone connectivity to the Public Switched Telephone Network (PSTN). When a new phone is added, a new line has to be run back to the PBX. The PBX switch is typically located in a Telco wiring closet, separate from the data and video wiring closets. The wiring closets are usually separated because different support personnel require access to each system. However, using a properly designed hierarchical network and implementing QoS policies that prioritize the audio data, voice data can be converged onto an existing data network with little to no impact on audio quality.

Figure 1-9 Voice Network

In Figure 1-10, videoconferencing equipment is wired separately from the voice and data networks. Videoconferencing data can consume significant bandwidth on a network. As a result, video networks were maintained separately to allow the videoconferencing equipment to operate at full speed without competing for bandwidth with voice and data streams. Using a properly designed hierarchical network and implementing QoS policies that prioritize the video data, video can be converged onto an existing data network with little to no impact on video quality.

Figure 1-10 Video Network

The data network, shown in Figure 1-11, interconnects the workstations and servers on a network to facilitate resource sharing. Data networks can consume significant data bandwidth, which is why voice, video, and data networks were kept separated for such a long time. Now that properly designed hierarchical networks can accommodate the bandwidth requirements of voice, video, and data communications at the same time, it makes sense to converge them all onto a single hierarchical network.

Figure 1-11 Data Network

Matching Switches to Specific LAN Functions

To select the appropriate switch for a one of the hierarchical network layers, you need to have specifications that detail the target traffic flows, user community, data stores, and data servers. We continue our discussion of switched LAN design with an analysis of topology diagrams, switch features, classification of switches, Power over Ethernet, Layer 3 functionality, and Cisco switch platforms appropriate for small- and medium-sized businesses.

Considerations for Hierarchical Network Switches

Companies need a network that can meet evolving requirements. A business may start with a few PCs interconnected so that they can share data. As the business adds more employees, devices such as PCs, printers, and servers are added to the network. Accompanying the new devices is an increase in network traffic. Some companies are replacing their existing telephone systems with converged VoIP phone systems, which adds additional traffic.

When selecting switch hardware, determine which switches are needed in the core, distribution, and access layers to accommodate the bandwidth requirements of your network. Your plan should take into account future bandwidth requirements. Purchase the appropriate Cisco switch hardware to accommodate both current needs as well as future needs. To help you more accurately choose appropriate switches, perform and record traffic flow analyses on a regular basis.

Traffic Flow Analysis

Traffic flow analysis is the process of measuring the bandwidth usage on a network and analyzing the data for the purpose of performance tuning, capacity planning, and making hardware improvement decisions. Traffic flow analysis is done using traffic flow analysis software. Although there is no precise definition of network traffic flow, for the purposes of traffic flow analysis we can say that network traffic is the amount of data sent through a network for a given period of time. All network data contributes to the traffic, regardless of its purpose or

source. Analyzing the various traffic sources and their impact on the network allows you to more accurately tune and upgrade the network to achieve the best possible performance.

Traffic flow data can be used to help determine just how long you can continue using existing network hardware before it makes sense to upgrade to accommodate additional bandwidth requirements. When you are making your decisions about which hardware to purchase, you should consider port densities and switch forwarding rates to ensure adequate growth capability. Port density is the number of ports per switch.

You can monitor traffic flow on a network in many ways. You can manually monitor individual switch ports to get the bandwidth utilization over time. When analyzing the traffic flow data, you want to determine future traffic flow requirements based on the capacity at certain times of the day and where most of the data is generated and sent. However, to obtain accurate results, you need to record enough data. Manual recording of traffic data is a tedious process that requires a lot of time and diligence. Fortunately, there are some automated solutions.

Analysis Tools

Many traffic flow analysis tools that automatically record traffic flow data to a database and perform a trend analysis are available. In large networks, software collection solutions are the only effective method for performing traffic flow analysis. Figure 1-12 displays sample output from Solarwinds Orion 8.1 NetFlow Analysis, which monitors traffic flow on a network. Using the included charts, you can identify traffic flow problems visually. This is much easier than having to interpret the numbers in a column of traffic flow data.

Figure 1-12 Traffic Flow Analysis



For a list of some commercial traffic flow collection and analysis tools, visit www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/index.shtml.

For a list of some freeware traffic flow collection and analysis tools, visit www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/index.shtml.

User Community Analysis

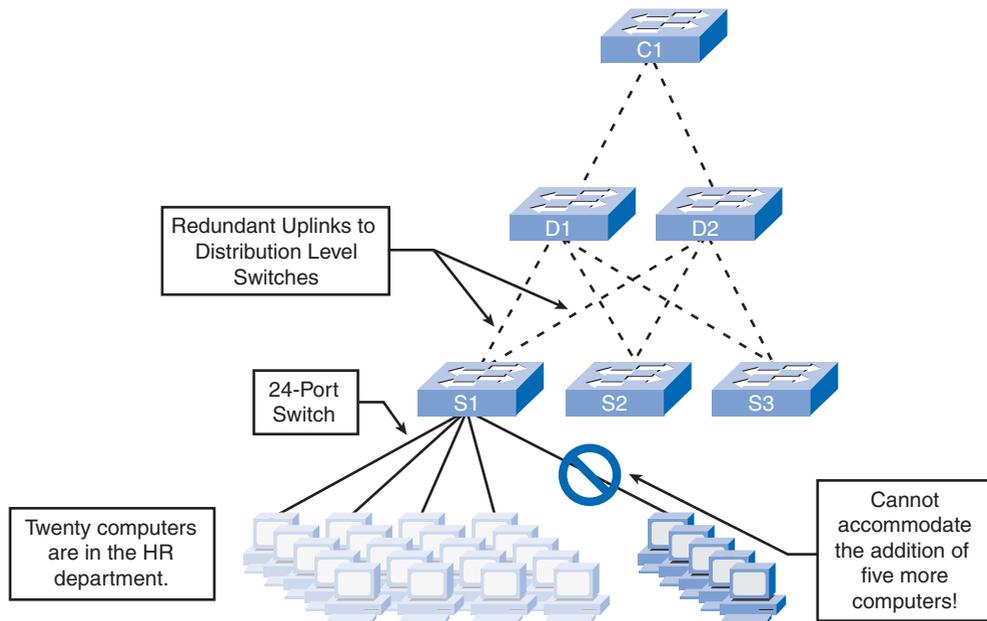
User community analysis is the process of identifying various groupings of users and their impact on network performance. The way users are grouped affects issues related to port density and traffic flow, which, in turn, influence the selection of network switches.

In a typical office building, end users are grouped according to their job function because they require similar access to resources and applications. You may find the Human Resource (HR) department located on one floor of an office building, whereas Finance is located on another floor. Each department has a different number of users and application needs and requires access to different data resources available through the network. For example, when selecting switches for the wiring closets of the HR and Finance departments, you would choose a switch that had enough ports to meet the department needs and was powerful enough to accommodate the traffic requirements for all the devices on that floor. Additionally, a good network-design plan factors in the growth of each department to ensure that there are enough open switch ports that can be utilized before the next planned upgrade to the network.

As shown in Figure 1-13, the HR department requires 20 workstations for its 20 users. That translates to 20 switch ports needed to connect the workstations to the network. If you were to select an appropriate access layer switch to accommodate the HR department, you would probably choose a 24-port switch, which has enough ports to accommodate the 20 workstations and the uplinks to the distribution layer switches.

But this plan does not account for future growth. Consider what will happen if the HR department grows by five employees, as shown on the bottom right of Figure 1-13. A solid network plan includes the rate of personnel growth over the past five years to be able to anticipate the future growth. With that in mind, you would want to purchase a switch that can accommodate more than 24 ports, such as stackable or modular switches that can scale.

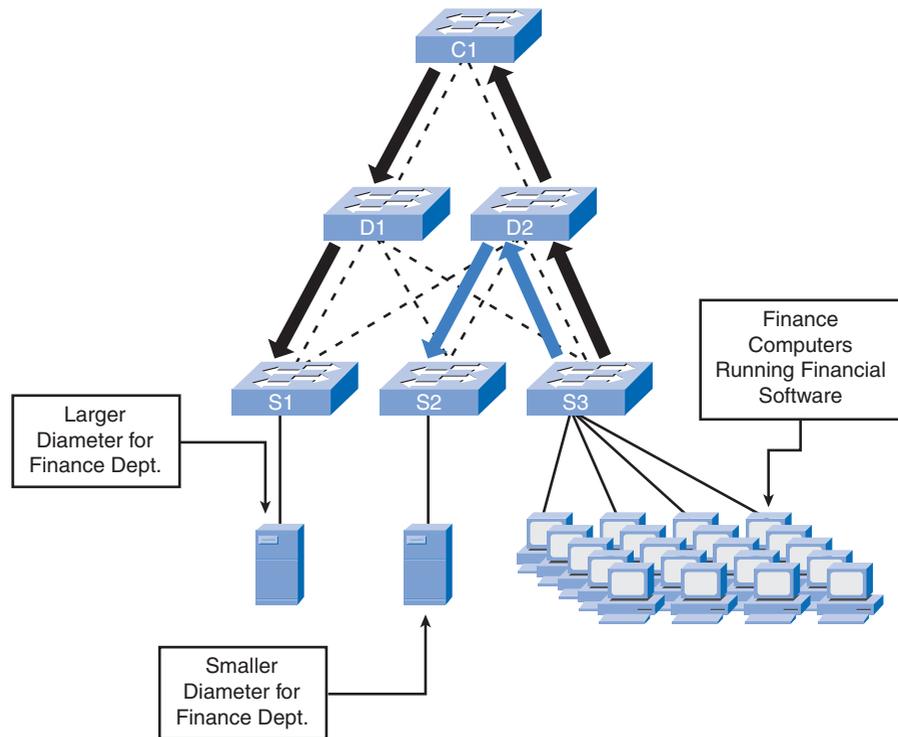
As well as looking at the number of devices on a given switch in a network, you should investigate the network traffic generated by end-user applications. Some user communities use applications that generate a lot of network traffic, whereas other user communities do not. By measuring the network traffic generated for all applications in use by different user communities, and determining the location of the data source, you can identify the effect of adding more users to that community.

Figure 1-13 HR Department Analysis

A workgroup-sized user community in a small business is supported by a couple of switches and is typically connected to the same switch as the server. In medium-sized businesses or enterprises, user communities are supported by many switches. The resources that medium-sized business or enterprise user communities need could be located in geographically separate areas. Consequently, the location of the user communities influences where data stores and server farms are located.

If the Finance users are using a network-intensive application that exchanges data with a specific server on the network, as shown in Figure 1-14, it may make sense to locate the Finance user community close to that server. By locating users close to their servers and data stores, you can reduce the network diameter for their communications, thereby reducing the impact of their traffic across the rest of the network. Note that spanning-tree protocol (STP), discussed in Chapter 5, is a determining factor in the displayed network diameters.

One complication of analyzing application usage by user communities is that usage is not always bound by department or physical location. You may have to analyze the impact of the application across many network switches to determine its overall impact.

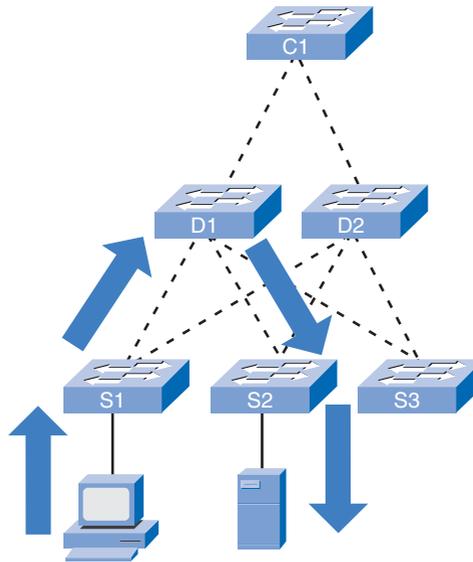
Figure 1-14 Finance Department Analysis

Data Stores and Data Servers Analysis

When analyzing traffic on a network, consider where the data stores and servers are located so that you can determine the impact of traffic on the network. Data stores can be servers, storage area networks (SANs), network-attached storage (NAS), tape backup units, or any other device or component where large quantities of data are stored.

When considering the traffic for data stores and servers, consider both client/server traffic and server/server traffic.

As you can see in Figure 1-15, client/server traffic is the traffic generated when a client device accesses data from data stores or servers. Client/server traffic typically traverses multiple switches to reach its destination. Bandwidth aggregation and switch forwarding rates are important factors to consider when attempting to eliminate bottlenecks for this type of traffic.

Figure 1-15 Client/Server Communication

Server/server traffic, shown in Figure 1-16, is the traffic generated between data storage devices on the network. Some server applications generate very high volumes of traffic between data stores and other servers. To optimize server/server traffic, servers needing frequent access to certain resources should be located in close proximity to each other so that the traffic they generate does not affect the performance of the rest of the network. Servers and data stores are typically located in data centers within a business. A data center is a secured area of the building where servers, data stores, and other network equipment are located. A device can be physically located in the data center but represented in quite a different location in the logical topology. Traffic across data center switches is typically very high because of the server/server and client/server traffic that traverses the switches. As a result, switches selected for data centers should be higher-performing switches than the switches you would find in the wiring closets at the access layer.

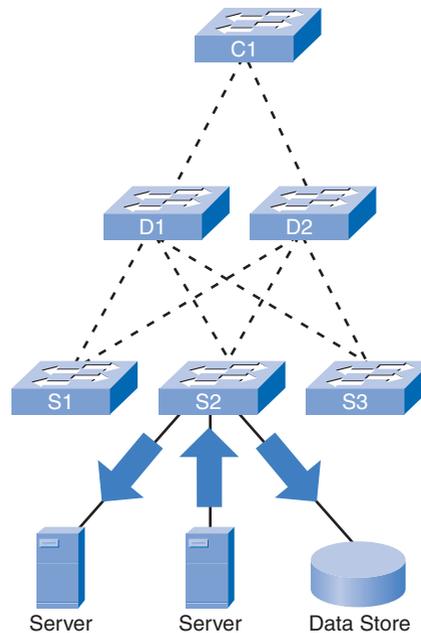
By examining the data paths for various applications used by different user communities, you can identify potential bottlenecks where performance of the application can be affected by inadequate bandwidth. To improve the performance, you could aggregate links to accommodate the bandwidth, or replace the slower switches with faster switches capable of handling the traffic load.

Topology Diagrams

A topology diagram is a graphical representation of a network infrastructure. A topology diagram shows how all switches are interconnected, detailed down to which switch port interconnects the devices. A topology diagram graphically displays any redundant paths or

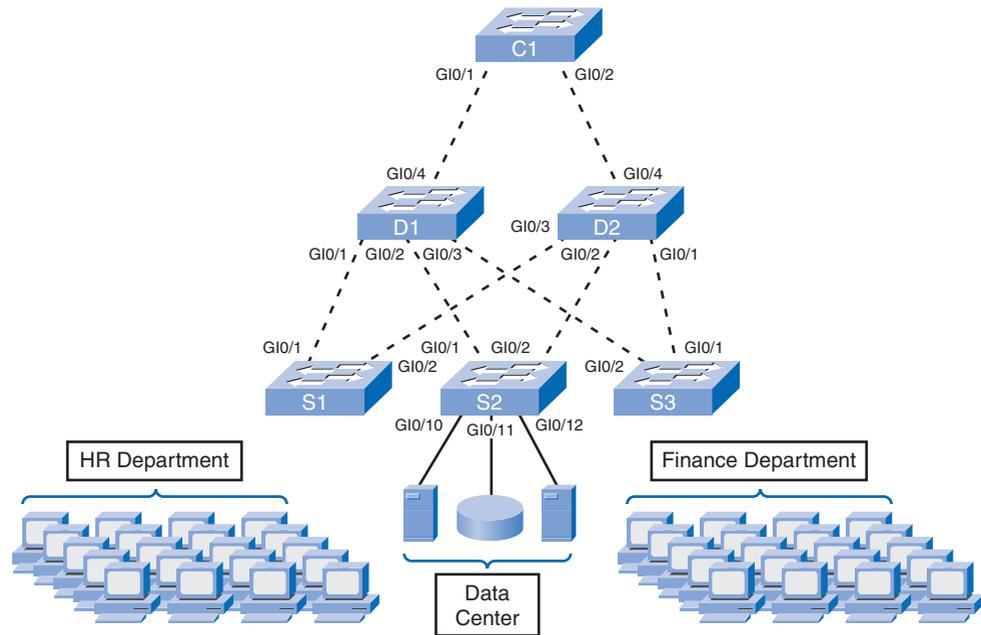
aggregated ports between switches that provide for resiliency and performance. It shows where and how many switches are in use on your network, and identifies their configuration. Topology diagrams can also contain information about device densities and user communities. Having a topology diagram allows you to visually identify potential bottlenecks in network traffic so that you can focus your traffic analysis data collection on areas where improvements can have the most impact on performance.

Figure 1-16 Server/Server Communication



A network topology can be very difficult to piece together after the fact if you were not part of the design process. Network cables in the wiring closets disappear into the floors and ceilings, making it difficult to trace their destinations. And because devices are spread throughout the building, it is difficult to know how all the pieces are connected together. Constructing a topology diagram from the physical layout of the network becomes a tedious and time-consuming exercise; however, this is an important piece of network documentation that significantly enhances the maintenance and troubleshooting of the network and should be done regardless of the current health of the network.

Figure 1-17 displays a simple network topology diagram. Notice how many switches are present in the network, as well as how each switch is interconnected. The topology diagram identifies each switch port used for interswitch communications and redundant paths between access layer switches and distribution layer switches. The topology diagram also displays where different user communities are located on the network and the location of the servers and data stores.

Figure 1-17 Topology Diagrams

Switch Features

What are the key features of switches that are used in hierarchical networks? When you look up the specifications for a switch, what do all the acronyms and word phrases mean? What does “PoE” mean and what is “forwarding rate”? In this section, you will learn about these features.

Switch Form Factors

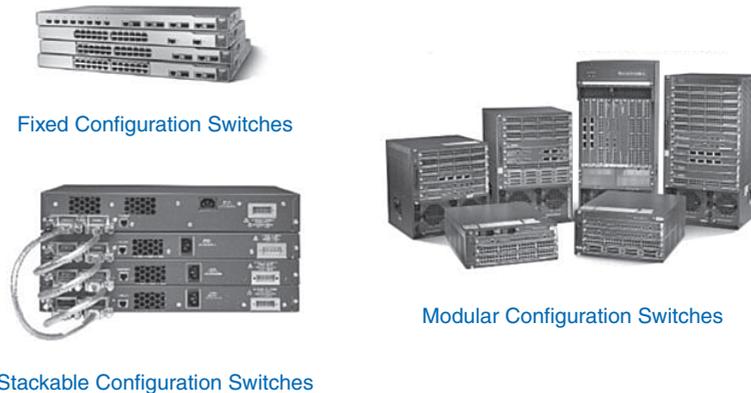
When you are selecting a switch, you need to decide between fixed configuration or modular configuration, and stackable or nonstackable. Another consideration is the thickness of the switch expressed in number of rack units. For example, the fixed configuration switches shown in Figure 1-18 are all 1 rack unit (1U). The physical size of the switches can be an important consideration when selecting switches to be deployed. Networking equipment in a hierarchical design is placed into central locations, such as the wiring closets; oftentimes, the space in these areas is limited, and switch form factors (physical configuration) becomes a significant issue.

Fixed Configuration Switches

Fixed configuration switches are just as you might expect, fixed in their configuration. What that means is that you cannot add features or options to the switch beyond those that

originally came with the switch. The particular model you purchase determines the features and options available. For example, if you purchase a 24-port gigabit fixed switch, you cannot add additional ports when you need them. Typically, different configuration choices vary in how many and what types of ports are included.

Figure 1-18 Switch Form Factors



Modular Switches

Modular switches offer more flexibility in their configuration. Modular switches come with different sized chassis that allow for the installation of different numbers of modular line cards. The line cards contain the ports. The line card fits into the switch chassis like expansion cards fit into a PC. The larger the chassis, the more modules it can support. As you can see in Figure 1-18, you can choose from many chassis sizes. If you bought a modular switch with a 24-port line card, you could easily add an additional 24-port line card to bring the total number of ports up to 48.

Stackable Switches

Stackable switches can be interconnected using a special backplane cable that provides high-bandwidth throughput between the switches. Cisco introduced StackWise technology in one of its switch product lines. StackWise allows you to interconnect up to nine switches using fully redundant backplane connections. As you can see in Figure 1-18, switches are stacked one atop of the other, and cables connect the switches in daisy-chain fashion. The stacked switches effectively operate as a single larger switch. Stackable switches are desirable where fault tolerance and bandwidth availability are critical and a modular switch is too costly to implement. Using cross-connected connections, the network can recover quickly if a single switch fails. Stackable switches use a special port for interconnections and do not use line ports for interswitch connections. The speeds are also typically faster than using line ports for connection switches.

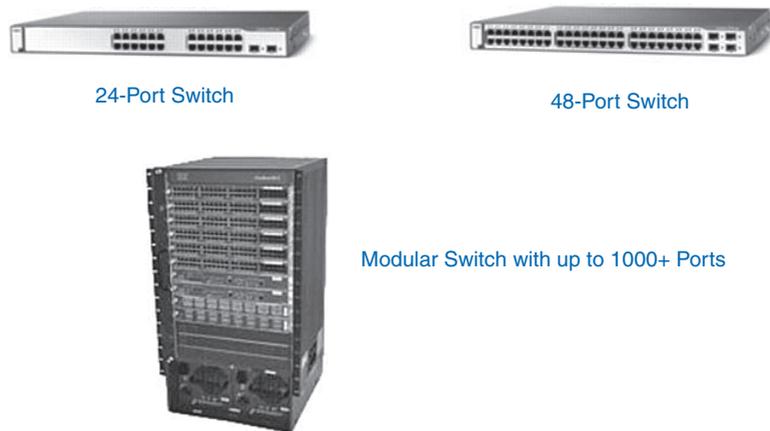
Switch Performance

When selecting a switch for the access, distribution, or core layers, consider the capability of the switch to support the port density, forwarding rates, and bandwidth aggregation requirements of your network.

Port Density

Port density is the number of ports available on a single switch. Fixed configuration switches typically support up to 48 ports on a single device, with options for up to four additional ports for small form-factor pluggable (SFP) devices, as shown in the 48-port switch in Figure 1-19. High port densities allow for better use of space and power when both are in limited supply. If you have two switches that each contain 24 ports, you would be able to support up to 46 devices because you lose at least one port per switch to connect each switch to the rest of the network. In addition, two power outlets are required. On the other hand, if you have a single 48-port switch, 47 devices can be supported, with only one port used to connect the switch to the rest of the network, and only one power outlet needed to accommodate the single switch.

Figure 1-19 Port Density



Modular switches can support very high port densities through the addition of multiple switch port line cards, as shown in Figure 1-19. For example, the Catalyst 6500 switch can support in excess of 1000 switch ports on a single device.

Large *enterprise networks* that support many thousands of network devices require high density, modular switches to make the best use of space and power. Without using a high-density modular switch, the network would need many fixed configuration switches to accommodate the number of devices that need network access. This approach can consume many power outlets and a lot of closet space.

You must also address the issue of uplink bottlenecks. A series of fixed configuration switches may consume many additional ports for bandwidth aggregation between switches for the purpose of achieving target performance. With a single modular switch, bandwidth aggregation is less of an issue because the backplane of the chassis can provide the necessary bandwidth to accommodate the devices connected to the switch port line cards.

Forwarding Rates

As illustrated in Figure 1-20, forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates. Entry-layer switches have lower forwarding rates than enterprise-layer switches. Forwarding rates are important to consider when selecting a switch. If the switch forwarding rate is too low, it cannot accommodate full wire-speed communication across all its switch ports. Wire speed is the data rate that each port on the switch is capable of attaining—either 100 Mbps Fast Ethernet or 1000 Mbps Gigabit Ethernet. For example, a 48-port gigabit switch operating at full wire speed generates 48 Gbps of traffic. If the switch supports a forwarding rate of only 32 Gbps, it cannot run at full wire speed across all ports simultaneously. Fortunately, access layer switches typically do not need to operate at full wire speed because they are physically limited by their uplinks to the distribution layer. This allows you to use less expensive, lower-performing switches at the access layer, and use the more expensive, higher-performing switches at the distribution and core layers, where the forwarding rate makes a bigger difference.

Figure 1-20 Forwarding Rates



Link Aggregation

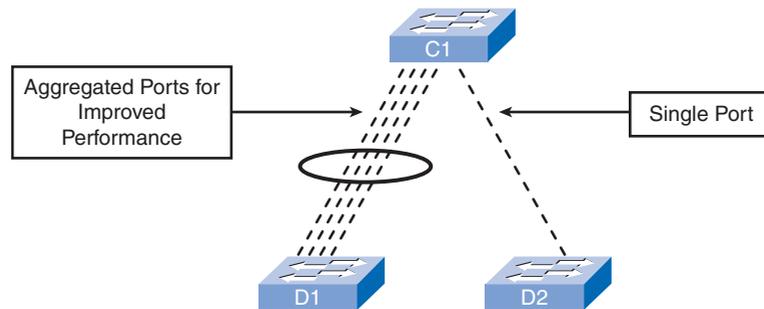
As part of bandwidth aggregation, you should determine if there are enough ports on a switch to aggregate to support the required bandwidth. For example, consider a Gigabit Ethernet port, which carries up to 1 Gbps of traffic. If you have a 24-port switch, with all ports capable of running at gigabit speeds, you could generate up to 24 Gbps of network traffic. If the switch is connected to the rest of the network by a single network cable, it can forward only 1 Gbps of the data to the rest of the network. Due to the contention for bandwidth, the data would forward more slowly. That results in 1/24th wire speed available to each of the 24 devices connected to the switch. Wire speed describes the theoretical maximum data transmission rate of a connection.

Link aggregation helps to reduce these bottlenecks of traffic by allowing up to eight switch ports to be bound together for data communications, providing up to 16 Gbps of data

throughput when Gigabit Ethernet ports are used. With the addition of multiple 10 Gigabit Ethernet uplinks on some enterprise-layer switches, 160 Gbps throughput rates can be achieved. Cisco uses the term EtherChannel when describing aggregated switch ports. Keep in mind that EtherChannel reduces the number of available ports to connect network devices.

As you can see in Figure 1-21, four separate ports on switches C1 and D1 are used to create a 4-port EtherChannel. EtherChannel technology allows a group of physical Ethernet links to create one logical Ethernet link for the purpose of providing fault tolerance and high-speed links between switches, routers, and servers. In this example, there is four times the throughput when compared to the single port connection between switches C1 and D2.

Figure 1-21 Link Aggregation



Power over Ethernet and Layer 3 Functionality

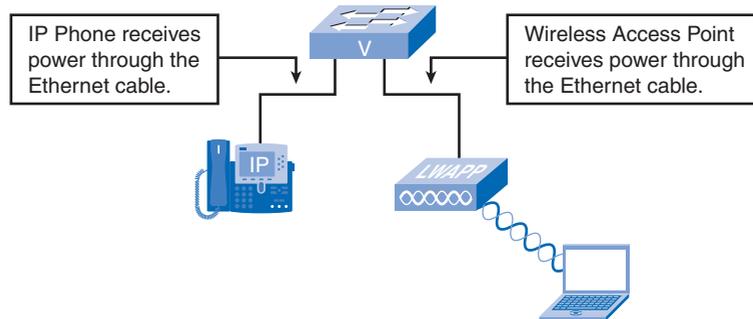
Two other characteristics you want to consider when selecting a switch are Power over Ethernet (PoE) and Layer 3 functionality.

Power over Ethernet

Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. As you can see in Figure 1-22, this feature can be used by IP phones and some wireless access points.

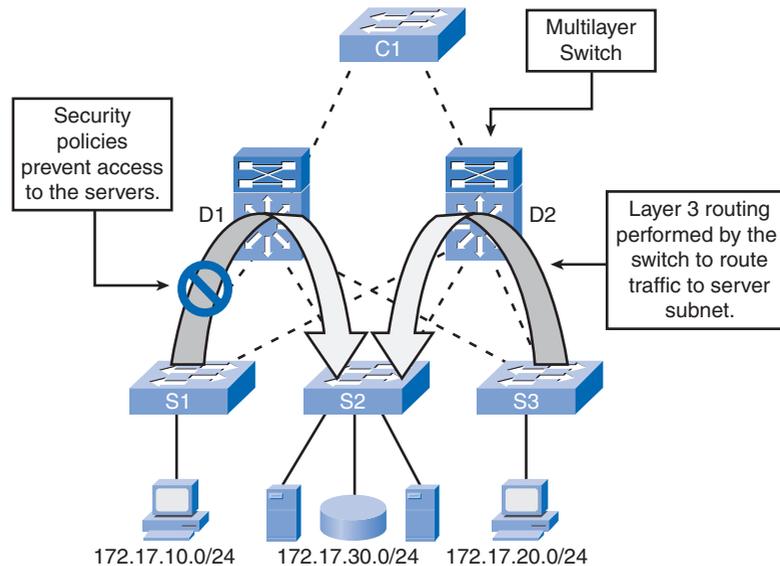
PoE ports on a switch, IP phone, access point, and wireless LAN controller look the same as any switch port, as shown in Figure 1-23. Check the model of the networking device to determine whether the port supports PoE.

PoE allows you more flexibility when installing wireless access points and IP phones because you can install them anywhere you can run an Ethernet cable. You do not need to consider how to run ordinary power to the device. You should select a switch that supports PoE only if you are actually going to take advantage of the feature because it adds considerable cost to the switch.

Figure 1-22 Power over Ethernet**Figure 1-23** Appearance of Power over Ethernet Ports

Layer 3 Functionality

Typically, switches operate at Layer 2 of the OSI reference model, where they deal primarily with the MAC addresses of devices connected to switch ports. Layer 3 switches offer advanced functionality that will be discussed in greater detail in the later chapters of this book. Layer 3 switches are also known as *multilayer switches*. Figure 1-24 illustrates some functions of Layer 3 switches.

Figure 1-24 Layer 3 Switch Functionality

Switch Features in a Hierarchical Network

Now that you know which factors to consider when choosing a switch, let us examine which features are required at each layer in a hierarchical network. You will then be able to match the switch specification with its capability to function as an access, distribution, or core layer switch.

Access Layer Switch Features

Access layer switches facilitate the connection of end node devices to the network. For this reason, they need to support features such as port security, VLANs, Fast Ethernet/Gigabit Ethernet, PoE, and link aggregation, as shown in Figure 1-25.

Port security allows the switch to decide how many or what specific devices are allowed to connect to the switch. All Cisco switches support port layer security. Port security is applied at the access. Consequently, it is an important first line of defense for a network. You will learn about port security in Chapter 2, “Basic Switch Concepts and Configuration.”

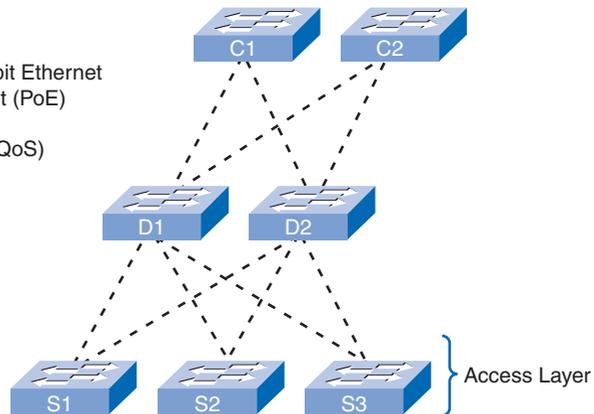
VLANs are an important component of a converged network. Voice traffic is typically given a separate VLAN. In this way, voice traffic can be supported with more bandwidth, more redundant connections, and improved security. Access layer switches allow you to set the VLANs for the end node devices on your network.

Port speed is also a characteristic you need to consider for your access layer switches. Depending on the performance requirements for your network, you must choose between Fast Ethernet and Gigabit Ethernet switch ports. Fast Ethernet allows up to 100 Mbps of traffic per switch port. Fast Ethernet is adequate for IP telephony and data traffic on most business

networks; however, performance is slower than Gigabit Ethernet ports. Gigabit Ethernet allows up to 1000 Mbps of traffic per switch port. Most modern devices, such as workstations, notebooks, and IP phones, support Gigabit Ethernet. This allows for much more efficient data transfers, enabling users to be more productive. Gigabit Ethernet does have a drawback—switches supporting Gigabit Ethernet are more expensive.

Figure 1-25 Access Layer Switch Features

- Port Security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link Aggregation
- Quality of Service (QoS)



Another feature requirement for some access layer switches is PoE. PoE dramatically increases the overall price of the switch across all Cisco Catalyst switch product lines, so it should be considered only when voice convergence is required or wireless access points are being implemented, and power is difficult or expensive to run to the desired location.

Link aggregation is another feature that is common to most access layer switches. Link aggregation allows the switch to operate multiple links simultaneously as a logically singular high bandwidth link. Access layer switches take advantage of link aggregation when aggregating bandwidth up to distribution layer switches.

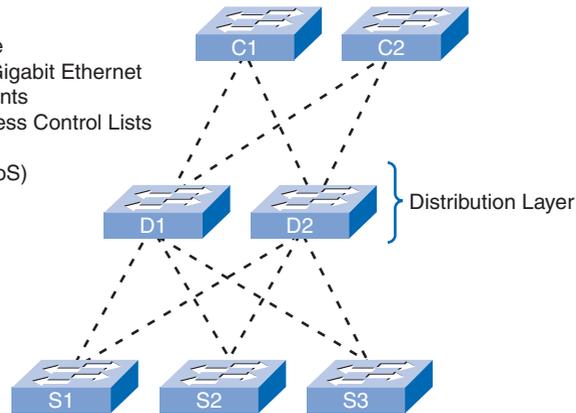
Although the uplink connection between the access layer and distribution layer switches can become a bottleneck, it does not present a significant bottleneck to the entire network, because the effect is localized to the devices connected to the switch. The uplink from the distribution layer to the core presents a much more significant bottleneck to the entire network because distribution layer switches collect the traffic of multiple network segments. Bottlenecks present a much more significant quality of service issue for voice and video data than they do for data; this is because voice and video cannot afford gaps and delays in transmissions for obvious reasons. In a converged network supporting voice, video, and data network traffic, access layer switches need to support QoS to maintain the prioritization of traffic. Cisco IP phones are types of equipment that are found at the access layer. When a Cisco IP phone is plugged into an access layer switch port configured to support voice traffic, that switch port tells the IP phone how to send its voice traffic. QoS needs to be enabled on access layer switches so that voice traffic from the IP phone has priority over, for example, data traffic.

Distribution Layer Switch Features

Distribution layer switches have a very important role on the network. Features of distribution layer switches are illustrated in Figure 1-26.

Figure 1-26 Distribution Layer Switch Features

- Layer 3 Support
- High Forwarding Rate
- Gigabit Ethernet/10 Gigabit Ethernet
- Redundant Components
- Security Policies/Access Control Lists
- Link Aggregation
- Quality of Service (QoS)



Distribution layer switches receive the data from all the access layer switches and forward it to the core layer switches. As you will learn later in this book, traffic that is generated at Layer 2 on a switched network needs to be managed, or segmented into VLANs, so it does not needlessly consume bandwidth throughout the network. Distribution layer switches provide the inter-VLAN routing functions so that one VLAN can communicate with another on the network. This routing typically takes place at the distribution layer because distribution layer switches have higher processing capabilities than the access layer switches. Distribution layer switches alleviate the core switches from needing to perform that task, because the core is busy handling the forwarding of very high volumes of traffic. Because inter-VLAN routing is performed at the distribution layer, the switches at this layer need to support Layer 3 functions.

Another reason why Layer 3 functionality is required for distribution layer switches is because of the advanced security policies that can be applied to network traffic. Access lists are used to control how traffic flows through the network. An access control list (ACL) allows the switch to prevent certain types of traffic and permit others. ACLs also allow you to control which network devices can communicate on the network. Using ACLs is processing-intensive because the switch needs to inspect every packet to see if it matches one of the ACL rules defined on the switch. This inspection is performed at the distribution layer because the switches at this layer typically have the processing capability to handle the additional load, and it also simplifies the use of ACLs. Instead of using ACLs for every access layer switch in the network, they are defined on the fewer distribution layer switches, making management of the ACLs much easier.

The distribution layer switches are under high demand on the network because of the functions that they provide. It is important that distribution switches support redundancy for adequate

availability. Loss of a distribution layer switch could have a significant impact on the rest of the network because all access layer traffic passes through the distribution layer switches. Distribution layer switches are typically implemented in pairs to ensure availability. It is also recommended that distribution layer switches support multiple, hot-swappable power supplies. Having more than one power supply allows the switch to continue operating even if one of the power supplies failed during operation. Having hot-swappable power supplies allows you to change a failed power supply while the switch is still running. This allows you to repair the failed component without impacting the functionality of the network.

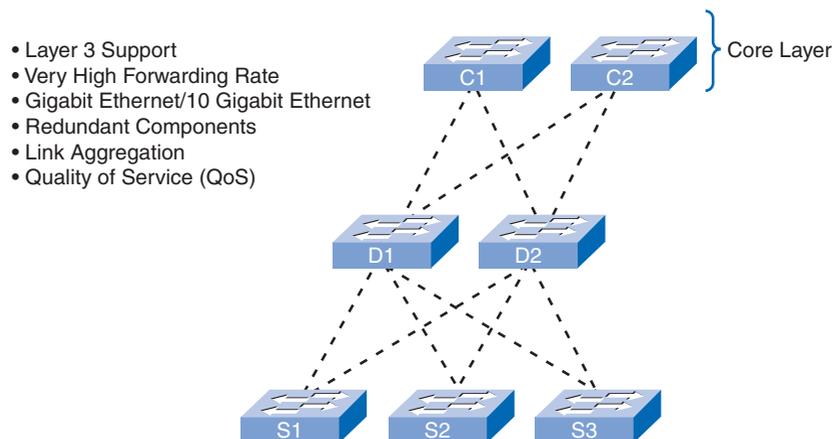
Also, distribution layer switches need to support link aggregation. Typically, access layer switches use multiple links to connect to a distribution layer switch to ensure adequate bandwidth to accommodate the traffic generated on the access layer and provide fault tolerance in case a link is lost. Because distribution layer switches accept incoming traffic from multiple access layer switches, they need to be able to forward all that traffic as fast as possible to the core layer switches. As a result, distribution layer switches also need high-bandwidth aggregated links back to the core layer switches. Newer distribution layer switches support aggregated 10 Gigabit Ethernet (10GbE) uplinks to the core layer switches.

Finally, distribution layer switches need to support QoS to maintain the prioritization of traffic coming from the access layer switches that have implemented QoS. Priority policies ensure that audio and video communications are guaranteed adequate bandwidth to maintain an acceptable quality of service. To maintain the priority of the voice data throughout the network, all the switches that forward voice data must support QoS; if not all the network devices support QoS, the benefits of QoS will be reduced. This results in poor performance and quality for audio and video communications.

Core Layer Switch Features

Core layer switches are responsible for handling the majority of data on a switched LAN. Core layer switch features are illustrated in Figure 1-27.

Figure 1-27 Core Layer Switch Features



The core layer of a hierarchical topology is the high-speed backbone of the network and requires switches that can handle very high forwarding rates. The required forwarding rate is largely dependent on the number of devices participating in the network. You determine the necessary forwarding rate by conducting and examining various traffic flow reports and user community analyses. Based on your results, you can identify an appropriate switch to support the network. Take care to evaluate your needs for the present and near future. If you choose an inadequate switch to run in the core of the network, you face potential bottleneck issues in the core, slowing down all communications on the network.

The availability of the core layer is also critical, so you should build in as much redundancy as you can. Layer 3 redundancy typically has faster convergence than Layer 2 redundancy in the event of hardware failure. Convergence in this context refers to the time it takes for the network to adapt to a change, not to be confused with a converged network that supports data, audio, and video communications. With that in mind, you want to ensure that your core layer switches support Layer 3 functions. A complete discussion on the implications of Layer 3 redundancy is beyond the scope of this book. It remains an open question about the need for Layer 2 redundancy in this context. Layer 2 redundancy is examined in Chapter 5 when we discuss the spanning-tree protocol. Also, look for core layer switches that support additional hardware redundancy features, such as redundant power supplies that can be swapped while the switch continues to operate. Because of the high workload carried by core layer switches, they tend to operate hotter than access or distribution layer switches, so they should have more sophisticated cooling options. Many true core-layer-capable switches have the capability to swap cooling fans without having to turn the switch off.

For example, it would be disruptive to shut down a core layer switch to change a power supply or a fan in the middle of the day when the network usage is at its highest. To perform a hardware replacement, you could expect to have at least a 5-minute network outage, and that is if you are very fast at performing the maintenance. In a more realistic situation, the switch could be down for 30 minutes or more, which most likely is not acceptable. With hot-swappable hardware, there is no downtime during switch maintenance.

The core layer also needs to support link aggregation to ensure adequate bandwidth coming into the core from the distribution layer switches. Core layer switches should have support for aggregated 10 Gigabit Ethernet connections, which is currently the fastest available Ethernet connectivity option. This allows corresponding distribution layer switches to deliver traffic as efficiently as possible to the core.

QoS is an important part of the services provided by core layer switches. For example, service providers (who provide IP, data storage, e-mail, and other services) and enterprise wide-area networks (WANs) are adding more voice and video traffic to an already growing amount of data traffic. At the core and network edge, mission-critical and time-sensitive traffic such as voice should receive higher QoS guarantees than less time-sensitive traffic such as file transfers or e-mail. Because high-speed WAN access is often prohibitively expensive, adding bandwidth at the core layer is not an option. Because QoS provides a

software-based solution to prioritize traffic, core layer switches can provide a cost-effective way of supporting optimal and differentiated use of existing bandwidth.

Switches for Small and Medium Sized Business (SMB)

Now that you know which switch features are used at which layer in a hierarchical network, you will learn about the Cisco switches that are applicable for each layer in the hierarchical network model. Today, you cannot simply select a Cisco switch by considering the size of a business. A small business with 12 employees might be integrated into the network of a large multinational enterprise and require all the advanced LAN services available at the corporate head office. The following classification of Cisco switches within the hierarchical network model represents a starting point for your deliberations on which switch is best for a given application. The classification presented reflects how you might see the range of Cisco switches if you were a multinational enterprise. For example, the port densities of the Cisco 6500 switch make sense as an access layer switch only where there are many hundreds of users in one area, such as the floor of a stock exchange. If you think of the needs of a medium-sized business, a switch that is typically known as an access layer switch, such as the Cisco 3560 switch, could be used as a distribution layer switch if it met the criteria determined by the network designer for that application.

Cisco currently has seven switch product lines. Each product line offers different characteristics and features, allowing you to find the right switch to meet the functional requirements of your network. The Cisco switch product lines are as follows:

- Catalyst Express 500
- Catalyst 2960
- Catalyst 3560
- Catalyst 3750
- Catalyst 4500
- Catalyst 4900
- Catalyst 6500

Catalyst Express 500

The Catalyst Express 500, shown in Figure 1-28, is the Cisco entry-layer switch.

The Catalyst Express 500 offers the following:

- Forwarding rates from 8.8 Gbps to 24 Gbps
- Layer 2 port security
- Web-based management
- Converged data/IP communications support

Figure 1-28 Catalyst Express 500

This switch series is appropriate for access layer implementations where high port density is not required. The Cisco Catalyst Express 500 series switches are scaled for small business environments ranging from 20 to 250 employees. The Catalyst Express 500 series switches are available in different fixed configurations:

- Fast Ethernet and Gigabit Ethernet connectivity
- Up to 24 10/100 ports with optional PoE or 12 10/100/1000 ports

Catalyst Express 500 series switches do not allow management through the Cisco IOS CLI. They are managed using a built-in web management interface, the Cisco Network Assistant or the new Cisco Configuration Manager developed specifically for the Catalyst Express 500 series switches. The Catalyst Express does not support console access.

To learn more about the Cisco Express 500 series of switches, go to www.cisco.com/en/US/products/ps6545/index.html.

Catalyst 2960

The Catalyst 2960 series switches enable entry-layer enterprise, medium-sized, and branch office networks to provide enhanced LAN services. The Catalyst 2960 series switches, shown in Figure 1-29, are appropriate for access layer implementations where access to power and space is limited. The CCNA Exploration 3 LAN Switching and Wireless labs are based on the features of the Cisco 2960 switch.

Figure 1-29 Catalyst 2960

The Catalyst 2960 series switches offer the following:

- Forwarding rates from 16 Gbps to 32 Gbps
- Multilayered switching
- QoS features to support IP communications
- Access control lists
- Fast Ethernet and Gigabit Ethernet connectivity
- Up to 48 10/100 ports or 10/100/1000 ports with additional dual purpose gigabit uplinks

The Catalyst 2960 series of switches does not support PoE.

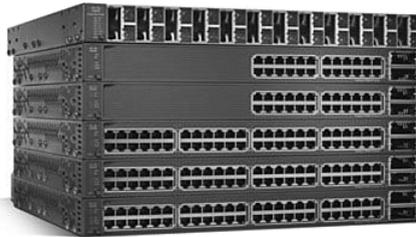
The Catalyst 2960 series supports the Cisco IOS CLI, integrated web management interface, and Cisco Network Assistant. This switch series supports console and auxiliary access to the switch.

To learn more about the Catalyst 2960 series of switches, visit www.cisco.com/en/US/products/ps6406/index.html.

Catalyst 3560

The Cisco Catalyst 3560 series is a line of enterprise-class switches that include support for PoE, QoS, and advanced security features such as ACLs. These switches, shown in Figure 1-30, are ideal access layer switches for small enterprise LAN access or branch-office converged network environments.

Figure 1-30 Catalyst 3560



The Cisco Catalyst 3560 series supports forwarding rates of 32 Gbps to 128 Gbps (Catalyst 3560-E switch series).

The Catalyst 3560 series switches are available in different fixed configurations:

- Fast Ethernet and Gigabit Ethernet connectivity
- Up to 48 10/100/1000 ports, plus four small form-factor pluggable ports

- Optional 10 Gigabit Ethernet connectivity in the Catalyst 3560-E models
- Optional integrated PoE (Cisco prestandard and IEEE 802.3af); up to 24 ports with 15.4 watts or 48 ports with 7.3 watts

To learn more about the Catalyst 3560 series of switches, visit www.cisco.com/en/US/products/hw/switches/ps5528/index.html.

Catalyst 3750

The Cisco Catalyst 3750 series of switches, shown in Figure 1-31, is ideal for access layer switches in midsize organizations and enterprise branch offices. This series offers forwarding rates from 32 Gbps to 128 Gbps (Catalyst 3750-E switch series). The Catalyst 3750 series supports Cisco StackWise technology. StackWise technology allows you to interconnect up to nine physical Catalyst 3750 switches into one logical switch using a high-performance (32 Gbps), redundant, backplane connection.

Figure 1-31 Catalyst 3750



The Catalyst 3750 series switches are available in different stackable fixed configurations:

- Fast Ethernet and Gigabit Ethernet connectivity
- Up to 48 10/100/1000 ports, plus four SFP ports
- Optional 10 Gigabit Ethernet connectivity in the Catalyst 3750-E models
- Optional integrated PoE (Cisco prestandard and IEEE 802.3af); up to 24 ports with 15.4 watts or 48 ports with 7.3 watts

To learn more about the Catalyst 3750 series of switches, visit www.cisco.com/en/US/products/hw/switches/ps5023/index.html.

Catalyst 4500

The Catalyst 4500, shown in Figure 1-32, is the first midrange modular switching platform offering multilayer switching for enterprises, small- to medium-sized businesses, and service providers.

Figure 1-32 Catalyst 4500

With forwarding rates up to 136 Gbps, the Catalyst 4500 series is capable of managing traffic at the distribution layer. The modular capability of the Catalyst 4500 series allows for very high port densities through the addition of switch port line cards to its modular chassis. The Catalyst 4500 series offers multilayer QoS and sophisticated routing functions.

The Catalyst 4500 series switches are available in different modular configurations:

- Modular 3, 6, 7, and 10 slot chassis offering different layers of scalability
- High port density: up to 384 Fast Ethernet or Gigabit Ethernet ports available in copper or fiber with 10 Gigabit uplinks
- PoE (Cisco prestandard and IEEE 802.3af)
- Dual, hot-swappable internal AC or DC power supplies
- Advanced hardware-assisted IP routing capabilities

To learn more about the Catalyst 4500 series of switches, visit www.cisco.com/en/US/products/hw/switches/ps4324/index.html.

Catalyst 4900

The Catalyst 4900 series switches, shown in Figure 1-33, are designed and optimized for server switching by allowing very high forwarding rates. The Cisco Catalyst 4900 is not a typical access layer switch. It is a specialty access layer switch designed for data center deployments where many servers may exist in close proximity. This switch series supports dual, redundant power supplies and fans that can be swapped out while the switch is still running. This allows the switches to achieve higher availability, which is critical in data center deployments.

Figure 1-33 Catalyst 4900

The Catalyst 4900 series switches support advanced QoS features, making them ideal candidates for the back-end IP telephony hardware. Catalyst 4900 series switches do not support the StackWise feature of the Catalyst 3750 series, nor do they support PoE.

The Catalyst 4900 series switches are available in different fixed configurations:

- Up to 48 10/100/1000 ports with four SFP ports or 48 10/100/1000 ports with two 10 Gigabit Ethernet ports
- Dual, hot-swappable internal AC or DC power supplies
- Hot-swappable fan trays

To learn more about the Catalyst 4900 series of switches, visit www.cisco.com/en/US/products/ps6021/index.html.

Catalyst 6500

The Catalyst 6500 series modular switch, shown in Figure 1-34, is optimized for secure, converged voice, video, and data networks. The Catalyst 6500 is capable of managing traffic at the distribution and core layers. The Catalyst 6500 series is the highest-performing Cisco switch, supporting forwarding rates up to 720 Gbps. The Catalyst 6500 is ideal for very large network environments found in enterprises, medium-sized businesses, and service providers.

Figure 1-34 Catalyst 6500



The Catalyst 6500 series switches are available in different modular configurations:

- Modular 3, 4, 6, 9, and 13 slot chassis
- LAN/WAN service modules
- PoE up to 420 IEEE 802.3af Class 3 (15.4W) PoE devices
- Up to 1152 10/100 ports, 577 10/100/1000 ports, 410 SFP Gigabit Ethernet ports, or 64 10 Gigabit Ethernet ports
- Dual, hot-swappable internal AC or DC power supplies
- Advanced hardware-assisted IP routing capabilities

To learn more about the Catalyst 6500 series of switches, visit www.cisco.com/en/US/products/hw/switches/ps708/index.html.

Comparing Switches

The following tool can help identify the correct switch for an implementation:

www.cisco.com/en/US/products/hw/switches/products_promotion0900aecd8050364f.html.

Last, the following guide provides a detailed comparison of current switch offerings from Cisco:

www.cisco.com/application/pdf/en/us/guest/products/ps708/c2072/cdccont_0900aecd805f0955.pdf.

Packet Tracer
□ Activity

Build a Hierarchical Topology (1.2.4)

Use the Packet Tracer Activity to build a topology representative of the switched LANs discussed in the book. You will add all the necessary devices and connect them with the correct cabling. Use file e3-1243.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Summary

In this chapter, we discussed the hierarchical design model. Implementing this model improves the performance, scalability, availability, manageability, and maintainability of the network. Hierarchical network topologies facilitate network convergence by enhancing the performance necessary for voice and video data to be combined onto the existing data network.

The traffic flow, user community, data store and data server locations, and topology diagram analysis are used to help identify network bottlenecks. The bottlenecks can then be addressed to improve the performance of the network and accurately determine appropriate hardware requirements to satisfy the desired performance of the network.

We surveyed the different switch features, such as form factor, performance, PoE, and Layer 3 support, and how they relate to the different layers of the hierarchical network design. An array of Cisco Catalyst switch product lines are available to support any application or business size.

Labs

The labs available in the companion *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-202-8) provide hands-on practice with the following topics introduced in this chapter:



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

In this lab, you will design and configure a small routed network and verify connectivity across multiple network devices. This requires creating and assigning two subnetwork blocks, connecting hosts and network devices, and configuring host computers and one Cisco router for basic network connectivity. You will use common commands to test and document the network.



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

In this lab, you will repeat the procedures in Lab 1.3.1 without the guidance provided therein. You are given only the set of objectives to complete.



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

In this lab, you are given a completed configuration for a small routed network. The configuration contains design and configuration errors that conflict with stated requirements and prevent end-to-end communication. You examine the given design and identify and correct any design errors. You then cable the network, configure the hosts, and load configurations

onto the router. Finally, you will troubleshoot the connectivity problems to determine where the errors are occurring and correct them using the appropriate commands. When all errors have been corrected, each host should be able to communicate with all other configured network elements and with the other host.



Many of the hands-on labs include Packet Tracer Companion Activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *LAN Switching and Wireless*, *CCNA Exploration Labs and Study Guide* (ISBN 1-58713-202-8) for hands-on labs that have a Packet Tracer Companion.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in the appendix, “Check Your Understanding and Challenge Questions Answer Key.”

1. Which three options correctly associate a layer of the hierarchical design model with its function? (Choose three.)
 - A. Core—interface for end devices
 - B. Distribution—traffic control and security policies
 - C. Access—interface for end devices
 - D. Distribution—high-speed backbone
 - E. Core—high-speed backbone
 - F. Access—implementation of security policies
2. With respect to network design, what is convergence?
 - A. Implementation of standard equipment sets for LAN design
 - B. Implementation of a core-distribution-access design model for all sites in an enterprise
 - C. A point in the network where all traffic “converges” before transmission to the destination, normally the core switch
 - D. Combining conventional data with voice and video on a common network

3. Which three options are potential benefits of a converged network? (Choose three.)
 - A. Simplified data network configuration
 - B. Combines voice and data network staffs
 - C. Combines voice, video, and applications in one computer
 - D. Simpler maintenance than hierarchical networks
 - E. Simplified network changes
 - F. Lower quality of service configuration requirements

4. Which four options describe data store and data server analysis actions? (Choose four.)
 - A. Workstation ports required for a department
 - B. Amount of server-to-server traffic
 - C. Intensity of use of a department application server
 - D. Amount of traffic for a SAN
 - E. Anticipated department port growth
 - F. Data backed up to tape
 - G. Network attached storage

5. What factor may complicate user community analysis?
 - A. Application changes may radically affect predicted data growth.
 - B. Server-to-server traffic may skew user port usage data.
 - C. Application usage is not always bound by department or physical location.
 - D. Different organization applications may share data stores.

6. Which two of the following pairings are accurate? (Choose two.)
 - A. Port density—capability to use multiple switch ports concurrently for higher throughput data communication
 - B. Forwarding rates—processing capabilities of a switch by quantifying performance of the switch by how much data it can process per second
 - C. Link aggregation—number of ports available on a single switch
 - D. Wire speed—data rate that each port on the switch is capable of attaining

7. What would be the port capacity of a single port on a 48-port Gigabit Ethernet switch?
 - A. 48 Gbps
 - B. 10 Mbps
 - C. 1000 Mbps
 - D. 100 Mbps

8. A switch that uses MAC addresses to forward frames operates at which layer of the OSI model?
- A. Layer 1
 - B. Layer 2
 - C. Layer 3
 - D. Layer 4
9. What is a feature offered by all stackable switches?
- A. Predetermined number of ports
 - B. Fully redundant backplane
 - C. Support for Gigabit connectivity
 - D. Low bandwidth for interswitch communications
 - E. PoE capability
10. What function is performed by a Cisco Catalyst access layer switch?
- A. Inter-VLAN support
 - B. Routing
 - C. Providing PoE
 - D. Link aggregation
11. Which three features are associated with the core layer of the hierarchical design model? (Choose three.)
- A. Port security
 - B. Layer 3 support
 - C. Redundant components
 - D. VLANs
 - E. 10 Gigabit Ethernet
 - F. PoE
12. Which two characteristics describe the core layer of the hierarchical network model? (Choose two.)
- A. Redundant paths
 - B. High-level policy enforcement
 - C. PoE
 - D. Controls access of end devices to network
 - E. Rapid forwarding of traffic

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in the appendix, “Check Your Understanding and Challenge Questions Answer Key.”

1. List and describe the three layers of the hierarchical network model.
2. Match the terms with the correct descriptions.

__Fixed Configuration Switch

__Forwarding Rate

__Quality of Service

__Power over Ethernet

__Modular Switch

__Link Aggregation

__Port Density

__Stackable Switch

__Redundancy

- A. Ratio of number of ports to number of switches.
- B. Ratio of quantity of data to time.
- C. Capable of interconnection via a special backplane cable.
- D. Ports cannot be added to the device.
- E. Binding together of distinct links for enhanced throughput.
- F. Allows for the installation of line cards or modules.
- G. Capability of a device to power another device using Ethernet.
- H. Capability to recover connectivity after a network failure.
- I. Prioritization of network traffic.



Look for this icon in *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-202-8) for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

Numbers

2.4 GHz channels, 392

3DES (Triple DES) algorithm, 94

802.1Q support website, 151

A

AAA (Authentication, Authorization, and Accounting) server, 76, 407

access

console, 85-86

distribution path failures, 232

ports

configuring with PortFast, 271-272

VTP, configuration, 211

privileged EXEC, 88-89

spoofing attacks, 100-101

virtual terminal, 87-88

WLANs, 410

access points, configuring, 410-417

protocols, 409

access layer (hierarchical network design model), 2, 28-29

access mode (VLAN trunks), 150

access points. See APs

ad hoc topologies, 394

addresses

dynamic, 77

IP, 362-365

MAC

address tables, 77-78, 236

determining root bridges, 260

Ethernet, 49

flooding, 96-99

port security, 105-106, 109

sticky secure MAC addresses, 106

switch configuration, 77-78

switch tables, 51-52

static, 77, 105

advertisements (VTP), 185, 190-192

802.1Q frame encapsulation, 191

configuration revision numbers, 192-193

frame structure, 191

header/message fields, 190

types, 193-196

AES (Advanced Encryption Standard), 408

AID (association identifier), 398

algorithms

3DES (Triple DES), 94

STA, 244

best paths, 249-252

port types, 247-248

root bridges, 248

allowed VLANs list issues, 169-171

alternate ports (RSTP), 300

APs (access points), 382

configuring, 410-412

basic wireless settings, 413-415

security, 415-417

placement, 431-433

radio/firmware, troubleshooting, 426

rogue, 402-403

wireless, 388-389

WLANs, 382

assigning port roles, 264

association, 396-398

association identifier (AID), 398

asymmetric switching, 60

attacks (security), 96

CDP, 101

MAC address flooding, 96-99

spoofing, 100-101

Telnet, 102-103

attenuation, 389

authentication, 396

AAA, 76

TACAS, 76

WLANs, 397

open, 406

protocols, 407-408

troubleshooting, 434

WEP, 406

Authentication, Authorization, and Accounting (AAA)

server, 76, 407

auto-MDIX feature, 51

B

BackboneFast STP extensions website, 287

backing up configuration files, 81

backup ports (RSTP), 301

bandwidth

- aggregation, 8
- Ethernet 802.3 networks, 52

banner login command, 92

banner motd command, 92

basic service area (BSA), 394

basic service set (BSS), 393-394

basic wireless settings (WLANs), configuring, 413-415

- network mode, 413
- network names, 413
- radio bands, 414
- SSID broadcasts, 414
- standard channels, 415
- wide channels, 414

beacons, 396

benefits

- converged networks, 12
- hierarchical network designs, 4
 - maintainability, 6*
 - manageability, 6*
 - performance, 5*
 - redundancy, 5*
 - scalability, 5*
 - security, 5*
- one-router-interface-per-VLAN, 345-346
- router-on-a-stick, 345-346
- VLANs, 124-125
- VTP, 184
- WLANs, 379-380

BIDs (bridge IDs), 247, 258, 261

- bridge priorities, 259
- configuring, 261-263
- extended system IDs, 259
- fields, 258
- lowest bridge priority, 260
- MAC addresses determining root, 260
- PVST+, 290
- verifying, 262

black hole VLANs, 128

blocking STP port state, 268-269

boot sequences, 71-72

bottlenecks (LAN designs), 57

BPDU (bridge protocol data units), 247, 252

- fields, 252
- guards, 271, 287, 318

process, 253-258

RSTP, 295-296

TC bit sets, 285

TCA bit sets, 285

timers, 269-270

topology change notification (TCN), 285

Wireshark capture, 253

bridge IDs. See BIDs

bridges

designated, 263

priorities, 259, 293

root

election, 273-276

primary/secondary, 292-293

root. *See* root bridges

broadcast communications, 47

broadcast domains

controlling with VLANs, 138-143

inter-VLAN communication with SVIs, 142

intra-VLAN communication, 140-141

Layer 3 switching, 141

single VLANs, 138

two VLANs, 139

Ethernet 802.3 networks, 54

broadcast frames

egress, 234

forwarding, 236

broadcast loops, 234

broadcast storms, 125, 238-240

brute-force password attacks, 102

BSA (basic service area), 394

BSS (basic service set), 393-394

BSSID (BSS identifier), 394

C

CAM tables. See MAC addresses, tables

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), 388

carrier sense multiple access/collision detection (CSMA/CD), 46-47

Catalyst 2960 switches, 34-35

Catalyst 3560 switches, 35-36

Catalyst 3750 switches, 36

Catalyst 4500 switches, 36-37

Catalyst 4900 switches, 37-38

Catalyst 6500 switches, 38

Catalyst Express 500, 33-34

CCNA Exploration: Routing Protocols and Concepts website, 349

CDP (Cisco Discovery Protocol), 101, 131

certification (WLANs), 386-387

channel settings (WLANs), 426-429

channels, 389

choosing

- hierarchical network switches, 15
 - data server analysis, 19-20*
 - data store analysis, 19-20*
 - topology diagrams, 20-21*
 - traffic flow analysis, 15-17*
 - user community analysis, 17-18*
- WLAN standards, 384

Cisco

- Device Manager, 66
- Discovery Protocol (CDP), 101, 131
- EtherChannels, 8, 242, 358
- IP phones, 132
- Network Assistant, 65

CiscoView, 65

clear spanning-tree detected-protocols command, 310

clear-to-send (CTS) messages, 404

CLI (command-line interface), 63

- command history, 70-71
- GUI alternatives, 65
- help, 68-70
 - console error messages, 69*
 - context-sensitive, 68*
- navigating, 63-65

clients

- server traffic, 19
- VTP, 185, 197, 206, 209

collision domains (Ethernet 802.3 networks), 53-54

command-line interface. See CLI

commands

- adding VLANs, 152
- banner login, 92
- banner motd, 92
- clear spanning-tree detected protocols, 310
- configure terminal, 64
 - console access, 86*
 - port security, 108*
 - privileged EXEC access, 89*
 - virtual terminal access, 87*
- copy running-config startup-config, 75
- crypto key generate rsa, 94
- delete flash:filename, 84
- dir flash:, 91
- disable, 64

- enable, 64
- enable password, 88
- enable secret, 88-89
- encapsulation dot1q vlan-id, 344
- end
 - console access, 86*
 - port security, 108*
 - privileged EXEC access, 89*
 - virtual terminal access, 87*
- erase nvram:, 84
- erase startup-config, 84
- exit, 65
- flash_init, 91
- history
 - CLI, 70-71*
 - viewing, 78*
- inter-VLAN routing troubleshooting, 359-360
- interface f0/0.10, 344
- interface fastEthernet 0/18, 108
- interface interface-name command, 65
- interface range, 110
- interface vlan 99, 73
- ip address 172.17.10.1 255.255.255.0, 344
- ip default-gateway, 75
- ip dhcp snooping, 101
- ip dhcp snooping trust command, 101
- ip dhcp snooping vlan number, 101
- ip http authentication enable, 77
- line console 0, 85-86
- line vty 0 4, 87
- line vty 0 15, 87
- load_helper, 91
- login
 - console access, 86*
 - virtual terminal access, 87*
- mac-address-table static mac-addr vlan vlan-id interface interface-id, 77
- no banner login, 92
- no enable password, 89
- no enable secret, 89
- no mac-address-table static mac-addr vlan vlan-id interface interface-id, 77
- no service password-encryption, 90
- no shutdown, 73, 110
- no spanning-tree, 250
- no spanning-tree portfast, 272
- no switchport access vlan, 158
- no switchport port-security mac-address sticky, 106
- no vlan vlan-id, 160
- password cisco
 - console access, 86*
 - virtual terminal access, 87*
- password password, 85
- port security, 107

Rapid PVST+, 310
 reload, 82
 rename flash:config.text flash:config.text.old, 91
 service password-encryption, 89
 show, 78
 show dtp interface, 151
 show flash, 78
 show history, 70, 78
 show interface, 78
 show interface interface-id switchport command, 359
 show interfaces, 79, 158
 show interfaces f0/18 switchport, 158
 show interfaces FastEthernet 0/1, 79
 show interfaces interface-id switchport, 147
 show interfaces switchport, 155-158
 show interfaces trunk, 203
 show interfaces vlan 20, 156
 show ip, 78
 show ip interface brief, 75
 show ip route, 344
 show ip ssh, 95
 show mac-address-table, 77-78
 show port-security [interface interface-id], 109
 show port-security [interface interface-id] address, 109
 show run, 294
 show running-config, 78-79
 Portfast verification, 272
 Rapid PVST+ verification, 311
 show spanning-tree, 251, 262
 designated/non-designated port election, 283
 parameters, 294
 root bridge election verification, 274
 root port election, 278
 show spanning-tree active, 293
 show spanning-tree detail, 252
 show ssh, 95
 show startup-config, 78
 show version, 78
 show vlan, 155, 158
 show vlan brief, 153-154
 show vlan name student, 155
 show vlan summary, 156
 show vtp status, 187, 207
 shutdown, 110
 spanning-tree cost, 250
 spanning-tree link-type point-to-point, 310
 spanning-tree port-priority, 265
 spanning-tree portfast, 271, 297
 spanning-tree vlan 1 priority 24576, 262
 spanning-tree vlan 1 root primary, 262
 spanning-tree vlan 1 root secondary, 262
 spanning-tree vlan vlan-id priority value, 262
 spanning-tree vlan vlan-id root primary, 261
 spanning-tree vlan vlan-id root primary diameter
 value, 270

spanning-tree vlan vlan-id root secondary, 261
 sticky address port security, 108
 subinterface routing, 361-362
 switchport access vlan, 348
 switchport access vlan 10, 357
 switchport mode, 162
 switchport mode access, 108, m348
 switchport mode dynamic auto, 149, 351
 switchport mode dynamic desirable, 150-151, 351
 switchport mode trunk, 149, 160, 357
 switchport nonegotiate, 150
 switchport port-security, 108
 switchport port-security mac-address sticky, 106-108
 switchport port-security maximum 50, 108
 terminal no history, 71
 terminal no history size command, 71
 traceroute, 354
 transport input all, 94
 transport input telnet, 94
 vlan vlan-id, 154
 vtp domain, 214
 vtp mode, 214
 vtp mode client, 209
 vtp mode server, 207
 vtp password, 208, 212
 vtp pruning, 201
 vtp version, 208, 212

common distribution system, 394

communication

Ethernet, 47-49
 broadcast, 47
 duplex settings, 49
 frame, 48
 MAC addresses, 49
 multicast, 48
 unicast, 47
 inter-VLAN communication with SVIs, 142
 intra-VLAN communication, 140-141

components

VTP, 184-186
 WLANs, 383
 access points, 388-389
 routers, 390
 wireless NICs, 387

configuration files

backing up, 81
 erasing, 84-85
 renaming, 91
 restoring, 81-82
 storing on TFTP servers, 82-84

configure terminal command, 64

console access, 86
 port security, 108

privileged EXEC access, 89
virtual terminal access, 87

configuring

access ports, 271-272
BIDs, 261-263
dynamic VLANs, 137
inter-VLAN routing, 347-350, 360-362
Linksys, 411
native VLAN trunks, 147-148
path costs, 250
port costs, 250
port priorities, 265-266
port security, 105-109
 commands, 107
 default settings, 107
 MAC addresses, 105, 109
 security violations, 106-107
 sticky address commands, 108
 sticky secure MAC addresses, 106
 unused ports, 110
 verifying, 109
 websites, 108
PortFast, 271, 317-318
PVST+, 291-293
Rapid PVST+, 309-311
router-on-a-stick routing method, 351-355
SSH, 94-96
static VLANs, 137
STP switch diameters, 270-271
subinterfaces, 341-345
switches
 backing up, 81
 boot sequences, 71-72
 default gateways, 74-75
 duplex mode, 75-76
 erasing configuration files, 84-85
 HTTP access, 76-77
 MAC address tables, 77-78
 management interface, 73-74
 preparations, 72
 restoring, 81-82
 speed, 75-76
 storing on TFTP servers, 82-84
 verifying, 78-80
Telnet, 93
VLANs, 152-154
 adding VLANs, 152-153
 static interfaces, 154
 SVIs, 142
 switch topology, 152
 trunks, 160-163
 vlan.dat file, 153
 voice, 137

VTP, 186-188, 204-206

access ports, 211
 clients, 206, 209
 confirming, 210-211
 connections, 210
 passwords, 208
 reference topology, 204
 revision numbers, 192-193
 servers, 204-208

wireless access points, 410-412
 basic wireless settings, 413-415
 security, 415-417
wireless NICs, 418
 connectivity, verifying, 423
 security protocols, 420-422
 SSIDs, scanning, 418-419
wireless parameters, 391-393
WLAN security, 415-417, 420-422

confirming VTP configuration, 210-211

connections

WLANs, 396-398
 association, 398
 authentication, 397
 beacons, 396
 probes, 397
 troubleshooting, 424-426
 verifying, 423
VTP, 210

console

access, 85-86
error messages (CLI), 69

context-sensitive help (CLI), 68

converged networks, 10-11

benefits, 12
data networks, 14
legacy equipment, 10
QoS, 10
software options, 12-13
STP, 273
 designated/non-designated port election, 279-284
 root bridge election, 273-276
 root port election, 276-279
 topology changes, 285-286
technology advancements, 11-12
video networks, 14
voice networks, 13

copy running-config startup-config command, 75

core layer (hierarchical network design model), 3, 31-33

core switch failures, 232

coverage areas (WLANs), 400-401

crackers, 402

crypto key generate rsa command, 94

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 388

CSMA/CD (carrier sense multiple access/collision detection), 46-47

CTS (clear-to-send) messages, 404

cubicle loops, 243-244

cut-through switching, 59-60

D

Data Encryption Standard (DES), 94

data

- networks, 14
- servers, 19-20
- stores, 19-20
- VLANs, 127

DCF (distributed coordination function), 388

default gateways, 74-75

default VLANs, 128

delete flash:filename command, 84

deleting

- configuration files, 84-85
- login banners, 92
- RSA keys, 95
- VLAN trunks, 164
- vlan.dat file, 160
- VLANs, 160

denial of service attacks (WLANs), 404

DES (Data Encryption Standard) algorithm, 94

design

- Ethernet/802.3 networks
 - bandwidth/throughput, 52*
 - broadcast domains, 54*
 - collision domains, 53-54*
 - LAN segmentation, 55-56*
 - latency, 54-55*
 - network congestion, 55*
- hierarchical network design, 2
 - access layer, 2, 28-29*
 - bandwidth aggregation, 8*
 - benefits, 4-6*
 - business application, 4*
 - comparing switches, 39*
 - convergence, 10-14*
 - core layer, 3, 31-33*
 - distribution layer, 3, 30-31*
 - Layer 3 functionality, 27*

network diameters, 7

performance, 24-26

Power over Ethernet (PoE), 26

redundancy, 9-10

small and medium sized business switches, 33-38

switch features, 22-23

switches, choosing, 15-21

three-layer model, 2

LANs, 56-58

Layer 2 redundancy, 231

STP, 312-313

blocked ports, minimizing, 313-314

Layer 3 switching, 314-316

management VLAN traffic, 316

not disabling STP, 316

designated bridges, 263

designated ports

definition, 248

election, 279-284

root bridges, 263

RSTP, 300

DHCP, 100-101

dialog boxes

Wireless Network Connection Status, 420

Wireless Network Properties, 420-421

dir flash: command, 91

direct-sequence spread spectrum (DSSS), 384

disable command, 64

disabled STP port state, 269

disabling

PortFast, 272

ports, 264

disadvantages

one-router-interface-per-VLAN routing method,
341, 345-346

router-on-a-stick routing method, 345-346

disaster recovery website, 10

discarding RSTP port state, 299

discovery (WLANs), 396-398

association, 398

authentication, 397

beacons, 396

probes, 397

distributed coordination function (DCF), 388

distribution-core path failures, 232

**distribution layer (hierarchical network design model),
3, 30-31**

distribution switch failures, 232

domains

broadcast

*controlling with VLANs, 138-143**Ethernet 802.3 networks, 54*

collision, 53-54

VTP, 184, 188-190

*default VTP configuration, 189**names, 189, 213-214**two domain example, 188**updates, 190***DoS (denial of service) attacks, 102, 404****draft 802.11n, 384-385****DSSS (direct-sequence spread spectrum), 384****DTP (Dynamic Trunking Protocol), 149-151****duplex settings**

Ethernet networks, 49

switch ports, 75-76

duplicate unicast frames, 240-241**dynamic addresses, 77****dynamic auto mode (VLAN trunks), 149****dynamic desirable mode (VLAN trunks), 150****dynamic secure MAC addresses, 105****Dynamic Trunking Protocol (DTP), 149****dynamic VLANs, 137****E****EAP (Extensible Authentication Protocol), 407****edge ports (RSTP), 296-297****electing**

designated/non-designated ports, 279-284

root bridges, 273-276

root ports, 276-279

enable command, 64**enable password command, 88****enable secret command, 88-89****encapsulation dot1q vlan-id command, 344****encryption**

3DES, 94

DES, 94

passwords, 89-90

standards, 90

WLANs

*protocols, 408-409**troubleshooting, 434***end command**

console access, 86

port security, 108

privileged EXEC access, 89

virtual terminal access, 87

enterprise networks, 24**erase nvram: command, 84****erase startup-config command, 84****ESA (extended service area), 394****ESS (extended service set), 394****EtherChannels, 8, 242, 358****Ethernet 802.3 networks, 46**

communications, 47-49

*broadcast, 47**duplex settings, 49**frame, 48**MAC addresses, 49**multicast, 48**unicast, 47*

CSMA/CD, 46-47

designing

*bandwidth/throughput, 52**broadcast domains, 54**collision domains, 53-54**LAN segmentation, 55-56**latency, 54-55**network congestion, 55*

switches

*MAC address tables, 51-52**port settings, 50-51***ethical hackers, 402****exit command, 65****extended range VLANs, 126****extended service area (ESA), 394****extended service set (ESS), 394****extended system IDs, 259****Extensible Authentication Protocol (EAP), 407****F****fast-forward switching, 59****files**

configuration

*backing up, 81**erasing, 84-85**renaming, 91**restoring, 81-82**storing on TFTP servers, 82-84*

helper, 91

vlan.dat, 160

fixed configuration switches, 22

Flash file systems

- files, deleting, 84
- initializing, 91
- viewing, 78

flash_init command, 91**flash memory, 91****forward delay BPDU timer, 269****forwarding**

- frames
 - asymmetric switching, 60*
 - forwarding methods, 59-60*
 - Layer 2/Layer 3 switches, 62*
 - memory buffering, 60-62*
 - symmetric switching, 60*
- rates, 25

forwarding RSTP port state, 299**forwarding STP port state, 269****fragment-free switching, 59****frames, forwarding**

- asymmetric switching, 60*
- forwarding methods, 59-60*
- Layer 2/Layer 3 switches, 62*
- memory buffering, 60-62*
- symmetric switching, 60*

full-duplex communication, 50

G

gateways (default), 74-75**global configuration mode (CLI), 64****GPS (global positioning systems), 380****guards (BPDU), 271, 287, 318****GUI alternatives to CLI, 65**

H

hackers, 402**half-duplex communication, 49****hardware**

- status, viewing, 78
- WLANs
 - access points, 388-389*
 - routers, 390*
 - wireless NICs, 387*

hello time BPDU timer, 269**help (CLI), 68-70**

- console error messages, 69
- context-sensitive, 68

helper files, loading, 91**hidden node problems, 389****hierarchical network design, 2**

- bandwidth aggregation, 8
- benefits, 4
 - maintainability, 6*
 - manageability, 6*
 - performance, 5*
 - redundancy, 5*
 - scalability, 5*
 - security, 5*
- business application, 4
- convergence, 10-11
 - benefits, 12*
 - data networks, 14*
 - legacy equipment, 10*
 - QoS, 10*
 - software options, 12-13*
 - technology advancements, 11-12*
 - video networks, 14*
 - voice networks, 13*

layers

- access, 2*
- core, 3*
- distribution, 3*
- network diameters, 7
- redundancy, 9-10
- switches, 22
 - access layer features, 28-29*
 - comparing, 39*
 - core layer features, 31-33*
 - distribution layer features, 30-31*
 - form factors, 22-23*
 - layer 3 functionality, 27*
 - performance, 24-26*
 - Power over Ethernet (PoE), 26*
 - small and medium sized businesses, 33-38*

switches, choosing, 15

- data server analysis, 19-20*
- data store analysis, 19-20*
- topology diagrams, 20-21*
- traffic flow analysis, 15-17*
- user community analysis, 17-18*

three-layer model, 2**high availability website discussion, 9****HP OpenView, 68****HTTP access, 76-77**

I–J

- IBSS (independent BSS), 394**
 - ICMP (Internet Control Message Protocol), 354**
 - ID ranges (VLANs), 126**
 - IEEE 802 LAN/MAN Standards Committee (LMSC), 386**
 - IEEE 802.11, 383, 395**
 - IEEE 802.11a, 384**
 - IEEE 802.11b, 384-385**
 - IEEE 802.11g, 384-385**
 - IEEE 802.11i, 387**
 - IEEE 802.11n draft, 384-385**
 - IEEE 802.1Q**
 - frame tagging, 145-146
 - trunk ports, 129
 - implementing redundant links, 9**
 - independent BSS (IBSS), 394**
 - industrial, scientific, and medical (ISM) frequency bands, 383**
 - initializing Flash file systems, 91**
 - interface configuration mode (CLI), 64**
 - interface f0/0.10 command, 344**
 - interface fastEthernet 0/18 command, 108**
 - interface interface-name command, 65**
 - interface range command, 110**
 - interface vlan 99 command, 73**
 - interfaces**
 - static VLAN, 154
 - status, viewing, 78
 - switch management, 73-74
 - interference (WLANS), 384**
 - International Telecommunications Union-Radio communication sector (ITU-R), 386**
 - Internet Control Message Protocol (ICMP), 354**
 - inter-switch link (ISL), 149-151**
 - inter-VLAN routing**
 - communication with SVIs, 142
 - configuring, 347-350
 - Layer 3 switches, 336-337
 - one-router-interface-per-VLAN, 332-334
 - advantages/disadvantages, 345-346*
 - disadvantages, 341*
 - physical interfaces, configuring, 338-341*
 - routing table, viewing, 341*
 - overview, 332
 - router-on-a-stick, 334-336
 - advantages/disadvantages, 345-346*
 - configuring, 351-355*
 - subinterfaces, configuring, 341-345*
 - troubleshooting
 - commands for, 359-360*
 - configurations, 360-362*
 - IP addresses, 362-365*
 - switch configuration issues, 356-358*
 - intra-VLAN communication, 140-141**
 - intrusion prevention systems (IPSs), 404**
 - IP**
 - addresses, inter-VLAN routing, 362-365
 - information, viewing, 78
 - multicast traffic, 134
 - phones, 132
 - telephony, 133
 - ip address 172.17.10.1 255.255.255.0 command, 344**
 - ip default-gateway command, 75**
 - ip dhcp snooping command, 101**
 - ip dhcp snooping trust command, 101**
 - ip dhcp snooping vlan number command, 101**
 - ip http authentication enable command, 77**
 - IPSs (intrusion prevention systems), 404**
 - ISL (inter-switch link), 149-151**
 - ISM (industrial, scientific, and medical) frequency bands, 383**
 - issues. See troubleshooting**
 - ITU-R (International Telecommunications Union-Radio communications sector), 386**
-
- K–L**

 - keys (RSA)**
 - creating, 94
 - deleting, 95
 - LANs**
 - designs, 56-58
 - segmentation, 55-56
 - WLANS, compared, 381-383
 - latency**
 - Ethernet 802.3 networks, 54-55
 - LAN designs, 57
 - Layer 2 switches**
 - forwarding frames, 62
 - redundancy, 229
 - access-distribution path failure, 232*
 - blocked paths, 230*

- broadcast frames, 234-236*
- broadcast loops, 234*
- broadcast storms, 238-240*
- core switch failures, 232*
- design, 231*
- distribution-core path failures, 232*
- distribution switch failures, 232*
- duplicate unicast frames, 240-241*
- loops in cubicles, 243-244*
- loops in wiring closets, 242-243*
- MAC address tables, 236*
- rerouting traffic, 231*
- troubleshooting, 234-237*

Layer 3 switches

- forwarding frames, 62
- hierarchical networks, 27
- inter-VLAN routing, 336-337
- website, 337
- STP design, 314-316
- VLANs, 141

layers (hierarchical network design model), 2-3

learning RSTP port state, 299

learning STP port state, 269

legacy equipment, 10

line console 0 command, 85-86

line vty 0 15 command, 87

line vty 0 4 command, 87

links

- aggregation, 8, 25-26
- redundant, 9
- types, 297-298
- VLAN trunks, 161-162

Linksys configuration, 411

listening STP port state, 268-269

LMSC (IEEE 802 LAN/MAN Standards Committee), 386

load_helper command, 91

loading helper files, 91

login banners, 92-93

login command

- console access, 86
- virtual terminal access, 87

loops

- cubicles, 243-244
- STP loop prevention, 245
- wiring closets, 242-243

M

MAC addresses

- determining root bridges, 260
- Ethernet, 49
- flooding, 96-99
- port security, 105-106, 109
- switch tables, 51-52
- tables
 - redundancy, 236*
 - switch configuration, 77-78*

MAC forwarding tables, 78

mac-address-table static mac-addr vlan vlan-id interface interface-id command, 77

maintenance (hierarchical network designs), 6

man-in-the-middle attacks (MITM), 403-404

manageability (hierarchical network designs), 6

management interfaces, 73-74

management VLANs, 130, 155-158

- commands
 - show interfaces switchport, 155-158*
 - show interfaces vlan 20, 156*
 - show vlan, 155*
 - show vlan name student, 155*
 - show vlan summary, 156*
- memberships, 158-160
- traffic, 316
- VTP servers, 217-218

manual site surveys, 430

maximum age BPDU timer, 270

MD5 digest, 188

memberships (VLANs), 158-160

memory buffering

- forwarding frames, 60-62
- port-based, 61
- shared memory, 62

message ages, 319

MICs (message integrity checks), 409

MIMO (multiple input/multiple output), 385

MISTP (Multiple Instance STP), 288

MITM (man-in-the-middle) attacks, 403-404

modes

- VLAN trunks, 149-151
 - access, 150*
 - dynamic auto, 149*
 - dynamic desirable, 150*
 - example, 150*
 - trunk, 149*

VTP, 185, 197-198
 client, 197
 server, 197
 server-to-client behavior, 198-199
 server-to-transparent-to-client behavior, 199-200
 transparent, 197

modular switches, 23

modulation, 384

monitoring traffic flow, 15-17

MOTD banners, 92

MSTP (Multiple Spanning Tree Protocol), 287-288

multicast communication, 48

multilayer switches. *See* Layer 3 switches

multiple input/multiple output (MIMO), 385

Multiple Instance STP (MISTP), 288

Multiple Spanning Tree Protocol (MSTP), 287-288

N

names

 configuration files, 91
 VTP domains, 189

native VLANs, 129

 mode issues, 167
 trunks, 166
 configuration, 147-148
 troubleshooting, 165-166

navigating CLI, 63-65

Netstumbler, 409

network diameters. *See* switch diameters

networks

 Ethernet 802.3, 46
 bandwidth/throughput, 52
 broadcast domains, 54
 collision domains, 53-54
 communications, 47-49
 CSMA/CD, 46-47
 duplex settings, 49
 LAN segmentation, 55-56
 latency, 54-55
 network congestion, 55
 switch MAC address tables, 51-52
 switch port settings, 50-51
 management traffic, 133

no banner login command, 92

no enable password command, 89

no enable secret command, 89

no mac-address-table static mac-addr vlan vlan-id interface interface-id command, 77

no service password-encryption command, 90

no shutdown command, 73, 110

no spanning-tree cost command, 250

no spanning-tree portfast command, 272

no switchport access vlan command, 158

no switchport port-security mac-address sticky command, 106

no vlan vlan-id command, 160

non-designated ports

 definition, 248
 election, 279-284
 root bridges, 264

normal data traffic, 134

normal range VLANs, 126

O

OFDM (orthogonal frequency division multiplexing), 384

one-router-interface-per-VLAN routing method

 advantages/disadvantages, 345-346
 configuring, 332-334
 disadvantages, 341
 physical interfaces, configuring, 338-341
 routing table, viewing, 341

open authentication (WLANs), 406

operating configurations, viewing, 78

operating modes (VTP switches), 214

orthogonal frequency division multiplexing (OFDM), 384

OUI (organizational unique identifier), 49

out-of-band connectivity, 317

P

parameters

 show spanning-tree command, 294
 show vtp status command, 187
 switchport mode command, 162

password cisco command

 console access, 86
 virtual terminal access, 87

password password command, 85

passwords, 85

- brute-force attacks, 102
- console access, 85-86
- encrypting, 89-90
- privileged EXEC access, 88-89
- recovering, 90-92
- virtual terminal access, 87-88
- VTP, 194
 - configuring, 208*
 - troubleshooting, 212-213*

path costs, 248

- configuring, 250
- verifying, 251

PBX (private branch exchange), 11**Per-VLAN Spanning Tree Plus. *See* PVST+****Per-VLAN Spanning Tree (PVST), 286-287****performance**

- hierarchical network designs, 5
- switches
 - forwarding rates, 25*
 - hierarchical networks, 24-26*
 - link aggregation, 25-26*
 - port density, 24-25*
- VLANs, 125

ping utility, 354**planning WLANs, 399-401**

- coverage areas, 400-401
- design map, 399

PoE (Power over Ethernet), 26**point-to-point links, 297****populating MAC address tables, 51-52****port-based memory buffering, 61****PortFast, 271-272**

- configuring, 271
- disabling, 272
- troubleshooting configuration errors, 317-318
- verifying, 272
- website, 318

ports

- access, 271-272
- alternate, 300
- backup, 301
- costs, 248
 - configuring/resetting, 250*
 - verifying, 251*
- density, 24-25
- designated
 - definition, 248*
 - election, 279-284*
 - root bridges, 263*
 - RSTP, 300*

disabled, 264

IDs, 265

IEEE 802.1Q trunk ports, 129

nondesigned

definition, 248

election, 279-284

root bridges, 264

numbers, 265

priorities, 265

configuring, 265-266

verifying, 267-268

reassigning to

VLAN 1, 158

VLAN 20, 159

roles, 300-301

root, 248

election, 276-279

RSTP, 300

RSTP

edge ports, 296-297

states, 298-299

security, 105-109

commands, 107

default settings, 107

MAC addresses, 105, 109

security violations, 106-107

sticky address commands, 108

sticky secure MAC addresses, 106

verifying, 109

websites, 108

STA, 247-248

STP

designated/nondesigned port election, 279-284

PortFast, 271-272

root port election, 276-279

states, 269

STP port roles, 263-265

assigning, 264

designated/nondesigned, 263-266

disabled ports, 264

loop-free spanning tree, creating, 267

port IDs, 265

priorities, configuring, 265-266

scenario, 266

states, 268-269

verifying, 267-268

switch port membership modes, 136-138

unused, 110

Power over Ethernet (PoE), 26**pre-shared keys (PSKs), 409****primary root bridges, 292-293**

priorities

- bridges, 259, 293
- ports
 - configuring, 265-266
 - verifying, 267-268

private branch exchange (PBX), 11**privileged EXEC access**

- CLI, 64
- security, 88-89

probes, 396-397**propagation delays, 54****proposal and agreement process (RSTP), 301-308**

- completion, 308
- designated discarding, 305
- new link begins, 301
- synchronization between
 - S1 and S4, 301
 - S2 and S3, 305-306
 - S2 and S4, 302-304
 - S3 and S1, 307-308

protocols

- CDP, 101, 131
- DTP, 149-151
- EAP, 407
- ISL, 149-151
- MSTP, 287-288
- PVST, 286-287
- PVST+, 286-291
 - BIDs, 290
 - configuring, 291-293
 - default switch configuration, 290-291
 - extended system ID field, 289-290
 - overview, 287
 - verifying, 293-294
- Rapid PVST+
 - command syntax, 310
 - configuring, 309-311
 - verifying, 311-312
- RSTP, 287, 294-295
 - BPDU, 295-296
 - edge ports, 296-297
 - link types, 297-298
 - overview, 288
 - port roles, 300-301
 - port states, 298-299
 - proposal and agreement process, 301-308
- STP
 - BIDs, 258-263
 - BPDU, 252-258
 - BPDU timers, 269-270
 - configuring on Cisco 2960 series switch website, 310

convergence. *See STP, convergence*

loop prevention, 245

port roles, 263-268

port states, 268-269

PortFast, 271-272

reconvergence, 246

scenario, 266

STA, 244, 247-252

switch diameters, 270-271

topology, 245-247

trouble avoidance design, 312-316

troubleshooting, 316-319

variants. *See STP, variants*

TKIP, 408

VTP, 182

advertisements, 185, 190-196

benefits, 184

clients, 185, 206, 209

components, 184-186

configuration revision numbers, 187, 192-193

configuring, 204-211

connecting, 210

default configuration, 186-188

domains, 184, 188-190, 213-214

modes, 185, 197-200

overview, 182-184

passwords, 194, 208, 212-213

pruning, 186, 201-204

revision numbers, troubleshooting, 215-216

servers, 185, 217-218

switch operating modes, troubleshooting, 214

transparent mode, 185

troubleshooting, 212-216

VLAN propagation, 183

wireless security, 405-406

access control, 409

authentication, 407-408

configuring, 420-422

encryption, 408-409

pruning VTP, 186, 201-204

example, 201-202

show interfaces trunk command, 203

VLAN 10 example, 203

website, 204

PSKs (pre-shared keys), 409**PSTN (Public Switched Telephone Network), 13****PVST (Per-VLAN Spanning Tree), 286-287****PVST+ (Per-VLAN Spanning Tree Plus), 286-291**

BIDs, 290

configuring, 291-293

default switch configuration, 290-291
 extended system ID field, 289-290
 overview, 287
 verifying, 293-294

Q–R

QoS (quality of service), 10

radio frequencies (RF), 382

radio resource management (RRM), 404

**RADIUS (Remote Authentication Dial In User Service)
 database, 406**

Rapid PVST+

command syntax, 310
 configuring, 309-311
 verifying, 311-312

Rapid Spanning Tree Protocol. *See* RSTP

read-only memory (ROM), 49

recovering passwords, 90-92

redundancy, 229

access-distribution path failure, 232
 blocked paths, 230
 core switch failures, 232
 design, 231
 distribution-core path failures, 232
 distribution switch failures, 232
 hierarchical network designs, 5, 9-10
 issues, 234-235
 broadcast frame egress, 234
 broadcast frame forwarding, 236
 broadcast loops, 234
 broadcast storms, 238-240
 duplicate unicast frames, 240-241
 issues, 237
 MAC address tables, 236
 real-world loop issues, 242-244
 rerouting traffic, 231

reload command, 82

**Remote Authentication Dial In User Service (RADIUS)
 database, 406**

**rename flash:config.text flash: config.text.old
 command, 91**

request advertisements, 196

request to send/clear to send (RTS/CTS), 389

resetting

port costs, 250
 VLAN trunks, 163

restoring configuration files, 81-82

revision numbers (VTP), 215-216

RF (radio frequencies), 382, 429-431

rogue access points, 402-403

roles (ports)

RSTP, 300-301
 STP, 263-265
 assigning, 264
 designated ports, 263, 266
 disabled ports, 264
 loop-free spanning tree, creating, 267
 nondesignated ports, 264-266
 port IDs, 265
 priorities, configuring, 265-266
 scenario, 266
 verifying, 267-268

ROM (read-only memory), 49

root bridges, 247-248

best paths, 249-250
 BIDs, 258-261
 bridge priorities, 259
 configuring, 261-263
 extended system IDs, 259
 fields, 258
 lowest bridge priority, 260
 MAC addresses determining root, 260
 verifying, 262
 BPDUs, 252
 fields, 252
 process, 253-258
 Wireshark capture, 253
 election, 273-276
 path costs, 250-251
 port costs, 250-251
 primary/secondary, 292-293

root ports, 248

election, 276-279
 RSTP, 300

router-on-a-stick routing method

advantages/disadvantages, 345-346
 configuration, 334-336, 351-355
 subinterfaces, configuring, 341-345

routing (inter-VLAN routing)

communication with SVIs, 142
 configuring, 347-350
 Layer 3 switches, 336-337
 one-router-interface-per-VLAN, 332-334
 advantages/disadvantages, 345-346
 disadvantages, 341
 physical interfaces, configuring, 338-341
 routing table, viewing, 341

- overview, 332
- router-on-a-stick, 334-336
 - advantages/disadvantages*, 345-346
 - configuring*, 351-355
 - subinterfaces, configuring*, 341-345
- troubleshooting
 - commands for*, 359-360
 - configurations*, 360-362
 - IP addresses*, 362-365
 - switch configuration issues*, 356-358

RRM (radio resource management), 404

RSA keys

- creating, 94
- deleting, 95
- websites, 96

RSTP (Rapid Spanning Tree Protocol), 287-288, 294-295

- BPDU, 295-296
- edge ports, 296-297
- link types, 297-298
- overview, 288
- ports
 - roles*, 300-301
 - states*, 298-299
- proposal and agreement process, 301-308
 - completion*, 308
 - designated discarding*, 305
 - new link begins*, 301
 - synchronization between S1 and S4*, 301
 - synchronization between S2 and S3*, 305-306
 - synchronization between S2 and S4*, 302-304
 - synchronization between S3 and S1*, 307-308

RTS/CTS (request to send/clear to send), 389

S

scalability (hierarchical network designs), 5

Scavenger class, 136

secondary root bridges, 292-293

Secure Shell. *See* SSH

security

- attacks, 96
 - CDP*, 101
 - MAC address flooding*, 96-99
 - spoofing*, 100-101
 - Telnet*, 102-103
- hierarchical network designs, 5
- login banners, 92-93
- passwords, 85

- console access*, 85-86
- encrypting*, 89-90
- privileged EXEC access*, 88-89
- recovering*, 90-92
- virtual terminal access*, 87-88

ports, 105-109

- commands*, 107
- default settings*, 107
- MAC addresses*, 105, 109
- security violations*, 106-107
- sticky address commands*, 108
- sticky secure MAC addresses*, 106
- verifying*, 109
- websites*, 108

SSH, 93-96

- Telnet, 93
- tools, 103-104
- unused ports, 110
- VLANs, 125
- WLANS, 402
 - configuring*, 415-417
 - protocols*, 405-409, 420-422
 - threats*, 402-404

segmenting LANs, 55-56

server mode (VTP), 197

servers

- AAA, 407
- data, 19-20
- DHCP, 100-101
- SSH, 95
- TFTP, 80-84
- VTP, 185
 - configuring*, 204-208
 - VLANs, managing*, 217-218

server/server traffic, 20

service password-encryption command, 89

service set identifiers (SSIDs), 392, 418-419

seven-switch diameter, 270

shared links, 297

shared memory buffering, 62

show commands, 78

show dtp interface command, 151

show flash command, 78

show history command, 70, 78

show interface command, 78

show interface interface-id switchport command, 359

show interfaces command, 79, 158

show interfaces f0/18 switchport command, 158

- show interfaces FastEthernet 0/1 command, 79
- show interfaces interface-id switchport command, 147
- show interfaces switchport command, 155-158
- show interfaces trunk command, 203
- show interfaces vlan 20 command, 156
- show ip command, 78
- show ip interface brief command, 75
- show ip route command, 344
- show ip ssh command, 95
- show mac-address-table command, 77-78
- show port-security [interface interface-id] address command, 109
- show port-security [interface interface-id] command, 109
- show run command, 294
- show running-config command, 78-79
 - Portfast verification, 272
 - Rapid PVST+ verification, 311
- show spanning-tree active command, 293
- show spanning-tree command, 251, 262
 - designated/nondesignated port election, 283
 - parameters, 294
 - root bridge election verification, 274
 - root port election, 278
- show spanning-tree detail command, 252
- show ssh command, 95
- show startup-config command, 78
- show version command, 78
- show vlan brief command, 153-154
- show vlan command, 155, 158
- show vlan name student command, 155
- show vlan summary command, 156
- show vtp status command, 187, 207
- shutdown commands, 110
- signal attenuation, 389
- site surveys, 429
- small and medium sized business switches, 33
 - Catalyst
 - 2960, 34-35
 - 3560, 35-36
 - 3750, 36
 - 4500, 36-37
 - 4900, 37-38
 - 6500, 38
 - Express 500, 33-34
 - comparing, 39
- softphones, 13
- software
 - converged networks, 12-13
 - status, viewing, 78
- Spanning Tree Algorithm. *See* STA
- spanning-tree cost command, 250
- spanning-tree link-type point-to-point command, 310
- spanning-tree port-priority command, 265
- spanning-tree portfast command, 271, 297
- Spanning Tree Protocol. *See* STP
- spanning-tree vlan 1 priority 24576 command, 262
- spanning-tree vlan 1 root primary command, 262
- spanning-tree vlan 1 root secondary command, 262
- spanning-tree vlan vlan-id priority value command, 262
- spanning-tree vlan vlan-id root primary command, 261
- spanning-tree vlan vlan-id root primary diameter value command, 270
- spanning-tree vlan vlan-id root secondary command, 261
- speed (switch ports), 75-76
- spoofing attacks, 100-101
- SSH (Secure Shell), 93
 - configuring, 94-96
 - server status, viewing, 95
- SSIDs (service set identifiers), 392, 418-419
- STA (Spanning Tree Algorithm), 244
 - best paths, 249-252
 - port types, 247-248
 - root bridges, 248
- stackable switches, 23
- standards (WLANs), 383-386
 - choosing, 384
 - IEEE 802.11, 383
 - IEEE 802.11a, 384
 - IEEE 802.11b, 384-385
 - IEEE 802.11g, 384-385
 - IEEE 802.11n draft, 384-385
 - modulation, 384
- startup configuration, 78
- states (ports)
 - RSTP, 298-299
 - STP, 268-269
- static addresses, 77, 105
- static VLANs
 - configuring, 137
 - interfaces, 154
- sticky secure MAC addresses, 106

store-and-forward switching, 59**STP (Spanning Tree Protocol), 244**

- BIDs, 258-261
 - bridge priorities, 259*
 - configuring, 261-263*
 - extended system IDs, 259*
 - fields, 258*
 - lowest bridge priority, 260*
 - MAC addresses determining root, 260*
 - verifying, 262*
- BPDUs, 252
 - fields, 252*
 - process, 253-258*
 - timers, 269-270*
 - Wireshark capture, 253*
- configuring on Cisco 2960 series switch website, 310
- convergence, 273
 - designated/nondesigned port election, 279-284*
 - root bridge election, 273-276*
 - root port election, 276-279*
 - topology changes, 285-286*
- loop prevention, 245
- PortFast, 271-272
- port roles, 263-265
 - assigning, 264*
 - designated ports, 263, 266*
 - disabled ports, 264*
 - loop-free spanning tree, creating, 267*
 - nondesigned ports, 264-266*
 - port IDs, 265*
 - priorities, configuring, 265-266*
 - scenario, 266*
 - verifying, 267-268*
- port states, 268-269
 - blocking, 268-269*
 - disabled, 269*
 - forwarding, 269*
 - learning, 269*
 - listening, 268-269*
- reconvergence, 246
- scenario, 266
- STA, 244
 - best paths, 249-252*
 - port types, 247-248*
 - root bridges, 248*
- switch diameters, 270-271
- topology, 245-247
- trouble avoidance design, 312-313
 - blocked ports, minimizing, 313-314*
 - Layer 3 switching, 314-316*

- management VLAN traffic, 316*
- not disabling STP, 316*
- troubleshooting, 316-317
 - PortFast configuration errors, 317-318*
 - switch diameters, 318-319*
 - website, 317*
- variants, 286-287
 - MSTP, 287-288*
 - PVST, 286-287*
 - PVST+, 286-294*
 - Rapid PVST+, 309-312*
 - RSTP. See RSTP*

subinterfaces

- inter-VLAN routing, 334, 341-345
- routing commands, 361-362

subset advertisements, 194-196**summary advertisements, 193-194****SVIs (switch virtual interfaces), 142****switch diameters**

- hierarchical network designs, 7
- STP
 - configuring, 270-271*
 - troubleshooting, 318-319*

switch port membership modes (VLANs), 136-138**switch virtual interfaces (SVIs), 142****switches**

- access layer features, 28-29
- boot sequences, 71-72
- choosing, 15
- configuring
 - backing up, 81*
 - default gateways, 74-75*
 - duplex mode, 75-76*
 - erasing configuration files, 84-85*
 - HTTP access, 76-77*
 - MAC address tables, 77-78*
 - management interface, 73-74*
 - preparations, 72*
 - restoring, 81-82*
 - speed, 75-76*
 - storing on TFTP servers, 82-84*
 - verifying, 78-80*
- core layer features, 31-33
- data server analysis, 19-20
- data store analysis, 19-20
- distribution layer features, 30-31
- Ethernet networks
 - MAC address tables, 51-52*
 - port settings, 50-51*
- fixed configuration, 22

- form factors, 22-23
- forwarding frames
 - asymmetric switching*, 60
 - forwarding methods*, 59-60
 - Layer 2/Layer 3 switches*, 62
 - memory buffering*, 60-62
 - symmetric switching*, 60
- hierarchical network performance, 25-26
- Layer 2. *See* Layer 2 switches
- Layer 3
 - forwarding frames*, 62
 - hierarchical networks*, 27
 - inter-VLAN routing*, 336-337
 - website*, 337
 - STP design*, 314-316
 - VLANs*, 141
- modular, 23
- performance, 24
 - forwarding rates*, 25
 - link aggregation*, 25-26
 - port density*, 24-25
- Power over Ethernet (PoE), 26
- security
 - attacks*, 96-103
 - login banners*, 92-93
 - passwords*, 85-92
 - ports*, 105-109
 - SSH*, 93-96
 - Telnet*, 93
 - tools*, 103-104
 - unused ports*, 110
- small and medium sized businesses, 33
 - Catalyst 2960*, 34-35
 - Catalyst 3560*, 35-36
 - Catalyst 3750*, 36
 - Catalyst 4500*, 36-37
 - Catalyst 4900*, 37-38
 - Catalyst 6500*, 38
 - Catalyst Express 500*, 33-34
 - comparing*, 39
- stackable, 23
- topology diagrams, 20-21
- traffic flow analysis, 15-17
- user community analysis, 17-18
- VTP operating modes, 214
- switchport access vlan 10 command**, 357
- switchport access vlan command**, 348
- switchport mode access command**, 108, 348
- switchport mode command**, 162
- switchport mode dynamic auto command**, 149, 351

- switchport mode dynamic desirable command**, 150-151, 351
- switchport mode trunk command**, 149, 160, 357
- switchport nonegotiate command**, 150
- switchport port-security command**, 108
- switchport port-security mac-address sticky command**, 106-108
- switchport port-security maximum 50 command**, 108
- symmetric switching**, 60
- system hardware/software status, viewing**, 78

T

- tables (MAC addresses)**, 236
- TACAS authentication**, 76
- TC (topology change) bit**, 285
- TCA (topology change acknowledgement) bits**, 285
- TCN (topology change notification)**, 285
- technologies**
 - converged networks, 11-12
 - wireless, 380
- Telnet, 93**
 - attacks, 102-103
 - configuring, 93
- Temporal Key Integrity Protocol (TKIP)**, 408
- terminal no history command**, 71
- terminal no history size command**, 71
- TFTP (Trivial File Transfer Protocol) servers**, 80-84
- threats (WLAN security)**, 402
 - denial of service, 404
 - man-in-the-middle attacks, 403-404
 - rogue access points, 402-403
 - website, 404
- timers (BPDU)**, 269-270
- TKIP (Temporal Key Integrity Protocol)**, 408
- tools**
 - ping, 354
 - security, 103-104
 - tracert, 354
 - traffic flow analysis, 16
- topology change (TC) bit**, 285
- topology change acknowledgement (TCA) bits**, 285
- topology change notification (TCN)**, 285
- topology diagrams (hierarchical network switches)**, 20-21
- traceroute command**, 354

tracert utility, 354**traffic**

- flow data, analyzing, 15-17
- VLANs
 - IP multicast traffic, 134*
 - IP telephony traffic, 133*
 - management VLANs, 316*
 - network management traffic, 133*
 - normal data traffic, 134*
- VoIP, 131

transmit power, 399**transparent mode (VTP), 185, 197****transport input all command, 94****transport input telnet command, 94****Triple DES (3DES), 94****Trivial File Transfer Protocol (TFTP) servers, 80-84****troubleshooting**

- hidden node problems, 389
- inter-VLAN routing
 - commands for, 359-360*
 - configurations, 360-362*
 - IP addresses, 362-365*
 - switch configuration issues, 356-358*
- redundancy, 234-237
 - broadcast frames, 234-236*
 - broadcast loops, 234*
 - broadcast storms, 238-240*
 - duplicate unicast frames, 240-241*
 - loops in cubicles, 243-244*
 - loops in wiring closets, 242-243*
 - MAC address tables, 236*
- STP, 316-317
 - PortFast configuration errors, 317-318*
 - switch diameters, 318-319*
 - website, 317*
- VLANs, 171-172
 - allowed VLAN list issues, 169-171*
 - mode issues, 167*
 - native VLANs, 165-166*
 - trunks, 165-171*
- VTP, 212
 - domain names, 213-214*
 - incompatible VTP versions, 212*
 - passwords, 212-213*
 - revision numbers, 215-216*
 - switches operating mode, 214*
- WLANs, 424-425
 - access point placement, 431-433*
 - access point radio/firmware, 426*
 - authentication/encryption, 434*

- channel settings, 426-429*
- connectivity, 424-426*
- RF interference, 429-431*

trunks (VLAN), 144, 149

- configuring, 160-163
 - links, 161-162*
 - resetting, 163*
 - verifying, 162*
- deleting, 164
- IEEE 802.1Q frame tagging, 145-146
- modes, 149-151
 - access, 150*
 - dynamic auto, 149*
 - dynamic desirable, 150*
 - example, 150*
 - trunk, 149*
- native VLANs configuration, 147-148
- operation, 148
- troubleshooting, 165-171
 - allowed VLAN list issues, 169-171*
 - mode issues, 167*
 - native VLANs, 165-166*

type 5 encryption, 90**type 7 encryption, 90****types**

- links, 297-298
- VLANs, 126-130
 - black hole, 128*
 - data, 127*
 - default, 128*
 - management, 130*
 - native, 129*
 - voice, 131-133*
- VTP advertisements, 193-196
 - request, 196*
 - subset, 194-196*
 - summary, 193-194*

U**unicast communication, 47****unicast frames, redundancy, 240-241****untagged frames, 147****unused ports, 110****updating VTP domains, 190****UplinkFast STP extension website, 287****user EXEC mode (CLI), 64****users, community analysis, 17-18****utilities. *See* tools****utility-assisted site surveys, 430**

V

variants (STP), 286-287

- MSTP, 287-288
- PVST, 286-287
- PVST+, 286-294
 - BIDs*, 290
 - configuring*, 291-293
 - default switch configuration*, 290-291
 - extended system ID field*, 289-290
 - overview*, 287
 - verifying*, 293-294
- Rapid PVST+, 309-312
 - command syntax*, 310
 - configuring*, 309-311
 - verifying*, 311-312
- RSTP, 287-288, 294-308
 - BPDU*, 295-296
 - edge ports*, 296-297
 - link types*, 297-298
 - overview*, 288
 - ports*, 298-301
 - proposal and agreement process*, 301-308

verifying

- BIDs*, 262
- designated/non-designated port election, 283-284
- IP addressing commands, 364
- path costs, 251
- Portfast, 272
- ports
 - costs*, 251
 - priorities*, 267-268
 - security*, 109
- PVST+, 293-294
- Rapid PVST+, 311-312
- root bridge election, 274-276
- switch configuration, 78-80
- VLAN trunk configuration, 162
- WLAN connectivity, 423

video networks, 14

viewing

- command history, 78
- flash file system, 78
- flash memory contents, 91
- interface status, 78
- IP information, 78
- MAC forwarding tables, 78
- one-router-interface-per-VLAN routing table, 341
- operating configurations, 78
- SSH server status, 95
- startup configuration contents, 78
- system hardware/software status, 78
- vlan.dat file contents, 153

virtual LANs. *See* VLANs

virtual terminal access, 87-88

vlan.dat file

- contents, viewing, 153
- deleting, 160

VLAN Trunking Protocol. *See* VTP

vlan vlan-id command, 154

VLANs (virtual LANs), 3, 123

- after VLANs three buildings example, 123
- before VLANs examples, 122-123
- benefits, 124-125
- black hole, 128
- broadcast domains, 54, 138-143
 - inter-VLAN communication with SVIs*, 142
 - intra-VLAN communication*, 140-141
 - Layer 3 switching*, 141
 - single VLANs*, 138
 - two VLANs*, 139
- broadcast storm mitigation, 125
- configuring, 152-154
 - adding VLANs*, 152-153
 - static VLAN interfaces*, 154
 - switch topology*, 152
 - vlan.dat file contents, viewing*, 153
- data, 127
- default, 128
- deleting, 160
- distribution layer, 3
- dynamic, 137
- ID ranges, 126
- inter-VLAN routing. *See* inter-VLAN routing managing, 130, 155-158
 - memberships*, 158-160
 - show interfaces switchport command*, 155-158
 - show interfaces vlan 20 command*, 156
 - show vlan command*, 155
 - show vlan name student command*, 155
 - show vlan summary command*, 156
 - traffic*, 316
 - with VTP servers*, 217-218
- native, 129
 - modes*, 167
 - trunks*, 165-166
- overview, 123-124
- performance, 125
- port reassignments to
 - VLAN 1*, 158
 - VLAN 20*, 159
- security, 125
- static, configuring, 137
- SVIs, configuring, 142
- switch port membership modes, 136-138

- traffic
 - IP multicast*, 134
 - IP telephony*, 133
 - network management*, 133
 - normal data*, 134
- troubleshooting, 171-172
- trunks, 144
 - configuring*, 160-163
 - deleting*, 164
 - IEEE 802.1Q frame tagging*, 145-146
 - modes*, 149-151
 - native VLANs*, 147-148
 - operation*, 148
 - troubleshooting*, 165-171
- types, 126-130
 - black hole*, 128
 - data*, 127
 - default*, 128
 - management*, 130
 - native*, 129
 - voice*, 131-133
- voice, 131-133
 - Cisco IP phone integrated switch*, 132
 - configuring*, 137
 - output example*, 132-133
 - VoIP traffic requirements*, 131
- voice networks, 13**
- Voice over IP (VoIP), 11, 131**
- voice VLANs, 131-133**
 - Cisco IP phone integrated switch*, 132
 - configuring*, 137
 - output example*, 132-133
 - VoIP traffic requirements*, 131
- VoIP (Voice over IP), 11**
 - converged networks*, 11
 - traffic requirements*, 131
- VTP (VLAN Trunking Protocol), 182**
 - advertisements*, 185, 190-192
 - 802.1Q frame encapsulation*, 191
 - configuration revision numbers*, 192-193
 - frame structure*, 191
 - header/message fields*, 190
 - types*, 193-196
 - benefits*, 184
 - clients*, 185, 206, 209
 - components*, 184-186
 - configuring*, 204-206
 - access ports*, 211
 - clients*, 206, 209
 - confirming*, 210-211
 - connections*, 210
 - reference topology*, 204
 - revision numbers*, 187, 192-193
 - servers*, 204-208
 - connecting*, 210
 - default configuration*, 186-188
 - domains*, 184, 188-190
 - default VTP configuration*, 189
 - names*, 189, 213-214
 - two domain example*, 188
 - updates*, 190
 - modes*, 185, 197-198
 - client*, 197
 - server*, 197
 - server-to-client behavior*, 198-199
 - server-to-transparent-to-client behavior*, 199-200
 - transparent*, 197
 - overview*, 182-184
 - passwords*, 194
 - configuring*, 208
 - troubleshooting*, 212-213
 - pruning*, 186, 201-204
 - example*, 201-202
 - show interfaces trunk command*, 203
 - VLAN 10 example*, 203
 - website*, 204
 - revision numbers*, troubleshooting, 215-216
 - servers*, 185
 - configuring*, 204-208
 - VLANs, managing*, 217-218
 - switch operating modes*, troubleshooting, 214
 - transparent mode*, 185
 - troubleshooting*, 212
 - domain names*, 213-214
 - incompatible VTP versions*, 212
 - passwords*, 212-213
 - revision numbers*, 215-216
 - switches operating modes*, 214
 - VLAN propagation*, 183
- vtp domain command, 214**
- vtp mode client command, 209**
- vtp mode command, 214**
- vtp mode server command, 207**
- vtp password command, 208, 212**
- vtp pruning command, 201**
- vtp version command, 208, 212**

W-X-Y-Z

war driving, 402

websites

- 802.1Q support, 151
- AAA authentication, 77
- BackboneFast STP extension, 287
- BPDU guards, 271, 287, 318
- Catalyst switches
 - 2960, 35
 - 3560, 36
 - 3750, 36
 - 4500, 37
 - 4900, 38
 - 6500, 39
 - Express 500, 34
- CCNA Exploration: Routing Protocols and Concepts, 349
- Cisco
 - Device Manager, 66
 - EtherChannel, 8, 242, 358
 - Network Assistant, 65
- CiscoView, 65
- disaster recovery, 10
- DTP support, 150-151
- EtherChannels, 8, 242, 358
- high availability discussion, 9
- HP OpenView, 68
- ISL support, 151
- Layer 3 switches, 337
- MSTP, 288
- Netstumbler, 409
- password recovery procedures, 92
- port security, 108
- PortFast, 318
- rapid PVST+ commands, 311
- reload command, 82
- RSA technology, 96
- show interfaces command output fields, 158
- show spanning-tree command parameters, 294
- show vlan command output fields, 158
- SSH, 96
- STP
 - configuration on Cisco 2960 series switch, 310
 - troubleshooting, 317
- switches comparison, 39
- switchport mode command parameters, 162
- TACAS authentication, 77
- TFTP server, 83
- traffic flow analysis tools, 17
- UplinkFast STP extension, 287
- voice VLAN configuration, 138

VTP pruning, 204

WEP keys, 407

Wi-Fi Alliance, 386

WLAN security threats, 404

WEP (Wired Equivalent Privacy) key, 397, 406-407

Wi-Fi Alliance, 386-387

Wi-Fi Protected Access (WPA), 406

wireless

access points, 388-389

association

association, 398

authentication, 397

beacons, 396

probes, 397

design map, 399

NICs, 387, 418

connectivity, verifying, 423

security protocols, 420-422

SSIDs, scanning, 418-419

operation

configurable parameters, 391-393

discovery/connection, 396-398

topologies, 393-395

parameters, configuring, 391-393

routers, 390

security protocols, 405-406

access control, 409

authentication, 407-408

encryption, 408-409

technologies, 380

topologies, 380, 393-395

ad hoc, 394

BSS, 394

ESS, 394

IEEE 802.11, 395

wireless LANs. See WLANs

Wireless Network Connection Status dialog box, 420

Wireless Network Properties dialog box, 420-421

wiring closet loops, 242-243

WLANs (wireless LANs), 379

access, 409-410

access points, 382, 388-389, 410-412

basic wireless settings, 413-415

security, 415-417

authentication

open, 406

protocols, 407-408

WEP, 406

- basic wireless settings, configuring, 413-415
 - network mode*, 413
 - network names*, 413
 - radio bands*, 414
 - SSID broadcasts*, 414
 - standard channels*, 415
 - wide channels*, 414
 - benefits, 379-380
 - BSS, 393
 - certification, 386-387
 - components, 383
 - configurable parameters, 391-393
 - connectivity, 423
 - discovery/connection, 396-398
 - association*, 398
 - authentication*, 397
 - beacons*, 396
 - probes*, 397
 - encryption, 408-409
 - interference, 384
 - LANs, compared, 381-383
 - planning, 399-401
 - coverage areas*, 400-401
 - design map*, 399
 - radio frequencies, 382
 - routers, 390
 - security, 402
 - configuring*, 415-417
 - protocols*, 405-409, 420-422
 - threats*, 402-404
 - standards, 383-386
 - choosing*, 384
 - IEEE 802.11*, 383
 - IEEE 802.11a*, 384
 - IEEE 802.11b*, 384-385
 - IEEE 802.11g*, 384-385
 - IEEE 802.11n draft*, 384-385
 - modulation*, 384
 - topologies, 380, 393-395
 - ad hoc*, 394
 - BSS*, 394
 - ESS*, 394
 - IEEE 802.11*, 395
 - transmit power, 399
 - troubleshooting, 424-425
 - access point placement*, 431-433
 - access point radio/firmware*, 426
 - authentication/encryption*, 434
 - channel settings*, 426-429
 - connectivity*, 424-426
 - RF interference*, 429-431
 - wireless NICs, 387, 418
 - connectivity, verifying*, 423
 - security protocols*, 420-422
 - SSIDs, scanning*, 418-419
 - wireless technologies and standards, 380
- WPA (Wi-Fi Protected Access), 406**