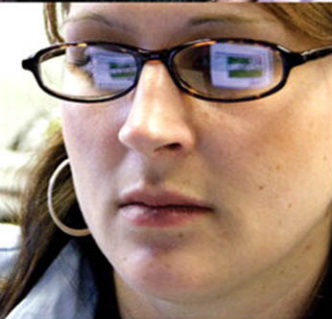




Designing and Supporting Computer Networks

CCNA Discovery
Learning Guide



Kenneth D. Stewart III • Aubrey Adams

Cisco | Networking Academy
Mind Wide Open

Designing and Supporting Computer Networks

CCNA Discovery Learning Guide

Part I: Concepts

Kenneth D. Stewart III

Aubrey Adams

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Designing and Supporting Computer Networks

CCNA Discovery Learning Guide

Part I: Concepts

Kenneth D. Stewart III and Aubrey Adams

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

Stewart, Kenneth (Kenneth D.)

Designing and supporting computer networks / Kenneth Stewart, E. Aubrey Adams.

p. cm. -- (CCNA discovery learning guide)

ISBN-13: 978-1-58713-212-4 (pbk. w/CD)

ISBN-10: 1-58713-212-5 (pbk. w/CD)

1. Computer networks. 2. Computer networks--Management. I. Adams, E. Aubrey. II. Title. III. Series.

TK5105.5.S747 2008

004.6--dc22

2008012080

ISBN-13: 978-1-58713-212-4

ISBN-10: 1-58713-212-5

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

Warning and Disclaimer

This book is designed to provide information about the Designing and Supporting Computer Networks Discovery course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program

Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Managing Editor

Patrick Kanouse

Senior Development Editor

Christopher Cleveland

Project Editor

Seth Kerney

Copy Editors

Keith Cline

Margaret Berson

Technical Editors

Bill Chapman

Susanne Markowski

John Nelson

Lisa Oyler

Editorial Assistant

Vanessa Evans

Book and Cover Designer

Louisa Adair

Composition

Louisa Adair

Indexer

WordWise Publishing
Services, LLC

Proofreaders

Paula Lowell

Debbie Williams

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.



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, CCDP, CCIE, CCIIP, 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)

About the Authors

Kenneth D. Stewart III teaches computer science and computer networking courses at Flour Bluff High School and Delmar College in Corpus Christi, Texas. Kenneth has worked in the field for more than 17 years and has taught for the past 10 years. Before teaching, Kenneth was a nuclear, biological, and chemical warfare specialist in the 82nd Airborne Division at Ft. Bragg, North Carolina. He holds two degrees in computer science and is earning another in occupational career and technology development from Texas A&M, Corpus Christi.

Aubrey Adams is an electronic and computer system engineering lecturer and Cisco Networking Academy CCNA/IP Telephony instructor at Central College of Technical and Further Education (TAFE) in Perth, Western Australia. Coming from a background in telecommunications design, with qualifications in electronic engineering and management, and graduate diplomas in computing and education, he teaches across a broad range of related vocational education and training areas. In 2007, Aubrey took leave from Central TAFE to work as a member of the Networking Academy CCNA Exploration and Discovery course development teams. Since returning to teaching, he continues to contribute to Academy curriculum maintenance and development.

About the Contributing Authors

Allan Reid is the curriculum lead and a CCNA/CCNP instructor at the Centennial College CATC in Toronto, Canada. Allan is a professor in the Information and Communications Engineering Technology department and an instructor and program supervisor for the School of Continuing Education at Centennial College. He has developed and taught networking courses for both private and public organizations and has been instrumental in the development and implementation of numerous certificate, diploma, and degree programs in networking. Allan is also a curriculum developer for the Cisco Networking Academy.

Jim Lorenz is an instructor and curriculum developer for the Cisco Networking Academy. Jim co-authored several Cisco Press titles. He has more than 20 years of experience in information systems, ranging from programming and database administration to network design and project management. Jim has developed and taught computer and networking courses for numerous public and private institutions.

About the Technical Reviewers

William (Bill) Chapman is employed at Arcadia Unified School District, where he teaches advanced placement computer science, robotics, and the Cisco CCNA program. Bill has also taught the Cisco CCNA program at Pasadena City College. Bill has a master's degree in information systems management from the University of Phoenix and a bachelor of science degree in natural science, geoscience option from California State University, Los Angeles. Bill has CompTIA certifications in A+ Computer Servicing, Network+, and i-Net+.

Lisa Oyler is a Cisco Certified Academy Instructor at Summit Technology Academy in Lee's Summit, Missouri. She earned her bachelor of science degree in business education and master's degree in Curriculum and Instruction/Business from the University of Central Missouri. Lisa has been a Networking Academy instructor since August 2001, and has CCNA, Network+, A+, and i-Net+ certifications.

Susanne Markowski, Associate Professor of Information Systems Security at Anne Arundel Community College, Maryland, has been an active Cisco Academy Instructor since 2005. Susanne has a Master of Management degree from the University of Maryland University College, Adelphi, Maryland, and a bachelor of art degree in education from Goucher College, Towson, Maryland.

John Nelson teaches the Cisco Networking Academy at the Advance Technology Center and has been an active CCAI since 2000. John will complete his master of science in occupational technical studies in community college teaching with a concentration of business IT courses from Old Dominion University at Norfolk, Virginia in 2008. He currently holds valid CCNA and Microsoft Certified Systems Engineer certifications. Additionally, he was a member of the Small Market Trial team for Discovery 3 and 4. Presently, John is a member of the Discovery Assessment Team.

Dedications

This book is dedicated to my wife, Aletia, and my daughter, RyeLee. Your support and love have guided me through the long hours and hard work. Thank you for your patience, understanding, support, and love.

—Kenneth D. Stewart III

Dedicated to Jan, my wife; for always being there with her support, understanding, and love. And to Ben and Mel, my son and daughter; my inspirations.

—Aubrey Adams

Acknowledgments

We want to thank Allan Reid and Jim Lorenz for leading the way with the first three *CCNA Discovery Learning Guides* and providing great guidance and inspiration. To Mary Beth Ray, Chris Cleveland, Seth Kerney, and the Cisco Press team, thank you for your assistance and patience throughout this project. The technical editing skills of Bill Chapman, Lisa Oyler, Susan Markowski, and John Nelson ensured the final content was accurate and clear, and were much appreciated.

We also acknowledge the commitment and efforts of the members of all Cisco Networking Academy CCNA Discovery development teams who worked tirelessly to ensure courses like Designing and Supporting Computer Networks became a reality. And to the global community that is the Cisco Networking Academy—the Cisco Academy managers, the instructors, the students, and alumni—thank you for providing us with the opportunity to make a difference.

Contents at a Glance

Part I Concepts

Introduction xlii

Chapter 1	Introducing Network Design Concepts	1
Chapter 2	Gathering Network Requirements	49
Chapter 3	Characterizing the Existing Network	79
Chapter 4	Identifying Application Impacts on Network Design	113
Chapter 5	Creating the Network Design	149
Chapter 6	Using IP Addressing in the Network Design	181
Chapter 7	Prototyping the Campus Network	211
Chapter 8	Prototyping the WAN	237
Chapter 9	Presenting and Implementing the Network Design	269
Chapter 10	Course Summary: Putting It All Together	289
Appendix A	Check Your Understanding and Challenge Questions Answer Key	293
Appendix B	StadiumCompany Story	303
Appendix C	FilmCompany Story	309
Glossary		317
Index		333

Part II Labs

Introduction to Part II 373

Chapter 1 Introducing Network Design Concepts: Labs 375

Chapter 2 Gathering Network Requirements: Labs 415

Chapter 3 Characterizing the Existing Network: Labs 453

Chapter 4 Identifying Application Impacts on Network Design: Labs 523

Chapter 5 Creating the Network Design: Labs 587

Chapter 6 Using IP Addressing in the Network Design: Labs 625

Chapter 7 Prototyping the Campus Network: Labs 655

Chapter 8 Prototyping the WAN: Labs 703

Chapter 9 Presenting and Implementing the Network Design: Labs 757

Chapter 10 Putting It All Together: Lab 779

Appendix A StadiumCompany Story 783

Appendix B FilmCompany Story 789

Appendix C Lab Equipment Interfaces and Initial Configuration Restoration 795

Contents

Part I Concepts

Introduction **xlii**

Chapter 1 Introducing Network Design Concepts **1**

Objectives **1**

Key Terms **1**

Discovering Network Design Basics 2

Network Design Overview 2

Network Requirements 2

Building a Good Network 2

Network Requirements 3

Fundamental Design Goals 3

The Benefits of a Hierarchical Network Design 3

Hierarchical Network Design 3

Modular Design of Cisco Enterprise Architectures 5

Network Design Methodologies 6

Step 1: Identifying Network Requirements 7

Step 2: Characterizing the Existing Network 7

Step 3: Designing the Network Topology 7

Investigating Core Layer Design Considerations 9

What Happens at the Core Layer? 9

Goals of the Core Layer 10

Core Layer Technologies 11

Redundant Links 11

Mesh Topology 11

Network Traffic Prioritization 12

Preventing Failures 12

Reducing Human Error 13

Network Convergence 13

Convergence Definition and Factors 14

Selecting a Routing Protocol for Acceptable Convergence Time 14

Design Considerations with Convergence in Mind 14

Investigating Distribution Layer Design Considerations 14

What Happens at the Distribution Layer? 14

Distribution Layer Routing 14

Trunks 15

Redundant Links 15

Distribution Layer Topology 16

Limiting the Scope of Network Failure 16

Limiting the Size of Failure Domains 17

Switch Block Deployment 17

Building a Redundant Network at the Distribution Layer 18

Traffic Filtering at the Distribution Layer 19

Filtering Network Traffic 19

Complex ACLs 20

Placing ACLs 20

Routing Protocols at the Distribution Layer (1.3.5) 21

Route Summarization 21

Investigating Access Layer Design Considerations	22
<i>What Happens at the Access Layer?</i>	22
<i>Access Layer Physical Considerations</i>	23
<i>Wiring Closets</i>	23
<i>The Impact of Converged Networking at the Access Layer</i>	24
<i>The Need for Availability at the Access Layer</i>	24
<i>Access Layer Management</i>	25
<i>Designing for Manageability</i>	25
Network Topologies at the Access Layer	26
How VLANs Segregate and Control Network Traffic	26
<i>VLANs in the Past</i>	26
<i>VLANs Now</i>	27
Services at the Network Edge	27
<i>Providing QoS to Network Applications</i>	27
<i>Classification</i>	28
Security at the Network Edge	28
Security Measures	29
<i>Providing Physical Security</i>	29
<i>Securing Access Layer Networking Devices</i>	30
<i>Recommended Practice on Security</i>	30
Investigating Server Farms and Security	30
What Is a Server Farm?	30
Security, Firewalls, and Demilitarized Zones	32
<i>Protecting Server Farms Against Attack</i>	32
<i>Demilitarized Zones</i>	33
<i>Protecting Against Internal Attacks</i>	33
High Availability	33
<i>Building In Redundancy</i>	33
<i>Virtualization</i>	34
Investigating Wireless Network Considerations	34
Network Design Considerations Unique to WLANs	34
<i>Physical Network Design</i>	35
<i>Logical Network Design</i>	36
Network Access Considerations Unique to WLANs	37
<i>Open Guest Access</i>	37
<i>Secured Employee Access</i>	37
<i>Best Practice Guidelines for WLAN Access</i>	37
Supporting WANs and Remote Workers	39
Design Considerations at the Enterprise Edge	39
<i>Cost of Bandwidth</i>	39
<i>QoS</i>	40
<i>Security</i>	40
<i>Remote Access</i>	40
Integrating Remote Sites into the Network Design	40
<i>MPLS</i>	41
<i>VPNs</i>	42
Redundancy and Backup Links	42
Summary	44
Activities and Labs	45

Check Your Understanding	46
Challenge Questions and Activities	48

Chapter 2 Gathering Network Requirements 49

Objectives	49
-------------------	-----------

Key Terms	49
------------------	-----------

Introducing Cisco Lifecycle Services 50

Case Study: Sports Stadium Network	51
The Network Lifecycle Prepare Phase	52
The Network Lifecycle Plan Phase	53
<i>The Project Plan</i>	53
The Network Lifecycle Design Phase	54
<i>Planning the Installation</i>	55
The Network Lifecycle Implement Phase	55
<i>Testing the New Network</i>	55
The Network Lifecycle Operate Phase	56
<i>Defining Policies and Procedures</i>	56
The Network Lifecycle Optimize Phase	56

Explaining the Sales Process 57

Respond to a Customer Request for a Proposal or Quote	57
<i>Response Document</i>	57
Attend a Prebid Meeting	59
Explain the Request for a Proposal	59
Explain the Request for Quote	60
Explain the Role of the Account Manager	61
<i>Communications Channel</i>	61
<i>Account Manager Responsibilities</i>	61
Explain the Role of the Presales Systems Engineer	61
Explain the Role of the Network Designer	62
Explain the Role of the Postsales Field Engineer	63

Preparing for the Design Process 63

Working with the Customer	63
<i>The Importance of Interpersonal Skills</i>	63
Defining the Customer	64
<i>Identifying Relevant Information</i>	64
<i>Adding User Access</i>	65
<i>Identifying Business Goals and Priorities</i>	65
<i>Prioritizing Goals</i>	66

Identifying Technical Requirements and Constraints 66

Defining Technical Requirements	66
Identifying Constraints	69

Identifying Manageability Design Considerations 69

Using the Top-Down or Bottom-Up Approach	69
Monitoring Network Operations	70
Using Tools for Network Monitoring	72

	Summary	74
	Chapter Activities and Labs Summary	75
	Check Your Understanding	76
	Challenge Question and Activities	77
Chapter 3	Characterizing the Existing Network	79
	Objectives	79
	Key Terms	79
	Documenting the Existing Network	80
	Creating a Network Diagram	80
	<i>Upgrading the Stadium Network</i>	80
	<i>Producing a Network Topology Map</i>	81
	<i>Obtaining Information About Devices and Data Routes</i>	81
	Diagramming the Logical Architecture	82
	<i>Creating an Existing Network Overview Diagram</i>	82
	<i>Creating Network Segment Diagrams</i>	83
	<i>Creating a Logical Diagram of the Main Stadium LAN</i>	84
	Developing a Modular Diagram	85
	Strengths and Weaknesses of the Existing Networks	86
	<i>Strengths of the Existing Stadium Network</i>	86
	<i>Overcoming Weaknesses in Preparation for the Network Upgrade</i>	87
	Updating the Existing Cisco IOS	88
	Investigating the Installed Cisco IOS Software	89
	<i>Using the show version Command</i>	89
	<i>IOS Software File-Naming Conventions</i>	90
	<i>Testing the Upgrade Process</i>	91
	Choosing an Appropriate Cisco IOS Image	91
	<i>Using Feature Navigator</i>	91
	Download and Install Cisco IOS Software	92
	The Router Startup Process	94
	Upgrading Existing Hardware	95
	Investigating Installed Hardware Features	95
	Investigating Appropriate Hardware Options	95
	Installing a New Hardware Option	96
	Performing a Wireless Site Survey	97
	Visiting the Customer Site	97
	<i>Preparation</i>	97
	<i>Site Survey</i>	98
	<i>Security</i>	98
	<i>Safety Guidelines</i>	98
	Physical Network Considerations	98
	Planning a Wireless Site Survey	100
	Performing a Wireless Site Survey	100
	Documenting Network Design Requirements	102
	Overall Project Goal	102
	Project Scope	103

Business Goals and Technical Requirements 104

Business Goals 105

Technical Requirements 105

Users 106

Applications 106

Existing Network Characterization 107

Summary 109

Chapter Activities and Labs Summary 110

Check Your Understanding 111

Chapter 4 Identifying Application Impacts on Network Design 113

Objectives 113

Key Terms 113

Characterizing Network Applications 114

The Importance of Application Performance 114

Characteristics of Different Application Categories 115

Information Gathering 116

How Traffic Flow Affects Network Design 116

Internal Traffic 117

External Traffic 117

How Application Characteristics Affect Network Design 117

Explaining Common Network Applications 118

Transaction-Processing Applications 119

Redundancy in Transaction Processing 120

Secure Transaction Processing 121

Real-Time Streaming and Voice 121

Infrastructure 122

VoIP 122

IP Telephony 122

Real-Time Video Protocols 122

File Transfer and E-mail 123

E-mail 123

Supporting File Transfer and E-mail Applications 124

HTTP and Web Traffic 124

Network Media 124

Redundancy 125

Security 125

Microsoft Domain Services 125

Ports Used by Microsoft Domain Services 126

Active Directory and DNS 126

Introducing Quality of Service 127

Traffic Queues 128

QoS Mechanisms 128

Hardware and Software Queues 128

Implementing QoS in Traffic Queues 129

Priorities and Traffic Management 129

Where Can QoS Be Implemented? 130

Layer 2 Devices 131

<i>Layer 3 Devices</i>	131
<i>Classification and Marking</i>	131

Examining Voice and Video Options 131

Converged Network Considerations	131
<i>Managing Converged Networks</i>	132
<i>Quality of Service (QoS) on Converged Networks</i>	132
Requirements of an IP Telephony Solution	133
<i>Isolating Traffic</i>	133
<i>Benefits of Separate VLANs</i>	134
<i>Traditional Telephony</i>	135
<i>VoIP</i>	136
<i>IP Telephony</i>	136
Video: Live and On-Demand	138
Supporting Remote Workers with Voice and Video	138

Documenting Applications and Traffic Flows 139

What Is a Traffic Flow?	139
<i>Traffic Control</i>	139
<i>Application Traffic Flows</i>	139
Diagramming Internal (Intranet) Traffic Flows	140
Diagramming Traffic Flows to and from Remote Sites	142
Diagramming Traffic Flows to and from Remote Sites	143
Diagramming Extranet Traffic Flows	143

Summary 145

Chapter Activities and Labs Summary 146

Check Your Understanding 147

Chapter 5 Creating the Network Design 149

Objectives 149

Key Terms 149

Analyzing the Requirements 150

Analyzing Business Goals and Technical Requirements	150
<i>Dealing with Constraints</i>	150
<i>Making Trade-Offs</i>	151
Requirements for Scalability	152
Requirements for Availability	153
<i>Availability for E-Commerce</i>	154
<i>The Security Monitoring System</i>	154
<i>The IP Telephone System</i>	154
Requirements for Network Performance	155
Requirements for Security	156

Making Network Design Trade-Offs 157

Selecting an Appropriate LAN Topology 158

Designing an Access Layer Topology	158
<i>Access Layer Requirements</i>	158
<i>2960 Switch Capabilities</i>	159
<i>Limitations of the Existing Equipment</i>	159
<i>Power Requirements</i>	159

Designing Distribution Layer Topology	160
<i>Distribution Layer Requirements</i>	160
<i>Design Constraints</i>	160
<i>Multilayer Switch Capabilities</i>	160
Designing Core Layer Topology	161
<i>Core Layer Requirements</i>	161
Creating the Logical Network Design for the LAN	162

Designing the WAN and Remote Worker Support 163

Determining Connectivity for Remote Sites	163
<i>Extending Services to Remote Locations</i>	163
<i>Adding New WAN Connections</i>	164
<i>Frame Relay Connection Types</i>	165
Defining Traffic Patterns and Application Support	165
Designing VPN Endpoint Connectivity Options	166
Creating the Logical Network Design for the WAN	167

Designing Wireless Networks 168

Designing Coverage Options and Mobility	168
<i>Wireless Network Coverage</i>	168
<i>Unified Wireless and Wired Solutions</i>	168
Locating Wireless APs	170
Redundancy and Resiliency in a Wireless Network	172
Creating the Logical Network Design for the WLAN	172

Incorporating Security 173

Placing Security Functions and Appliances	173
<i>Infrastructure Protection</i>	173
<i>Secure Connectivity</i>	174
<i>Threat Detection, Defense, and Mitigation</i>	174
<i>Implementing Security Services</i>	174
<i>Using Integrated Services</i>	174
Implementing ACLs	175
Updating the Logical Network Design Documentation	175

Summary 177

Chapter Activities and Labs Summary 178

Check Your Understanding 179

Chapter 6 Using IP Addressing in the Network Design 181

Objectives 181

Key Terms 181

Creating an Appropriate IP Addressing Design 182

Using Hierarchical Routing and Addressing Schemes	182
Classful Subnets and Summarization	184
<i>Disabling Automatic Summarization</i>	185
Using VLSM When Designing IP Addressing	185
<i>Variable Length Subnet Masking (VLSM)</i>	185
<i>Classless InterDomain Routing (CIDR)</i>	185
CIDR and Summarization	186

Prefix Addresses and Summarization 187

Creating the IP Address and Naming Scheme 187

Designing the Logical LAN IP Addressing Scheme 187

Reachability of Hosts 188

Physical Layout of the Network 188

Security and Routing Policies 189

Determining the Addressing Blocks 189

Location and Description 189

VLAN or Network Type 190

Number of Networks and Hosts per Network 190

Designating the Routing Strategy 191

EIGRP Load Balancing 191

Unequal-Cost Load Balancing 192

Authentication 192

Key Management 192

Plan for Summarization and Route Distribution 193

Designing the Addressing Scheme 195

Assigning Address Blocks 195

Using Subnet 0 and the All-Is Subnet 196

Designing a Naming Scheme 197

Naming Guidelines 198

Describing IPv4 and IPv6 199

Contrasting IPv4 and IPv6 Addressing 199

Mobility and Security 199

Simpler Header 200

Address Formatting 200

Global Unicast Addresses 202

Reserved Addresses 202

Migrating from IPv4 to IPv6 202

Implementing IPv6 on a Cisco Device 202

Configuring and Verifying RIPng for IPv6 204

RIPng for IPv6 Configuration 204

Summary 206

Chapter Activities and Labs Summary 207

Check Your Understanding 208

Chapter 7 Prototyping the Campus Network 211

Objectives 211

Key Terms 211

Building a Prototype to Validate a Design 212

Prototypes and Pilots 212

Choosing a Pilot or Prototype 212

When to Create a Pilot 213

Creating a Test Plan 213

Verifying the Design Meets Goals and Requirements 214

Benefits of Prototyping 214

Basic Connectivity 214

Functionality Testing 214

Choosing a Testing Method 215

Validating LAN Technologies and Devices	215
<i>Cisco IOS Commands</i>	215
<i>IP Utilities and Tools</i>	216
<i>Protocol Analyzers</i>	216
<i>Network Simulation Tools</i>	216
Testing the Redundancy and Resiliency of the Network	216
<i>Redundant Links</i>	217
<i>Load Balancing</i>	217
Identifying Risks or Weaknesses in the Design	217

Prototyping the LAN 218

Identify Goals and Requirements Met by LAN Design	219
<i>Determining What Needs to Be Tested</i>	219
Creating the Test Plan	220
<i>The Test Plan</i>	220
<i>Testing Using a Sample Topology</i>	221
<i>Simulating a Three-Layer Hierarchy</i>	221
Validating the Choice of Devices and Topologies	222
<i>Routed Versus Flat Topologies</i>	222
Validating the Choice of Routing Protocol	222
Validating the IP Addressing Scheme	223
Identify Risks and Weaknesses	223

Prototyping the Server Farm 224

Identifying Server Farm Goals and Requirements	225
<i>Server Relocation for the Stadium Network</i>	226
Creating the Test Plan	226
<i>Testing the Prototype Network</i>	227
<i>Baseline Measurements</i>	227
Validating Device and Topology Selection	228
<i>LAN Simulation</i>	228
<i>Per VLAN Rapid Spanning Tree Plus</i>	228
<i>Port Roles</i>	228
<i>Stadium Network</i>	229
Validating the Security Plan	230
<i>Availability Requirements</i>	230
<i>Multilayer Security</i>	230
<i>Firewalls</i>	230
<i>Testing the ACL Design</i>	231
Identify Risks and Weaknesses	232
<i>Identified Weakness</i>	232
<i>Recommendations</i>	232

Summary 233

Chapter Activities and Labs Summary 234

Check Your Understanding 235

Chapter 8 Prototyping the WAN 237

Objectives 237

Key Terms 237

Prototyping Remote Connectivity 239

Testing WAN Connectivity with Simulation Software	239
<i>Network Simulation Software</i>	239
<i>Software Limitations</i>	239

Simulating WAN Connectivity in a Lab Environment	240
<i>Simulating a DSL or Cable Connection</i>	240
<i>Simulating Serial Connectivity</i>	241

Prototyping WAN Connectivity 242

Creating the Test Plan	242
Validating the Choice of Devices and Topologies	245
<i>Frame Relay</i>	246
<i>The Local Loop</i>	246
<i>Data-Link Connection Identifier</i>	247
<i>Guaranteed Data Rates</i>	247
<i>Zero CIR</i>	247
<i>Local Management Interface</i>	248
<i>Congestion Control</i>	248
Prototyping the WAN	249
<i>Inverse ARP and Frame Relay Maps</i>	249
<i>Point-to-Point</i>	250
<i>Multipoint</i>	250
Troubleshooting Frame Relay Operation	252
<i>Configuring the Backup Link</i>	252
<i>Troubleshooting a Primary Link Failure</i>	253
Identifying Risks and Weaknesses	256

Prototyping Remote Worker Support 256

Identifying VPN Goals and Requirements	256
<i>Team Office Requirements</i>	256
<i>How a VPN Works</i>	257
<i>VPN Security</i>	257
<i>VPN Server Location</i>	257
Creating the Test Plan	257
<i>Team Scout Support</i>	257
<i>VPN Server Management</i>	257
<i>Cisco EasyVPN</i>	258
Validate Choice of VPN Devices and Topologies	259
<i>VPN Components</i>	259
Prototype VPN Connectivity for Remote Workers	261
<i>IPsec</i>	261
<i>Split Tunnels</i>	261
Validate Placement of VPN Server	263
Identify Risks or Weaknesses	264

Summary 265

Chapter Activities and Labs Summary 266

Check Your Understanding 267

Chapter 9 Presenting and Implementing the Network Design 269

Objectives 269

Key Terms 269

Assembling the Existing Proposal Information 270

Organizing the Existing Information 270

Integrating the Existing Information 271

Developing the Implementation Plan 272

The Implementation Plan 272

Implementing the Network Design 272*Stadium Design* 272*Customer Approval* 272

Determining the Best Installation Method 273

New Installation 273*Phased Installation into Existing Network* 273*Complete Network Replacement* 274*Stadium Installation Method* 274*Estimating Timelines and Resources* 275*Networking Company Resources* 275*Estimated Timeline* 275*Customer-Caused Delays* 275*Project Management Software* 275

Maintenance Windows and Downtime Planning 276

Planning for the Installation 276

Creating the Bill of Materials 276

Identifying Additional Devices 278*Upgrades to Existing Devices* 279*Software Requirements* 279*Existing Applications* 279*New Applications* 279

Recommending SMARTnet Services 280

Additional Service Contracts 280*SMARTnet Agreements* 280

Cisco Technical Services and Support 281

Software IOS Services and Support 282

Creating and Presenting the Proposal 283

Finalizing the Proposal 283

Presenting the Proposal 284

Summary 285**Chapter Activities and Labs Summary 286****Check Your Understanding 286****Chapter 10 Course Summary: Putting It All Together 289****Finding the Right Networking Job 289**

Question Types 290

Interview Methods and Tips 290

Preparing for the CCNA Exam and Lifelong Learning 291**Chapter Activities and Labs Summary 292**

Appendix A	Check Your Understanding and Challenge Questions Answer Key	293
	Chapter 1	293
	Challenge Question and Activities	293
	Chapter 2	294
	Challenge Question and Activities	295
	Chapter 3	295
	Chapter 4	296
	Chapter 5	297
	Chapter 6	298
	Chapter 7	299
	Chapter 8	299
	Chapter 9	300
Appendix B	StadiumCompany Story	303
	StadiumCompany Organization	304
	StadiumCompany Phones and PCs	304
	Existing Facilities and Support	304
	Team A Organization	305
	Team B Organization	306
	Visiting Team Support	306
	Concession Vendor	306
	Luxury Restaurant Organization	306
	Luxury Skybox Support	307
	Press Area Support	307
	Remote Site Support	307
	StadiumCompany Plans	308
Appendix C	FilmCompany Story	309
	FilmCompany Background	310
	Interview with FilmCompany on Current and Future Organization	311
	FilmCompany Network and Topology	313
	Design Considerations	314
Glossary		317
Index		333
Part II	Labs	
	Introduction to Part II	373
	A Word About the Discovery Server CD	374
Chapter 1	Introducing Network Design Concepts: Labs	375
	Lab 1-1: Creating an ACL (1.3.4)	375
	Expected Results and Success Criteria	375
	Background/Preparation	376

Task 1: Analyze the Traffic Filtering Requirements	376
Task 2: Design and Create the ACL	377
Task 3: Cable and Configure the Given Network	378
Task 4: Test the Network Services Without ACLs	379
Task 5: Configure the Network Services ACL	380
Task 6: Apply the ACLs	381
Task 7: Test the Network Services with ACLs	381
Task 8: Observe the Number of Statement Matches	382
Task 9: Clean Up	383
Challenge	383

Lab 1-2: Monitoring VLAN Traffic (1.4.3) 384

Expected Results and Success Criteria	384
Background/Preparation	384
Task 1: Demonstrate Broadcasts Across a Single LAN	385
Task 2: Demonstrate Broadcasts Within Multiple VLANs	387
Task 3: Clean Up	388
Reflection	388

Lab 1-3: Identifying Network Vulnerabilities (1.4.5) 389

Expected Results and Success Criteria	389
Background/Preparation	389
Task 1: Open the SANS Top 20 List	390
Task 2: Review Common Configuration Weaknesses	390
Task 3: Note CVE References	391
Task 4: Investigate a Topic and Associated CVE Hyperlink	391
Task 5: Record Vulnerability Information	391
Task 6: Record the Vulnerability Impact	391
Task 7: Record the Solution	392
Task 8: Zero-Day Attack	392
Reflection	392
Challenge	393

Lab 1-4: Gaining Physical Access to the Network (1.4.6A) 394

Expected Results and Success Criteria	394
Background/Preparation	394
Part 1: Access and Change Router Passwords	395
Task 1: Attempt Login to the Router	395
Task 2: Enter the ROM Monitor Mode	396
Task 3: Change the Configuration Register Setting to Bypass the Startup Configuration File	397
Task 4: Change the Configuration Register Setting to Boot Without Loading the Configuration File	397
Task 5: Restart the Router	398
Task 6: View and Change Passwords	398
Task 7: Change the Configuration Register Setting to Boot and Load the Configuration File	399
Task 8: Verify the New Password and Configuration	399

Task 9: Clean Up 399

Part 2: Access and Change Switch Passwords 399

Task 1: Attempt Login to the Switch 400

Task 2: Enter “Switch” Mode 401

Task 3: Restart the Switch 402

Task 4: View and Change Passwords 402

Task 5: Save the Configuration File 403

Task 6: Verify the New Password and Configuration 403

Task 7: Clean Up 403

Reflection 404

Lab 1-5: Implementing Port Security (1.4.6B) 405

Expected Results and Success Criteria 405

Background/Preparation 405

Task 1: Configure and Test the Switch Connectivity 406

Step 1: Prepare the Switch for Configuration 406

Step 2: Configure the Switch 407

Step 3: Configure the Hosts Attached to the Switch 407

Step 4: Verify Host Connectivity 407

Step 5: Record the Host MAC Addresses 407

Step 6: Determine What MAC Addresses the Switch Has Learned 407

Task 2: Configure and Test the Switch for Dynamic Port Security 408

Step 1: Set Port Security Options 408

Step 2: Verify the Configuration 409

Step 3: Verify the Port Security 409

Step 4: Test the Port Security 411

Step 5: Reactivate the Port 412

Discuss Switch Port Security Using Dynamic MAC Address Assignment 413

Task 3: Clean Up 413

Reflection 413

Chapter 2 Gathering Network Requirements: Labs 415

Lab 2-1: Creating a Project Plan (2.1.3) 415

Expected Results and Success Criteria 415

Background/Preparation 416

Task 1: Evaluate the Current Network, Operations, and Network Management Infrastructure 416

Task 2: Outline the Project Plan 417

Reflection 418

Lab 2-2: Observing Traffic Using Cisco Network Assistant (2.1.6) 419

Expected Results and Success Criteria 419

Background/Preparation 419

Task 1: Establish the Network Baseline Criteria 421

Task 2: Configure Network Connectivity 421

Task 3: Set Up Cisco Network Assistant 421

Task 4: Examine Cisco Network Assistant Features 424

Task 5: Examine Sample Cisco Network Assistant Output 424

Task 6: Clean Up 428

Reflection 428

Lab 2-3: Creating a Network Organization Structure (2.3.2) 429

Expected Results and Success Criteria 429

Background/Preparation 429

Task 1: Determine the Network Users 429

Task 2: Assess Impact of User Network Access 430

Reflection 430

Lab 2-4: Prioritizing Business Goals (2.3.3) 431

Expected Results and Success Criteria 431

Background/Preparation 431

Task 1: Determine the Business Goals 432

Task 2: Prioritize the Business Goals 432

Reflection 433

Lab 2-5: Establishing Technical Requirements (2.4.1) 434

Expected Results and Success Criteria 434

Background/Preparation 434

Task 1: Determine the Technical Requirements 435

Task 2: Prioritize the Technical Requirements 435

Reflection 436

Lab 2-6: Identifying Organizational Constraints (2.4.2) 437

Expected Results and Success Criteria 437

Background/Preparation 437

Task 1: Identify Possible Project Constraints 437

Task 2: Tabulate the Relevant Constraints 438

Reflection 438

Lab 2-7: Monitoring Network Performance (2.5.2) 439

Expected Results and Success Criteria 439

Background/Preparation 439

Task 1: Configure Network Connectivity 441

Task 2: Set Up Cisco Network Assistant 441

Task 3: Monitor Network Traffic 442

Task 4: Review the Data 448

Task 5: Clean Up 448

Reflection 448

Lab 2-8: Investigating Network Monitoring Software (2.5.3) 449

Expected Results and Success Criteria 449

Background/Preparation 449

Task 1: SNMP Overview 450

Task 2: Search for SNMP Monitoring Programs 450

Task 3: Example SNMP Program 452

Reflection 452

Chapter 3 Characterizing the Existing Network: Labs 453**Lab 3-1: Creating a Logical Network Diagram (3.1.2) 453**

Expected Results and Success Criteria 453

Background/Preparation 454

Part 1: Use Cisco IOS Commands to Obtain Information About the Network 454

Task 1: Discover and Document the First Device 454

Task 2: Discover the Remaining Devices 455

Part 2: Use Cisco Network Assistant to Obtain Information About the Network 456

Task 1: Launch Cisco Network Assistant 456

Task 2: Record the Network Topology 456

Task 3: Collate the Network Information 456

Task 4: Clean Up 456

Reflection 456

Device Tables 457

Network Diagram 462

Lab 3-2: Using show version to Create an Inventory List (3.2.2) 463

Expected Results and Success Criteria 463

Background/Preparation 463

Part 1: Determine the Capabilities of the IOS of a Cisco 1841 ISR 464

Task 1: Inspect the Installed Cisco IOS 464

Task 2: Examine a Cisco IOS Feature Set on Cisco.com 465

Task 3: Examine Your Cisco IOS Feature Set on Cisco.com 466

Task 4: Clean Up 466

Part 2: Determine the Capabilities of the IOS of a Cisco 2960 Switch 466

Task 1: Inspect the Installed Cisco IOS 466

Task 2: Examine a Cisco IOS Feature Set on Cisco.com 467

Task 3: Examine your Cisco IOS Feature Set on Cisco.com 468

Task 4: Clean Up 468

Challenge 468

Lab 3-3: Using Feature Navigator (3.2.3) 469

Expected Results and Success Criteria 469

Background / Preparation 469

Part 1: Create a Cisco.com Guest Registration 469

Task 1: Access the Cisco.com Registration Service 470

Task 2: Complete the Registration Process 470

Task 3: Test Your Cisco.com Guest Registration 471

Part 2: Access Cisco.com Feature Navigator 471

Task 1: Access and Log In to Cisco.com 471

Task 2: Examine the Feature Navigator Tools 471

Part 3: Examine 1841 Router IOS Features 472

Task 1: Search by Feature 472

Task 2: Search by Platform 473

Task 3: Search by Feature Set 473

Task 4: Compare Images 474

Part 4: Examine 2960 Switch IOS Features 475

Task 1: Search by Platform 475

Task 2: Search by Feature Set 475

Reflection 476

Lab 3-4: Installing a Cisco IOS Software Image (3.2.4) 477

Expected Results and Success Criteria 477

Background / Preparation 477

Part 1: Back Up the Cisco Router IOS File 478

*Task 1: Configure Network Connectivity 478**Task 2: Run the TFTP Server 479**Task 3: Configure the TFTP Server 479**Task 4: Collect Information to Document the Router 480**Task 5: Copy Cisco IOS Image to the TFTP Server 481**Task 6: Verify the Transfer to the TFTP Server 482*

Part 2: Restore or Upgrade the Current IOS 482

*Task 1: Prepare to Restore or Update the IOS Image 482**Task 2: Copy the IOS Image from the TFTP Server 483**Task 3: Test the Restored IOS Image 484**Task 4: Clean Up 484*

Challenge 484

Lab 3-5: Observing the Router Startup Process (3.2.5) 485

Expected Results and Success Criteria 485

Background/Preparation 485

Task 1: Connect and Set Up the Router 485

Task 2: Restart the Router and Observe the Output 486

Task 3: Examine the Router Startup Output 488

Task 4: Clean Up 489

Reflection/Challenge 489

Lab 3-6: Determining the Router Hardware Options (3.3.2) 490

Expected Results and Success Criteria 490

Background/Preparation 490

Part 1: Inspect a Cisco 1841 ISR 491

*Task 1: Physically Inspect the External Features of the Router 491**Task 2: Use IOS show commands to Inspect the Router 492**Task 3: Compare the Physical and IOS Inspections 493*

Part 2: Examine 1841 Router Hardware Options 493

*Task 1: Access the Cisco.com Documentation 493**Task 2: Record the Router Hardware Information 493**Task 3: Consider Possible Hardware Options 495**Task 4: Clean Up 495*

Reflection 496

Lab 3-7: Preparing for a Site Survey (3.4.1) 497

Expected Results and Success Criteria 497

Background/Preparation 497

Task 1: Clarify and Document the Purpose of the Site Visit 498

Task 2: Prepare a List of Tools and Equipment 499

Task 3: Arrange an Appointment to Visit the Site 501

Task 4: Approach to Site Visit 502

Reflection 503

Lab 3-8: Performing a Wireless Site Survey (3.4.3) 504

Expected Results and Success Criteria 504

Background/Preparation 504

Task 1: Configure the Wireless Client PC1 504

Task 2: Monitor Signal Strength Using NetStumbler 505

Task 3: Relocate the Wireless AP 506

Task 4: Relocate the Wireless AP to a Secure Location 506

Task 5: Clean Up 507

Challenge 507

Lab 3-9: Creating an Overall Project Goal (3.5.2) 508

Expected Results and Success Criteria 508

Background/Preparation 508

Task 1: Gather Information About the Company Goals That This Network Upgrade Will Facilitate 508

Task 2: Summarize Important Goals in a List 509

Task 3: Develop an Overall Project Goal Statement 509

Task 4: Obtain Agreement from the Company on the Project Goal Statement 509

Reflection 510

Lab 3-10: Creating a Scope Statement (3.5.3) 511

Expected Results and Success Criteria 511

Background/Preparation 511

Task 1: Consider How Meeting the Project Goals Will Impact the Existing Network 511

Task 2: Refine and Record the Proposed Changes to the Existing Network 512

Task 3: Define the Areas of the Existing Network Not Covered by the Project 512

Task 4: Compile and Present the Project Scope Document 512

Reflection 513

Lab 3-11: Developing Network Requirements (3.5.4) 514

Expected Results and Success Criteria 514

Background/Preparation 514

Task 1: Record the Company Business Goals and Constraints That Will Influence the Network Design 514

Task 2: Record the Technical Requirements That Will Influence the Network Design 515

Task 3: Record the User Requirements That Will Influence the Network Design 515

Task 4: Record the Application Requirements That Will Influence the Network Design 516

Task 5: Develop the Network Requirements 516

Reflection 517

Lab 3-12: Analyzing an Existing Network (3.5.5) 518

Expected Results and Success Criteria 518

Background/Preparation 518

Task 1: Document and Confirm Existing Network Topology, Addressing, and Naming Schemes	518
Task 2: Identify Those Parts of the Existing Network That Currently Meet the Project Technical Requirements	519
Task 3: Identify Those Parts of the Existing Network That Can Be Scaled to Meet the Project Technical Requirements	520
Task 4: Identify Those Parts of the Existing Network That Do Not Meet the Project Technical Requirements	520
Task 5: Obtain Agreement and Authorization from the Company to Continue with the Network Upgrade Design	521
Reflection	521

Chapter 4 Identifying Application Impacts on Network Design: Labs 523

Lab 4-1: Characterizing Network Applications (4.1.2) 523

Expected Results and Success Criteria	523
Background/Preparation	523
Task 1: Cable and Configure the Network	524
Task 2: Configure NetFlow on the Router Interfaces	525
Task 3: Verify the NetFlow Configuration	525
Task 4: Create Network Data Traffic	526
Task 5: View the Data Flows	527
Task 6: Stop the NetFlow Capture	528
Task 7: Clean Up	529
Reflection	529

Lab 4-2: Analyzing Network Traffic (4.2.3) 530

Expected Results and Success Criteria	530
Background/Preparation	530
Part 1: Design Network Access to FTP and E-mail Services	531
<i>Task 1: FTP Network Considerations</i>	531
<i>Task 2: E-mail Network Considerations</i>	531
Part 2: Configure and Examine Network Traffic	532
<i>Task 1: Configure and Connect the Network</i>	532
<i>Task 2: Configure NBAR to Examine Network Traffic</i>	533
<i>Task 3: Confirm That Protocol Discovery Is Configured</i>	533
<i>Task 4: Generate FTP Network Traffic</i>	533
<i>Task 5: Generate E-mail Network Traffic</i>	533
<i>Task 6: Display the NBAR Results</i>	534
<i>Task 7: Use NBAR to Monitor Other Data Traffic</i>	535
<i>Task 8: Clean Up</i>	535
Challenge	535

Lab 4-3: Prioritizing Traffic (4.3.3) 536

Expected Results and Success Criteria	536
Background/Preparation	536
Task 1: Compile Data Traffic Information	537
Task 2: Prioritize the Data Traffic	538
Task 3: Finalize the Data Priorities	540
Reflection	540

Lab 4-4: Exploring Network QoS (4.3.4) 541

- Expected Results and Success Criteria 541
- Background/Preparation 541
- Task 1: Cable and Configure the Network 541
- Task 2: Examine Priority Queue Commands 543
 - Configuring Priority Queueing 543*
 - Defining the Priority List 543*
- Task 3: Configure an Example Priority Queue 545
- Task 4: Assign the Priority List to an Interface 545
- Task 5: Examine Priority Queue Operation 546
- Task 6: Determine Priority Queue Requirements 547
- Task 7: Clean Up 547
- Challenge 547

Lab 4-5: Investigating Video Traffic Impact on a Network (4.4.4) 549

- Expected Results and Success Criteria 549
- Background/Preparation 549
- Task 1: Cable and Configure the Network 550
- Task 2: Observe Data Traffic 551
- Task 3: Stream the Video File 551
- Task 4: Observe Both Video and Data Traffic 551
- Task 5: Observe Data Flows for Different Serial Link Clock Rates 552
- Task 6: Record Your General Observations 553
- Task 7: Clean Up 553
- Reflection 553

Lab 4-6: Identifying Traffic Flows (4.5.1) 554

- Expected Results and Success Criteria 554
- Background/Preparation 554
- Task 1: Cable and Configure the Network 554
- Task 2: Configure NetFlow on the Interfaces 555
- Task 3: Verify the NetFlow Configuration 556
- Task 4: Create Network Data Traffic 556
- Task 5: View the Data Flows 557
- Task 6: Clean Up 558
- Reflection 558

Lab 4-7: Diagramming Intranet Traffic Flows (4.5.2) 559

- Expected Results and Success Criteria 559
- Background/Preparation 559
- Task 1: Cable and Configure the Network 560
- Task 2: Configure NetFlow on the Interfaces 561
- Task 3: Verify the NetFlow Configuration 561
- Task 4: Create Network Data Traffic 561
- Task 5: View the Data Flows 562

Task 6: Clean Up 562

Challenge 562

Lab 4-8: Diagramming Traffic Flows to and from Remote Sites (4.5.3) 564

Expected Results and Success Criteria 564

Background/Preparation 564

Task 1: Cable and Configure the Network 565

Task 2: Configure NetFlow on Router FC-CPE-1 566

Task 3: Verify the NetFlow Configuration 566

Task 4: Configure NetFlow on Router FC-CPE-2 567

Task 5: Verify the NetFlow Configuration 567

Task 6: Configure NetFlow on Router ISP 567

Task 7: Verify the NetFlow Configuration 568

Task 8: Create Network Data Traffic 568

Task 9: View the Data Flows 569

Task 10: Clean Up 570

Challenge 570

Lab 4-9: Diagramming External Traffic Flows (4.5.4) 572

Expected Results and Success Criteria 572

Background/Preparation 572

Task 1: Cable and Configure the Network 573

Task 2: Configure NetFlow on Router FC-CPE-1 574

Task 3: Verify the NetFlow Configuration 574

Task 4: Configure NetFlow on Router FC-CPE-2 575

Task 5: Verify the NetFlow Configuration 575

Task 6: Configure NetFlow on Router ISP 575

Task 7: Verify the NetFlow Configuration 576

Task 8: Create Network Data Traffic 576

Task 9: View the Data Flows 577

Task 10: Clean Up 578

Challenge 578

Lab 4-10: Diagramming Extranet Traffic Flows (4.5.5) 579

Expected Results and Success Criteria 579

Background/Preparation 579

Task 1: Cable and Configure the Network 580

Task 2: Configure NetFlow on Router FC-CPE-1 581

Task 3: Verify the NetFlow Configuration 581

Task 4: Configure NetFlow on Router FC-CPE-2 582

Task 5: Verify the NetFlow Configuration 582

Task 6: Configure NetFlow on Router ISP 582

Task 7: Verify the NetFlow Configuration 583

Task 8: Create Network Data Traffic 583

Task 9: View the Data Flows 583

Task 10: Clean Up 585

Challenge 585

Chapter 5 Creating the Network Design: Labs 587

Lab 5-1: Applying Design Constraints (5.1.1) 587

Expected Results and Success Criteria 587

Background/Preparation 587

Task 1: Identify Possible Project Constraints 588

Task 2: Tabulate Comments Based on Identified Constraints 588

Task 3: Identify Trade-Offs 589

Reflection 589

Lab 5-2: Identifying Design Strategies for Scalability (5.1.2) 590

Expected Results and Success Criteria 590

Background/Preparation 590

Task 1: Identify Useful Areas for a Design Strategy That Facilitates Scalability 591

Task 2: Create an Access Layer Module Design 591

Task 3: Select Distribution Layer Devices 591

Reflection 592

Lab 5-3: Identifying Availability Strategies (5.1.3) 593

Expected Results and Success Criteria 593

Background/Preparation 593

Task 1: Identify Areas Useful for a Design Strategy that Facilitates Availability 593

Task 2: Create Availability Strategies for Switches 594

Task 3: Create Availability Strategies for Routers 595

Task 4: Create Availability Strategies for Internet/Enterprise Edge 596

Reflection 597

Lab 5-4: Identifying Security Requirements (5.1.5) 599

Expected Results and Success Criteria 599

Background/Preparation 599

Task 1: Identify Potential Security Weaknesses of the FilmCompany Topology 600

Task 2: Create a Security Practices List 601

Task 3: Create a Security Strategy 602

Task 4: Create a Security Design 602

Reflection 603

Lab 5-5: Designing the Core Layer (5.2.3) 604

Expected Results and Success Criteria 604

Background/Preparation 604

Task 1: Identify Core Layer Requirements 605

Task 2: Create a Core Layer Module Design 605

Task 3: Select Core Layer Devices 605

Task 4: Design Redundancy 605

Task 5: Reflection/Challenge 606

Lab 5-6: Creating a Diagram of the FilmCompany LAN (5.2.4) 607

Expected Results and Success Criteria 607

Background/Preparation 607

Task 1: Identify LAN Requirements 608

Task 2: Determine Equipment Features 608

Task 3: Select LAN Devices 608

Task 4: Design Redundancy 608

Reflection/Challenge 609

Lab 5-7: Selecting Access Points (5.4.2) 611

Expected Results and Success Criteria 611

Background/Preparation 611

Task 1: Identify WLAN Requirements 612

Task 2: Determine Equipment Features 612

Task 3: Select WLAN Devices 613

Task 4: Design the WLAN 614

Reflection/Challenge 614

Lab 5-8: Developing ACLs to Implement Firewall Rule Set (5.5.3) 616

Expected Results and Success Criteria 616

Background/Preparation 617

Task 1: Cable and Configure the Network 617

Task 2: Create Firewall Rule Sets and Access List Statements 619

Task 3: Create Extended ACLs 622

Task 4: Configure and Test Access Lists 623

Task 5: Document the Router Configurations 623

Reflection 624

Chapter 6 Using IP Addressing in the Network Design: Labs 625

Lab 6-1: Using CIDR to Ensure Route Summarization (6.1.4) 625

Expected Results and Success Criteria 625

Background/Preparation 626

Task 1: Cable the Network and Configure the PCs 626

Task 2: Perform Basic Router Configurations 627

Task 3: Verify Connectivity of Routers 627

Task 4: Verify Connectivity of Host PCs 628

Task 5: Configure EIGRP Routing on Router R1 628

Task 6: Configure EIGRP on Router R2 628

Task 7: Configure EIGRP Routing on the Router R3 629

Task 8: Verify the Configurations 629

Task 9: Display the EIGRP Routing Table for Each Router 629

Task 10: Remove Automatic Summarization 631

Task 11: Configure Manual Summarization on R2 631

Task 12: Confirm R2 Is Advertising a CIDR Summary Route 631

Task 13: Clean Up 633

Reflection 633

Lab 6-2: Determining an IP Addressing Scheme (6.2.1) 634

Expected Results and Success Criteria 634

Background/Preparation 634

Task 1: Consider VLAN Issues 634

Task 2: Group Network Users and Services 636

Task 3: Tabulating the Groupings 637

Task 4: Determine Total Number of Hosts 638

Reflection/Challenge 639

Lab 6-3: Determining the Number of IP Networks (6.2.2) 640

Expected Results and Success Criteria 640

Background/Preparation 640

Task 1: Review Address Block Size 640

Task 2: Choose or Obtain an Address Block 641

Task 3: Allocate Addresses for the Network 642

Reflection/Challenge 645

Lab 6-4: Creating an Address Allocation Spreadsheet (6.2.5) 646

Expected Results and Success Criteria 646

Background/Preparation 646

Task 1: Create a Spreadsheet Showing VLSM Addresses and Assignment 647

Task 2: Define the Host Address Assignments 649

Task 3: Examine Address Blocks for Overlapping Addresses 650

Reflection/Challenge 650

Lab 6-5: Designing a Naming Scheme (6.2.6) 651

Expected Results and Success Criteria 651

Background/Preparation 651

Task 1: Identify the Appropriate VLAN 651

Task 2: Assign Addresses to the Devices 651

Task 3: Define the Codes for Device Naming 652

Task 4: Establish the Naming Convention 652

Task 5: Apply the Naming Convention 653

Reflection/Challenge 654

Chapter 7 Prototyping the Campus Network: Labs 655

Lab 7-1: Analyzing a Test Plan and Performing a Test (7.1.6) 655

Expected Results and Success Criteria 655

Background/Preparation 656

Example Test Plan 657

Part 1: Analyze the Test Plan 663

Part 2: Configure PCs and Switch VLANs and Perform Test 1 663

Task 1: Connect Devices and Configure PC IP addresses 663

Task 2: Prepare Switch for Configuration 664

Task 3: Configure VLANs on Switch S1 664

Task 4: Perform Test 1—Determine Whether Hosts Can Communicate Between VLANs 665

Part 3: Configure Switch and Router for VLAN Routing and Perform Test 2 666

Task 1: Configure VLAN Trunking on Switch S1 666

Task 2: Perform Basic Configuration of the Router 666

Task 3: Configure VLAN Trunking on the Router 667

Task 4: Perform Test 2—Determine Whether the Hosts Can Communicate Between VLANs 669

Reflection 670

Lab 7-2: Creating a Test Plan for the Campus Network (7.2.2) 671

Expected Results and Success Criteria 671

Background/Preparation 672

Task 1: Review the Supporting Documentation 672

Task 2: Create the LAN Design Test Plan 673

Lab 7-3: Testing the FilmCompany Network (7.2.5) 676

Expected Results and Success Criteria 676

Background/Preparation 677

Part 1: Perform Test 1—Basic Connectivity Test 677

Task 1: Build the Prototype Network 677

Task 2: Verify the Functionality of the Prototype Network 678

Task 3: Record the Test Results in the Results and Conclusions Section of the Test Plan 678

Part 2: Perform Test 2—VLAN Configuration Test 678

Task 1: Configure the Prototype Network 678

Task 2: Verify the VLAN Configuration Design 678

Task 3: Record the Test Results in the Results and Conclusions Section of the Test Plan 679

Part 3: Perform Test 3—VLAN Routing Test 679

Task 1: Configure the Prototype Network 679

Task 2: Verify the VLAN Routing Design 679

Task 3: Record the Test Results in the Results and Conclusions Section of the Test Plan 679

Reflection 680

Lab 7-4: Analyzing Results of Prototype Tests (7.2.6) 681

Expected Results and Success Criteria 681

Background/Preparation 681

Task 1: Identify Any Design Weaknesses 681

Task 2: Determine Risks of Identified Weaknesses 683

Task 3: Suggest Design Improvements to Reduce Risks 683

Task 4: Document Weaknesses and Risks 683

Reflection 683

Lab 7-5: Creating a Server Farm Test Plan (7.3.2) 684

Expected Results and Success Criteria 684

Background/Preparation 685

Task 1: Review the Supporting Documentation	685
Task 2: Determine the Testing Procedures	686
Task 3: Document the Expected Results and Success Criteria	686
Reflection	687

Lab 7-6: Configuring and Testing the Rapid Spanning Tree Prototype (7.3.3) 688

Expected Results and Success Criteria	688
Background/Preparation	688
Task 1: Configure Switch S1 and S2	689
Task 2: Configure Switch S2	690
Task 3: Configure Router R1	691
Task 4: Configure the Hosts	692
Task 5: Perform Basic Connectivity Tests	692
Task 6: Observe Results of Introduced Link and Device Failures	692
Task 7: Clean Up	693
Reflection	694

Lab 7-7: Testing a Prototype Network (7.3.5) 695

Expected Results and Success Criteria	695
Background/Preparation	696
Task 1: Assemble and Connect Network Devices	696
Task 2: Perform Test 1—Basic Connectivity Test	696
Task 3: Perform Test 2—VLAN Configuration Test	696
Task 4: Perform Test 3—VLAN Routing Test	697
Task 5: Perform Test 4—ACL Filtering Test	697
Reflection	698

Lab 7-8: Identifying Risks and Weaknesses in the Design (7.3.6) 699

Expected Results and Success Criteria	699
Background/Preparation	699
Task 1: Identify Areas of Risk and Weakness in the Server Farm Implementation	699
Task 2: Suggest Design Modifications to Address Identified Risks and Weaknesses	701
Reflection	701

Chapter 8 Prototyping the WAN: Labs 703

Lab 8-1: Simulating WAN Connectivity (8.1.3) 703

Expected Results and Success Criteria	703
Background/Preparation	703
Task 1: Cable the Network	704
Task 2: Configure the Serial Interface on R1	704
Task 3: Configure the Serial Interface on R2	705
Task 4: View the show interface Output	705
Task 5: Test Router Connectivity	706
Task 6: Change the Encapsulation Type to PPP	706

Task 7: View the show interface Output	707
Task 8: Configure PPP Authentication with CHAP	708
Task 9: Verify That the Serial Connection Is Functioning	709
Task 10: Clean Up	709
Challenge	709

Lab 8-2: Creating a WAN Connectivity Test Plan (8.2.2) 710

Expected Results and Success Criteria	710
Background/Preparation	711
Task 1: Review the Supporting Documentation	711
Task 2: Review the Test Equipment	712
Task 3: Document Test 1 Information	712
Task 4: Document Test 2 Information	713
Reflection/Challenge	714

Lab 8-3: Configuring and Verifying WAN Backup Links (8.2.5) 715

Expected Results and Success Criteria	715
Background/Preparation	716
Perform Test 1: Frame Relay Configuration Test	716
<i>Task 1: Build the Network</i>	716
<i>Task 2: Configure Router ISPX as a Backup</i>	716
<i>Task 3: Configure the Stadium Edge2 Router</i>	717
<i>Task 4: Configure the FilmCompany BR3 Router</i>	718
<i>Task 5: Conduct Primary Frame Relay Link Testing Based on the Test Plan</i>	719
Perform Test 2: Backup Link Configuration Test	722
<i>Task 1: Configure Floating Static Routes</i>	722
<i>Task 2: Conduct Backup Link Test</i>	723
<i>Task 3: Clean Up</i>	725
Reflection/Challenge	725

Lab 8-4: Evaluating the Prototype WAN Test (8.2.6) 726

Expected Results and Success Criteria	726
Background/Preparation	726
Task 1: Identify Any Weaknesses in the Design	726
Task 2: Determine the Risks If Weaknesses Are Not Corrected	727
Task 3: Suggest How Design Improvements Can Reduce Risk	728
Task 4: Document the Weaknesses and Risks on the Test Plan	728
Reflection	728

Lab 8-5: Creating a VPN Connectivity Test Plan (8.3.2) 729

Expected Results and Success Criteria	729
Background/Preparation	730
Task 1: Review the VPN Design Test Plan	730
Task 2: Review the Equipment Section	730
Task 3: Review the Design and Topology Section	731
Task 4: Review the Test 1 Description, Procedures, and Expected Results	732
Task 5: Review the Test 2 Description, Procedures, and Expected Results	732
Reflection/Challenge	732

Lab 8-6: Creating a Cisco EasyVPN Server (Optional Lab) (8.3.4.3) 733

Expected Results and Success Criteria 733

Background/Preparation 733

Task 1: Connect the Network and Configure the Devices for SDM Access 734

Task 2: Configure the PC to Connect to the Router and Launch Cisco SDM 735

Task 3: Use EasyVPN to Configure the Router as a VPN Server 736

Task 4: Record Test Plan Results 745

Task 5: Clean Up 745

Reflection 745

Lab 8-7: Configuring and Testing the VPN Client (Optional Lab) (8.3.4.4) 746

Expected Results and Success Criteria 746

Background/Preparation 746

Task 1: Connect the Network and Configure the Devices for SDM Access 747

Task 2: Configure the Router as a VPN Server 748

Task 3: Configure the VPN Client 749

Task 4: Verify VPN Tunnel Between Client, Server, and the Internal Network 751

Task 5: Verify VPN Access to an Internal Network Server (Alternate Configuration) 754

Task 6: Record Test Plan Results 755

Task 7: Clean Up 755

Reflection 755

Chapter 9 Presenting and Implementing the Network Design: Labs 757**Lab 9-1: Editing and Organizing the Existing Information (9.1.2) 757**

Expected Results and Success Criteria 757

Background/Preparation 757

Task 1: Collate and Organize the Information 757

Task 2: Review Existing Information 758

Task 3: Organize the Information 758

Task 4: Edit and Finalize the Information 759

Lab 9-2: Creating an Implementation Plan (9.2.1) 760

Expected Results and Success Criteria 760

Background/Preparation 760

Task 1: Determine the Tasks to Implement the Network Design 760

Task 2: Note Identified Success and Failure Criteria 761

Task 3: Include Provision for Customer Approval 762

Task 4: Document Phase 1 763

Task 5: Document Phase 2 763

Task 6: Document Phase 3 763

Lab 9-3: Creating a Phased Installation Plan (9.2.2) 764

Expected Results and Success Criteria 764

Background/Preparation 764

- Task 1: Compare the Installation Methods 764
- Task 2: Select the Installation Method 766
- Task 3: Complete Details for Each Installation Phase 766

Lab 9-4: Creating a Timeline (9.2.3) 767

- Expected Results and Success Criteria 767
- Background/Preparation 767
- Task 1: List and Prioritize Factors Affecting the Timeline 767
- Task 2: Complete Time Details for Each Installation Phase 768
- Task 3: Consider Customer-Caused Delays 768
- Task 4: Using Project Management Software (Optional) 768

Lab 9-5: Creating an Installation Schedule (9.2.4) 769

- Expected Results and Success Criteria 769
- Background/Preparation 769
- Task 1: List and Prioritize Tasks Requiring Current Network Downtime 770
- Task 2: Document Required Downtime on Project Timeline 770
- Task 3: Document Customer Approved Downtime 770

Lab 9-6: Creating the Bill of Materials (9.3.4) 771

- Expected Results and Success Criteria 771
- Background/Preparation 771
- Task 1: List the Items Required 772
- Task 2: Determine the Software Requirements 772
- Task 3: Add Maintenance Contracts 772
- Task 4: Create the BOM 773

Lab 9-7: Compiling the Documentation (9.4.1) 773

- Expected Results and Success Criteria 773
- Background/Preparation 773
- Part 1: Compile the Project Proposal 773
 - Task 1: Finalize the Documentation Requirements 773*
 - Task 2: Prepare the Cover Page 774*
 - Task 3: Prepare the Table of Contents 774*
 - Task 4: Create the Proposal 774*
 - Task 5: Update the Executive Summary 774*
 - Task 6: Organize the Proposal Binder 774*
 - Task 7: Prepare Terms and Signatures Page 774*
- Part 2: Prepare the Presentation 775
 - Task 1: Plan the Presentation 775*
 - Task 2: Create the Presentation 775*

Lab 9-8: Presenting the Project Proposal (9.4.2) 777

- Expected Results and Success Criteria 777
- Background/Preparation 777
- Part 1: Prepare for the Presentation 777
 - Task 1: Review the Content 777*
 - Task 2: Prepare for Questions 777*
 - Task 3: Prepare Yourself 778*
- Part 2: Deliver the Presentation 778

Task 1: Submit Your Portfolio and Proposal 778

Task 2: Begin the Presentation 778

Task 3: Conclude the Presentation 778

Part 3: Participate in the Class Debrief 778

Chapter 10 Putting It All Together: Lab 779

Lab 10-1: Finding the Right Networking Job (10.0.2) 779

Expected Results and Success Criteria 779

Background/Preparation 779

Task 1: Perform a Skills Strength and Interest Assessment 780

Task 2: Search a Job Website for Possible IT Position 781

Task 3: Create a Résumé and Cover Letter 781

Reflection 781

Appendix A StadiumCompany Story 783

StadiumCompany Organization 784

StadiumCompany Phones and PCs 784

Existing Facilities and Support 784

Team A Organization 785

Team B Organization 786

Visiting Team Support 786

Concession Vendor 786

Luxury Restaurant Organization 786

Luxury Skybox Support 787

Press Area Support 787

Remote Site Support 787

StadiumCompany Plans 788

Appendix B FilmCompany Story 789

FilmCompany Background 790

Interview with FilmCompany on Current and Future Organization 791

FilmCompany Network and Topology 793

Design Considerations 794

Appendix C Lab Equipment Interfaces and Initial Configuration Restoration 795

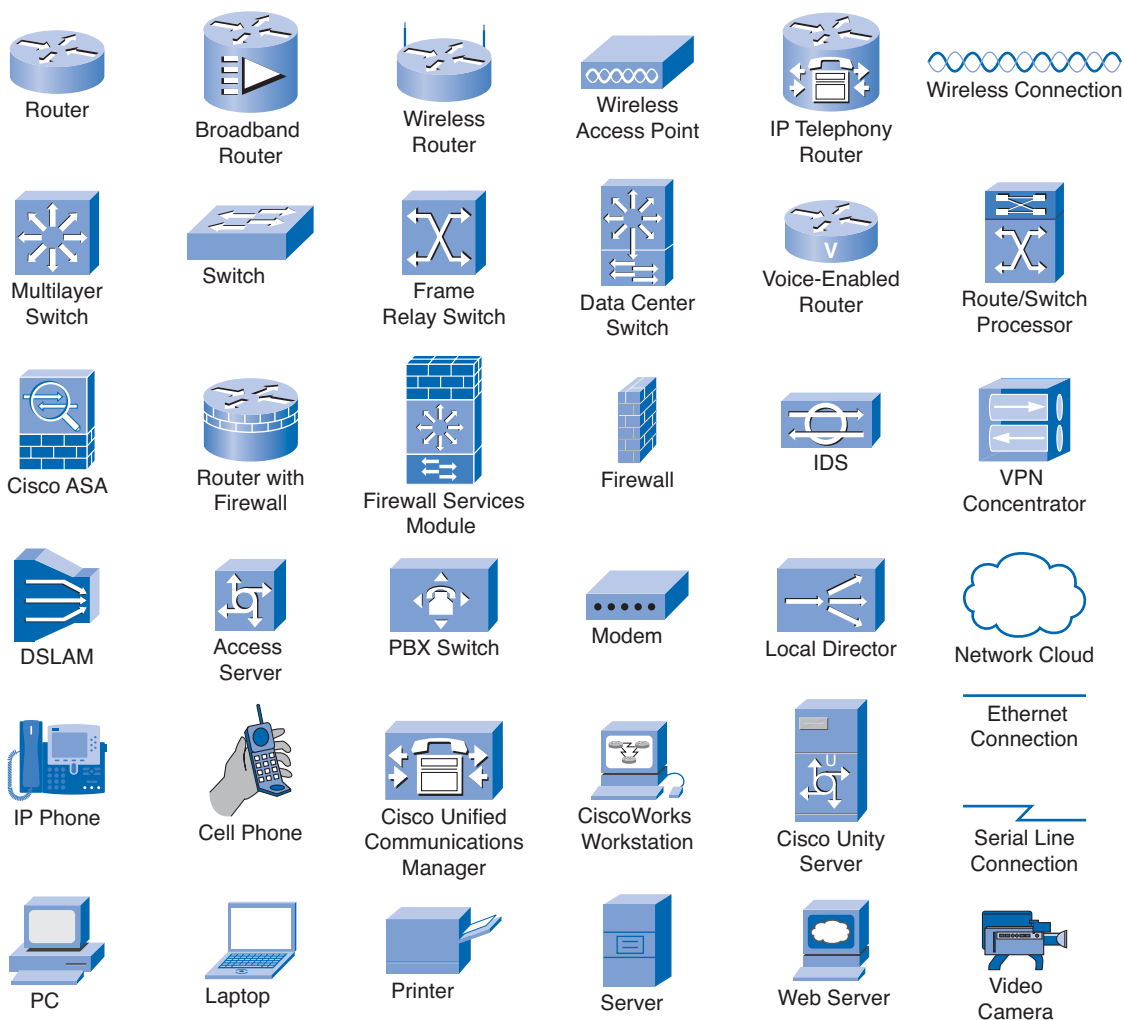
Router Interface Summary 795

Erasing and Reloading the Router 796

Erasing and Reloading the Switch 796

SDM Router Basic IOS Configuration 798

Icons Used in This Book



Command Syntax Conventions

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

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

Introduction

The following Introduction pertains to the Learning Guide as a whole.

Cisco Networking Academy is a comprehensive e-learning program that delivers information technology skills to students around the world. The CCNA Discovery curriculum consists of four courses that provide a comprehensive overview of networking, from fundamentals to advanced applications and services. The goal of the Designing and Supporting Computer Networks course is to assist you in developing the skills necessary to design small enterprise LANs and WANs. The course provides an introduction to collecting customer requirements, translating those requirements into equipment and protocol needs, and creating a network topology that addresses the needs of the customer. It will also familiarize you with how to create and implement a design proposal for a customer. This course prepares you with the skills required for entry-level presales support and entry-level network design jobs.

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

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

- Additional key Glossary terms
- Additional Check Your Understanding and Challenge questions
- Interactive activities and Packet Tracer activities (and all supplemental documents associated with them) on the CD-ROM

Goal of This Book

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

Audience for This Book

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

Book Features

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

Topic Coverage

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

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Learning Guide* encourages you to think about finding the answers as you read the chapter.
- **“How-to” feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes, tips, cautions, and warnings:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter’s key concepts. It provides a synopsis of the chapter and serves as a study aid.



How To

Readability

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

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 230 computer and networking terms.

Practice

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

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

Packet Tracer
Activity

- **Packet Tracer activities:** Interspersed throughout the chapters, you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer enables you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files, and any files associated with the Packet Tracer activities, are available on this book's CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.
- **Interactive activities:** These activities provide an interactive learning experience to reinforce the material presented in the chapter.
- **Labs:** This book contains all the hands-on labs from the curriculum. Part I includes references to the hands-on labs, as denoted by the lab icon, and Part II contains each lab in full. You may perform each lab as you see each lab referenced in the chapter or wait until you have completed the chapter.

A Word About Packet Tracer Software and Activities

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

Packet Tracer 4.1 is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book covers the major topics in the same sequence as the online curriculum for the CCNA Discovery Designing and Supporting Computer Networks course. The online curriculum has ten chapters for this course, so this book has ten chapters with the same names and numbers as the online course chapters.

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

Chapters and Topics

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

- **Chapter 1, “Introducing Network Design Concepts,”** discusses how network designers ensure communications networks can adjust and scale to the demands for new services. Topics include a network design overview, the benefits of a hierarchical network design, and network design methodologies.
- **Chapter 2, “Gathering Network Requirements,”** introduces the StadiumCompany and FilmCompany case studies. The StadiumCompany design project is used in the main text, media, and Packet Tracer activities. The FilmCompany design project is completed in the hands-on labs. Students are introduced to the six phases of the Cisco lifecycle, the proper way to respond to a Request For Proposal or Request For Quote, and the roles of a network partner team. How constraints and trade-offs affect the network design is also covered.
- **Chapter 3, “Characterizing the Existing Network,”** emphasizes how characterizing the network to identify strengths and weaknesses assists in the network design process and how to select the appropriate hardware and software to meet client needs. How to conduct a wireless site survey and the creation of a network Design Requirements document are used to solidify the students’ understanding of the material in this chapter.
- **Chapter 4, “Identifying Application Impacts on Network Design,”** describes how the network designer determines the success criteria for a project. Students learn how the characteristics of various applications affect the design of a network. Students also learn how the network requirements of various common applications, such as voice and video, impact the network. Students are also introduced to quality of service mechanisms and how to diagram the application traffic flows to determine bandwidth requirements of a network design.
- **Chapter 5, “Creating the Network Design,”** introduces how to properly analyze the business goals and technical requirements to create an efficient network design. Students learn how to design the application, distribution, and core layer for a campus design; how to design for the WAN connectivity module with remote worker support; and how to design a wireless topology while incorporating security features.
- **Chapter 6, “Using IP Addressing in the Network Design,”** describes how a network designer selects the appropriate hierarchical IP addressing scheme to meet the physical and logical network requirements. Students also learn to choose a routing protocol and design a route summarization strategy. Additional topics include how to create a logical naming structure for network devices, what IPv6 is, methods to implement IPv6 on a network, and how to implement IPv6 on a Cisco device.
- **Chapter 7, “Prototyping the Campus Network,”** has the student identify the purpose of creating proof-of-concept test. Students also learn how to create a test plan to perform simulated or prototype tests of a network upgrade, and how to identify risks and weaknesses in the design based on the proof-of-concept test conclusions.
- **Chapter 8, “Prototyping the WAN,”** discusses the components and technologies used for WAN connectivity. The components and configuration of Frame Relay connections are covered with regard to configuring a VPN client. Students are also introduced to a proof-of-concept test used to check WAN and remote worker connectivity.

- **Chapter 9, “Preparing the Proposal,”** is a summary activity in which students use what they have learned about designing a network to create a bill of materials, plan an implementation schedule, support contracts, and present a network upgrade proposal as a culminating activity.
- **Chapter 10, “Putting It All Together,”** guides students through the resources available to help their career search, including books, websites, classes, and consultants. Students write résumés, find job openings, and practice interviewing as they prepare to enter the workforce.

This book also includes the following:

- **Appendix A, “Check Your Understanding and Challenge Questions Answer Key,”** provides the answers to the Check Your Understanding questions that you find at the end of each chapter. It also includes answers for the Challenge questions and activities that conclude most chapters.
- **Appendix B, “StadiumCompany Story,”** provides the case study of the fictional StadiumCompany, which needs to upgrade its existing computer network to provide state-of-the-art services. You encounter the StadiumCompany design project in the main text of the chapters and in the interactive activities and Packet Tracer activities.
- **Appendix C, “FilmCompany Story,”** provides the case study of the fictional FilmCompany, which is performing contracted services for the StadiumCompany. The FilmCompany needs network upgrades similar to the StadiumCompany, and you encounter the FilmCompany design project primarily in the hands-on labs found in Part II.
- The **Glossary** provides a compiled list of all the key terms that appear throughout this book plus additional computer and networking terms.

Part II of this book includes the labs that correspond to each chapter. In addition, Part II provides the two case studies and an additional appendix, Appendix C, “Lab Equipment Interfaces and Initial Configuration Restoration,” which provides a reference for router interface designations and instructions for restoring routers and switches to their default configurations.

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. Some Packet Tracer activities also have PDF files associated with them, particularly for the activities in Chapters 7 and 8. These PDF files are also included on the CD-ROM.
- **Interactive activities:** The CD-ROM contains the interactive activities referenced throughout the book.
- **Network design portfolio documents:** To help you create a network design portfolio as you work through the labs in Part II of this book, the CD provides the following files:
 - Example Test Plan (in Microsoft Word format)
 - Prototype Network Installation Checklist (in PDF format)
 - LAN Design Test Plan (in PDF and Microsoft Word format)
 - Server Farm Design Test Plan (in PDF and Microsoft Word format)
 - WAN Design Test Plan (in PDF and Microsoft Word format)
 - VPN Design Test Plan (in PDF and Microsoft Word format)

- **Taking Notes:** This section includes a TXT file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill for not only learning and studying the material, but for on-the-job success, too. Also included in this section is “A Guide to Using a Networker’s Journal” PDF booklet providing important insight into the value of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.
- **IT Career Information:** This section includes a Student Guide to applying the toolkit approach to your career development. Learn more about entering the world of information technology as a career by reading two informational chapters excerpted from *The IT Career Builder’s Toolkit*: “The Job Search” and “The Interview.”
- **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.

This page intentionally left blank

Introducing Network Design Concepts

Objectives

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

- What are the benefits of a hierarchical network design?
- What is the design methodology used by network designers?
- What are the design considerations for the core, distribution, and access layers?
- What are the design considerations for the network enterprise edge?
- What are the design considerations that must be met to support remote workers?
- What are the design considerations for supporting enterprise wireless and/or data center/server farms?

Key Terms

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

Cisco Enterprise Architectures page 5

deterministic network page 5

top-down approach page 7

content networking page 8

storage networking page 8

network backbone page 9

virtual private networks (VPN) page 9

extranet page 9

multilayer switches page 11

load balancing page 11

Enhanced Interior Gateway Routing Protocol (EIGRP) page 11

Open Shortest Path First (OSPF) Protocol page 11

Spanning Tree Protocol (STP) page 11

full-mesh page 11

partial-mesh page 11

hot-swappable page 13

uninterruptible power supply (UPS) page 13

convergence time page 14

switch block page 17

Rapid Spanning Tree Protocol (RSTP) page 18

access control lists (ACL) page 19

dynamic ACL page 20

reflexive ACL page 20

time-based ACL page 20

Intermediate System-to-Intermediate System (IS-IS) Protocol page 21

Power-over-Ethernet (PoE) page 23

failover page 24

network access control page 30

security policy page 30

server farms page 30

data centers page 30

storage-area networks (SAN) page 32

denial-of-service (DoS) page 32

demilitarized zone (DMZ) page 33

Rapid Spanning Tree Protocol Plus (RSTP+) page 34

wireless LAN (WLAN) page 34

Wired Equivalent Privacy (WEP) page 37

Wi-Fi Protected Access (WPA) page 37

service set identifier (SSID) page 37

cell-switched networks page 40

Asynchronous Transfer Mode (ATM) page 40

service level agreements (SLA) page 40

Network designers ensure that our communications networks can adjust and scale to the demands for new services.

To support our network-based economy, designers must work to create networks that are available nearly 100 percent of the time.

Information network security must be designed to automatically fend off unexpected security incidents.

Using hierarchical network design principles and an organized design methodology, designers create networks that are both manageable and supportable.

Discovering Network Design Basics

The sections that follow cover the basics of network design with regard to the following concepts:

- Network design overview
- The benefits of a hierarchical network design
- Network design methodology

Network Design Overview

Computers and information networks are critical to the success of businesses, both large and small. They connect people, support applications and services, and provide access to the resources that keep the businesses running. To meet the daily requirements of businesses, networks themselves are becoming quite complex.

Network Requirements

Today, the Internet-based economy often demands around-the-clock customer service. This means that business networks must be available nearly 100 percent of the time. They must be smart enough to automatically protect against unexpected security incidents. These business networks must also be able to adjust to changing traffic loads to maintain consistent application response times. It is no longer practical to construct networks by connecting many standalone components without careful planning and design.

Building a Good Network

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business.

The steps required to design a good network are as follows:



- Step 1.** Verify the business goals and technical requirements.
- Step 2.** Determine the features and functions required to meet the needs identified in Step 1.
- Step 3.** Perform a network-readiness assessment.
- Step 4.** Create a solution and site acceptance test plan.
- Step 5.** Create a project plan.

After the network requirements have been identified, the steps to designing a good network are followed as the project implementation moves forward.

Network users generally do not think in terms of the complexity of the underlying network. They think of the network as a way to access the applications they need, when they need them.

Network Requirements

Most businesses actually have only a few requirements for their network:

- The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
- The network should reliably deliver applications and provide reasonable response times from any host to any host.
- The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.
- The network should be easy to modify to adapt to network growth and general business changes.
- Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

Fundamental Design Goals

When examined carefully, these requirements translate into four fundamental network design goals:

- **Scalability:** Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users.
- **Availability:** A network designed for availability is one that delivers consistent, reliable performance, 24 hours a day, 7 days a week. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.
- **Security:** Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.
- **Manageability:** No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.

The Benefits of a Hierarchical Network Design

To meet the four fundamental design goals, a network must be built on an architecture that allows for both flexibility and growth.

Hierarchical Network Design

In networking, a hierarchical design is used to group devices into multiple networks. The networks are organized in a layered approach. The hierarchical design model has three basic layers:

- **Core layer:** Connects distribution layer devices
- **Distribution layer:** Interconnects the smaller local networks
- **Access layer:** Provides connectivity for network hosts and end devices

Hierarchical networks have advantages over flat network designs. The benefit of dividing a flat network into smaller, more manageable hierarchical blocks is that local traffic remains local. Only traffic destined for other networks is moved to a higher layer.

Layer 2 devices in a flat network provide little opportunity to control broadcasts or to filter undesirable traffic. As more devices and applications are added to a flat network, response times degrade until the network becomes unusable. Figures 1-1 and 1-2 show the advantages of a hierarchical network design versus a flat network design.

Figure 1-1 Flat Network

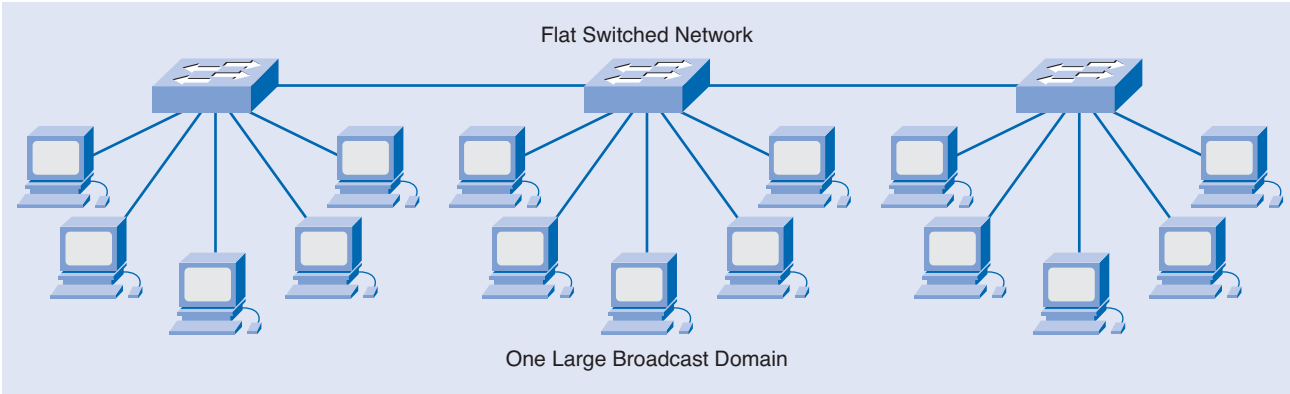
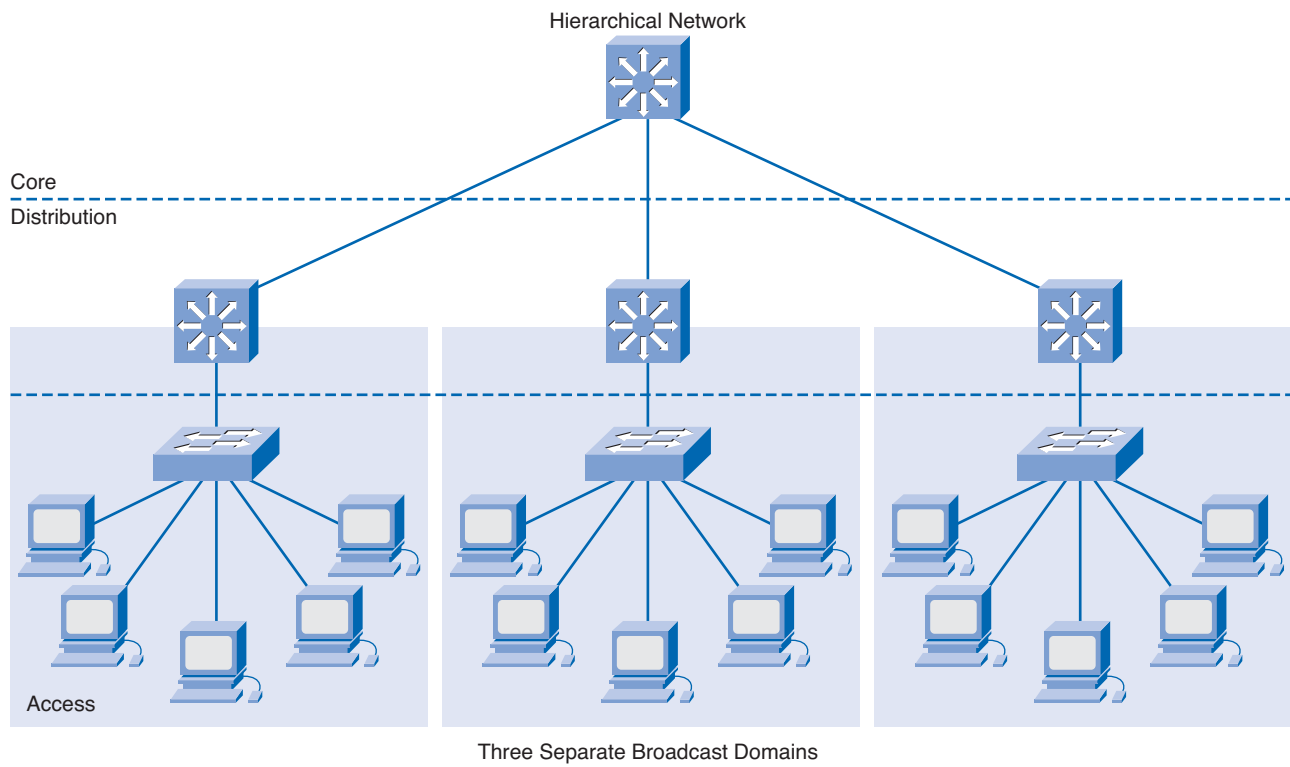


Figure 1-2 Hierarchical Network

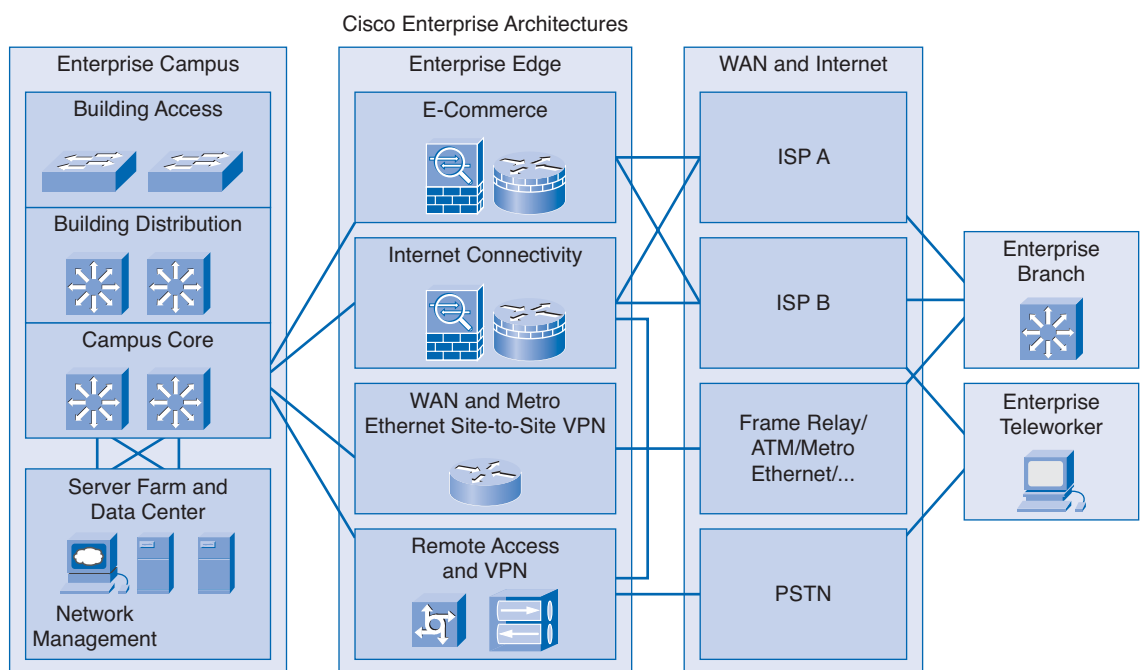


Modular Design of Cisco Enterprise Architectures

The *Cisco Enterprise Architectures* (see Figure 1-3) can be used to further divide the three-layer hierarchical design into modular areas. The modules represent areas that have different physical or logical connectivity. They designate where different functions occur in the network. This modularity enables flexibility in network design. It facilitates implementation and troubleshooting. Three areas of focus in modular network design are as follows:

- **Enterprise campus:** This area contains the network elements required for independent operation within a single campus or branch location. This is where the building access, building distribution, and campus core are located.
- **Server farm:** A component of the enterprise campus, the data center server farm protects the server resources and provides redundant, reliable high-speed connectivity.
- **Enterprise edge:** As traffic comes into the campus network, this area filters traffic from the external resources and routes it into the enterprise network. It contains all the elements required for efficient and secure communication between the enterprise campus and remote locations, remote users, and the Internet.

Figure 1-3 Cisco Enterprise Architectures

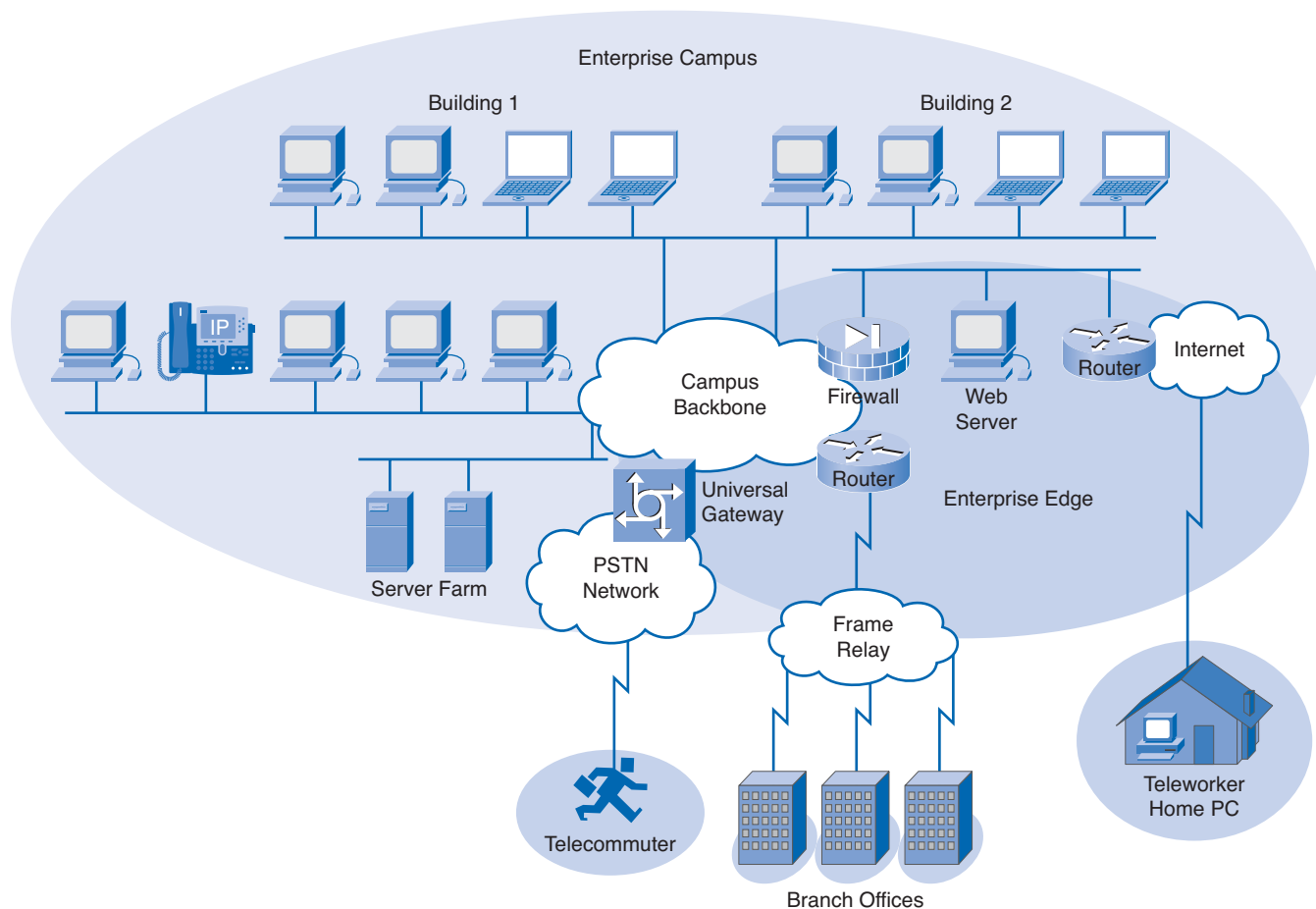


The modular framework of the Cisco Enterprise Architectures as depicted in Figure 1-4 has the following design advantages:

- It creates a *deterministic network* with clearly defined boundaries between modules. This provides clear demarcation points so that the network designer knows exactly where the traffic originates and where it flows.
- It eases the design task by making each module independent. The designer can focus on the needs of each area separately.

- It provides scalability by allowing enterprises to add modules easily. As network complexity grows, the designer can add new functional modules.
- It enables the designer to add services and solutions without changing the underlying network design.

Figure 1-4 Enterprise Campus



Interactive Activity 1-1: Match the Characteristics of the Hierarchical Model and the Cisco Enterprise Architecture (1.1.2)

In this interactive activity, you match the characteristics of the hierarchical model and the Cisco Enterprise Architecture to their correct location. Use file ia-112 on the CD-ROM that accompanies this book to perform this interactive activity.

Network Design Methodologies

Large network design projects are normally divided into three distinct steps:

- Step 1.** Identify the network requirements.
- Step 2.** Characterize the existing network.
- Step 3.** Design the network topology and solutions.

Step 1: Identifying Network Requirements

The network designer works closely with the customer to document the goals of the project. Figure 1-5 depicts a meeting between the designer and the business owner. Goals are usually separated into two categories:

- **Business goals:** Focus on how the network can make the business more successful
- **Technical requirements:** Focus on how the technology is implemented within the network

Step 2: Characterizing the Existing Network

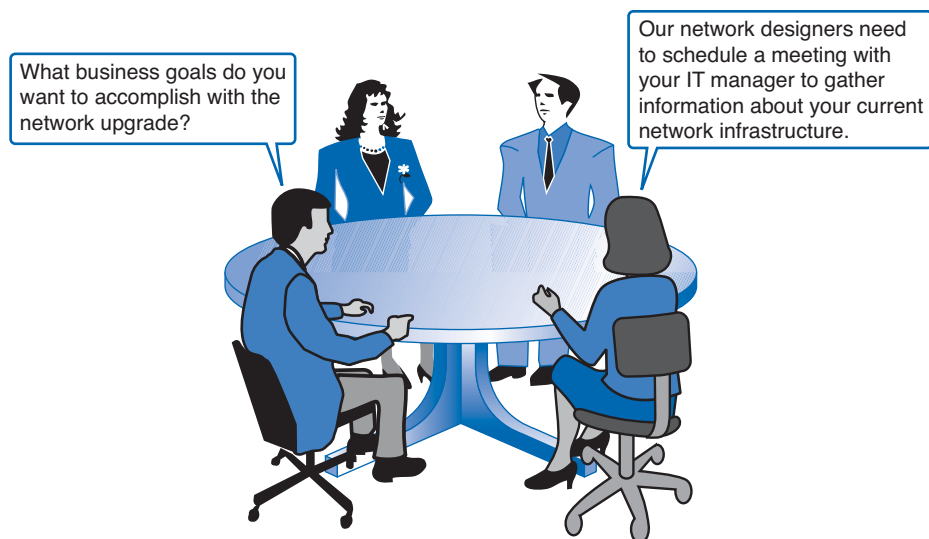
Information about the current network and services is gathered and analyzed. It is necessary to compare the functionality of the existing network with the defined goals of the new project. The designer determines whether any existing equipment, infrastructure, and protocols can be reused, and what new equipment and protocols are needed to complete the design.

Step 3: Designing the Network Topology

A common strategy for network design is to take a *top-down approach*. In this approach, the network applications and service requirements are identified, and then the network is designed to support them.

When the design is complete, a prototype or proof-of-concept test is performed. This approach ensures that the new design functions as expected before it is implemented.

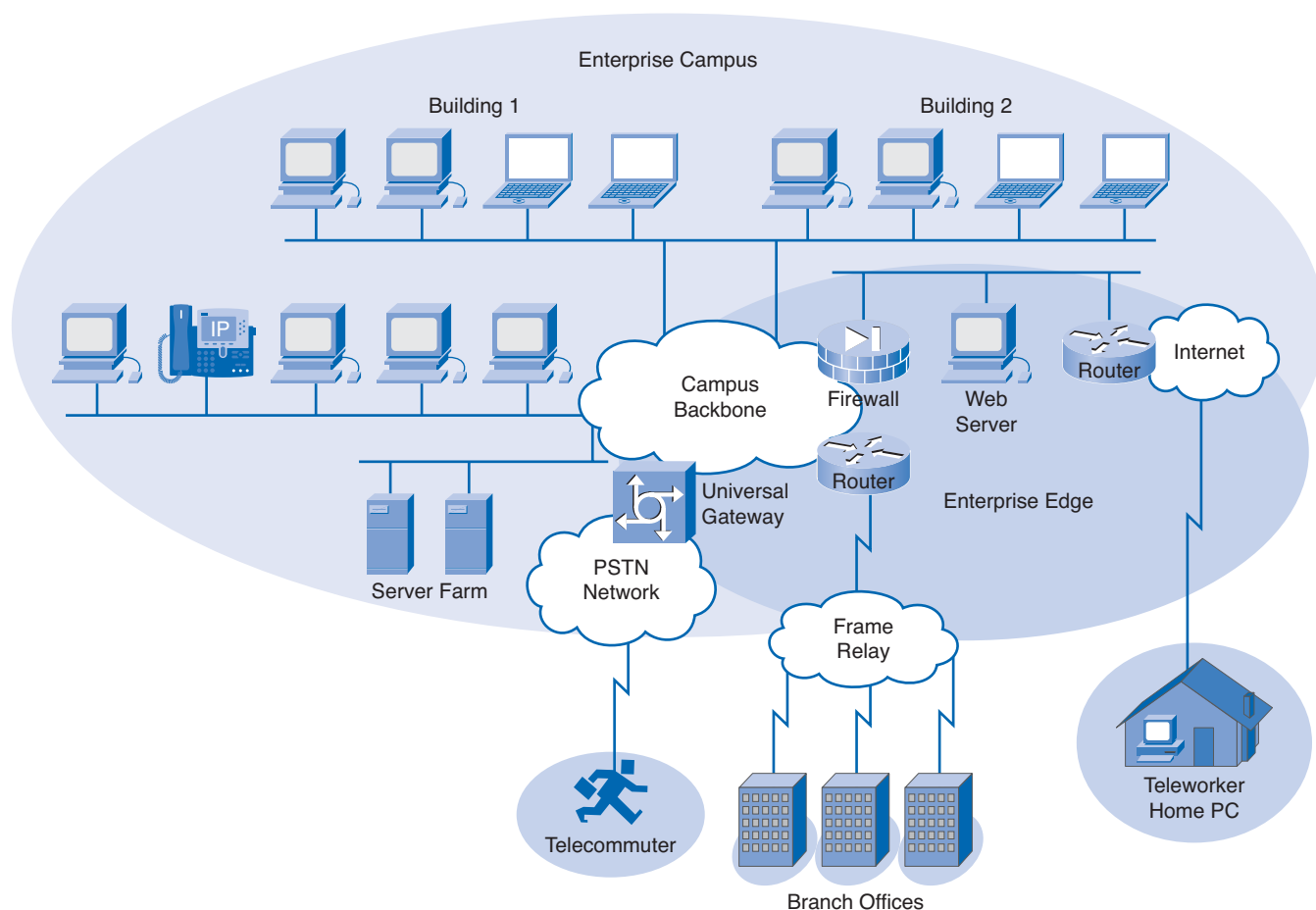
Figure 1-5 Client Interaction



A common mistake made by network designers is the failure to correctly determine the scope of the network design project.

Determining the Scope of the Project

While gathering requirements, the designer identifies the issues that affect the entire network and those that affect only specific portions. By creating a topology similar to Figure 1-6, the designer can isolate areas of concern and identify the scope of the project. Failure to understand the impact of a particular requirement often causes a project scope to expand beyond the original estimate. This oversight can greatly increase the cost and time required to implement the new design.

Figure 1-6 Enterprise Campus

Impacting the Entire Network

Network requirements that impact the entire network include the following:

- Adding new network applications and making major changes to existing applications, such as database or Domain Name System (DNS) structure changes
- Improving the efficiency of network addressing or routing protocol changes
- Integrating new security measures
- Adding new network services, such as voice traffic, *content networking*, and *storage networking*
- Relocating servers to a data center server farm

Impacting a Portion of the Network

Requirements that may only affect a portion of the network include the following:

- Improving Internet connectivity and adding bandwidth
- Updating access layer LAN cabling
- Providing redundancy for key services
- Supporting wireless access in defined areas
- Upgrading WAN bandwidth



Interactive Activity 1-2: Determining the Project Scope (1.1.3)

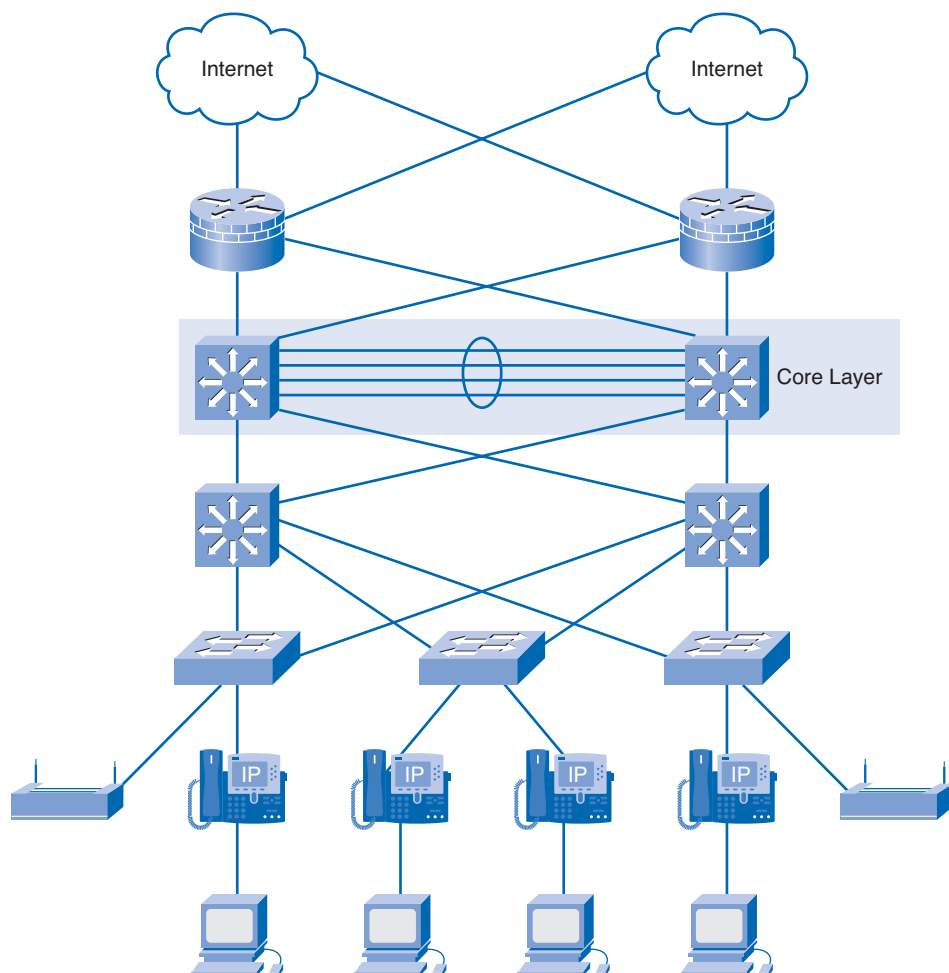
In this interactive activity, you determine whether each of the requirements affects the entire network or only a portion of the network. Use file ia-113 on the CD-ROM that accompanies this book to perform this interactive activity.

Investigating Core Layer Design Considerations

The Cisco three-layer hierarchical model is composed of the core layer, distribution layer, and access layer. Of the three layers, the core layer is responsible for transporting large amounts of data quickly and reliably. The designer must ensure that the core layer is designed with fault tolerance, especially because all users in the network can be affected by a failure. The ability to avoid unnecessary delays in network traffic quickly becomes a top priority for the network designer.

What Happens at the Core Layer?

The core layer is sometimes called the *network backbone*. Routers and switches at the core layer provide high-speed connectivity. In an enterprise LAN, the core layer, shown in Figure 1-7, may connect multiple buildings or multiple sites, and may provide connectivity to the server farm. The core layer includes one or more links to the devices at the enterprise edge to support Internet, *virtual private networks (VPN)*, *extranet*, and WAN access.

Figure 1-7 Core Layer

Implementing a core layer reduces the complexity of the network, making it easier to manage and troubleshoot.

Goals of the Core Layer

The core layer design enables the efficient, high-speed transfer of data between one section of the network and another. The primary design goals at the core layer are as follows:

- Provide 100% uptime.
- Maximize throughput.
- Facilitate network growth.

Core Layer Technologies

Technologies used at the core layer include the following:

- Routers or *multilayer switches* that combine routing and switching in the same device
- Redundancy and *load balancing*
- High-speed and aggregate links
- Routing protocols that scale well and converge quickly, such as *Enhanced Interior Gateway Routing Protocol (EIGRP)* and *Open Shortest Path First (OSPF) Protocol*

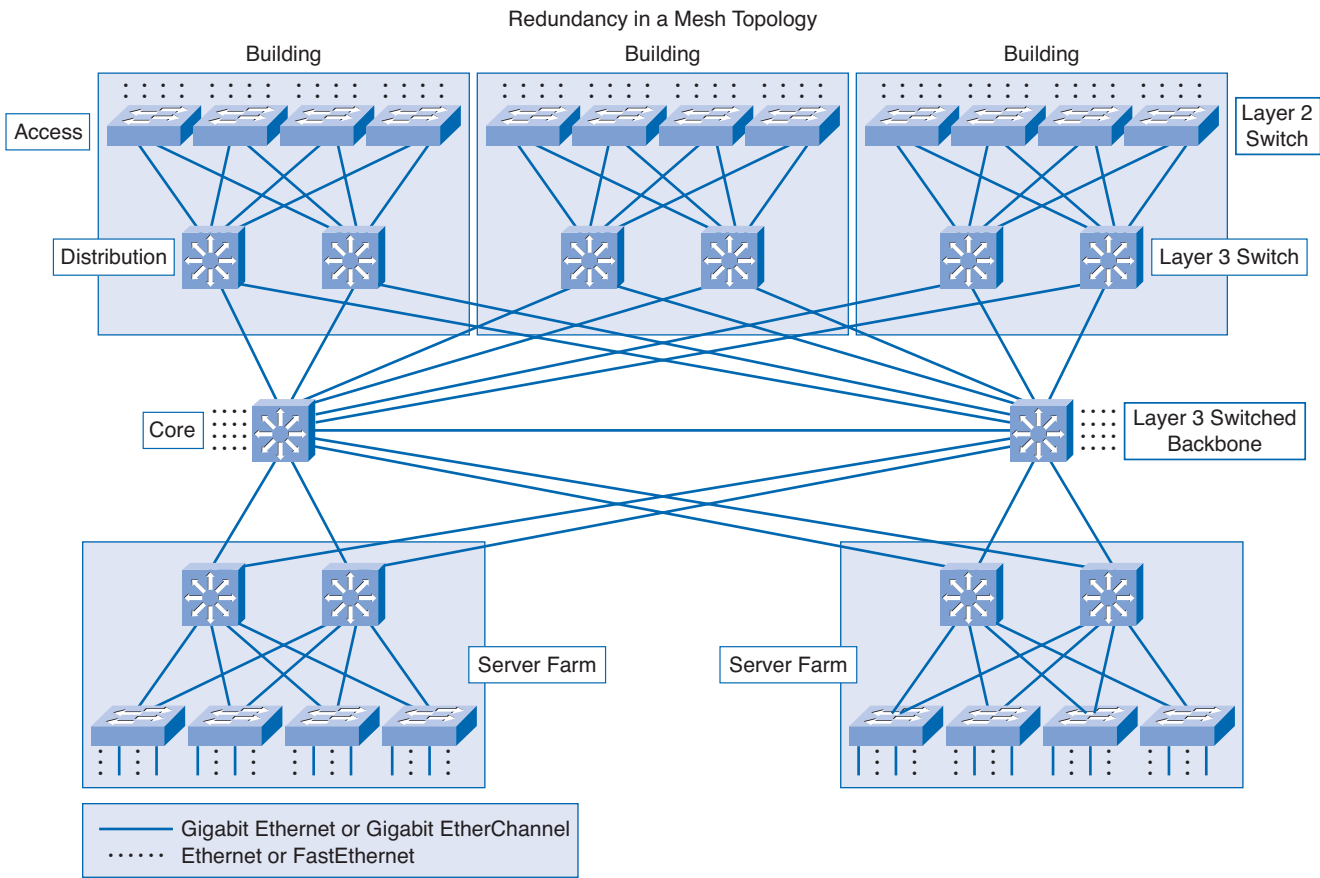
Redundant Links

Implementing redundant links at the core layer ensures that network devices can find alternate paths to send data in the event of a failure. When Layer 3 devices are placed at the core layer, these redundant links can be used for load balancing in addition to providing backup. In a flat, Layer 2 network design, *Spanning Tree Protocol (STP)* disables redundant links unless a primary link fails. This STP behavior prevents load balancing over the redundant links.

Mesh Topology

Most core layers in a network are wired in either a *full-mesh* or *partial-mesh* topology. A full-mesh topology is one in which every device has a connection to every other device (see Figure 1-8). Although full-mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly. For larger installations, a modified partial-mesh topology is used. In a partial-mesh topology, each device is connected to at least two others, creating sufficient redundancy without the complexity of a full mesh.

Figure 1-8 Redundancy in a Mesh Topology



Packet Tracer
Activity

Comparing Mesh Topologies (1.2.1)

In this activity, you create and compare full-mesh and partial-mesh topologies between routers. Use file d4-121.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Network Traffic Prioritization

Failures at the core layer can potentially affect all users of the network. Therefore, preventing failures becomes a daunting task. The network designer has to incorporate features or additions to the design to minimize or eliminate the effects of a core layer failure. The users on a network do not want to wait to complete their daily tasks because of a lack of care in the design.

Preventing Failures

The network designer must strive to provide a network that is resistant to failures and that can recover quickly in the event of a failure. Core routers and switches can contain the following:

- Dual power supplies and fans
- A modular chassis-based design
- Additional management modules

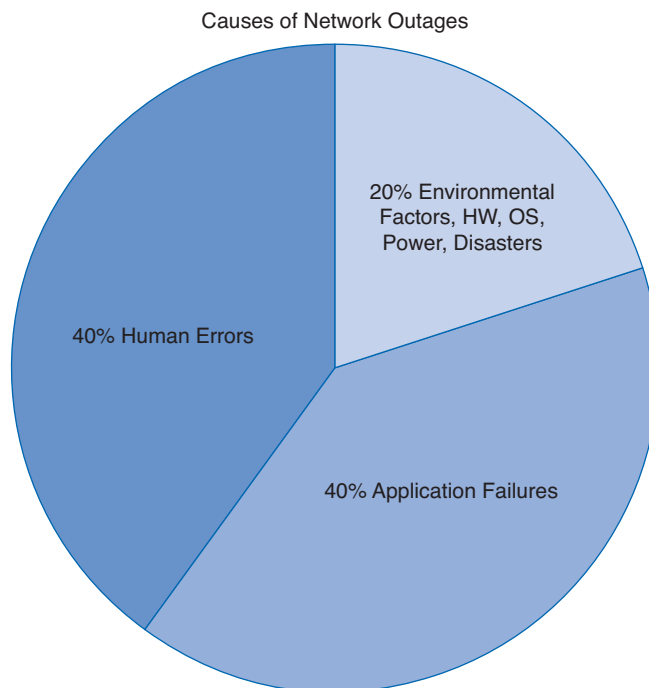
Redundant components increase the cost, but they are usually well worth the investment. Core layer devices should have *hot-swappable* components whenever possible. Hot-swappable components can be installed or removed without first having to turn off the power to the device. Using these components reduces repair time and disruption to network services.

Larger enterprises often install generators and large *uninterruptible power supply (UPS)* devices. These devices prevent minor power outages from causing large-scale network failures.

Reducing Human Error

Human errors contribute to network failures. Unfortunately, the addition of redundant links and equipment cannot eliminate these factors. Many network failures are the result of poorly planned, untested updates or additions of new equipment. Never make a configuration change on a production network without first testing it in a lab environment! Figure 1-9 shows the percentages of common network outages.

Figure 1-9 Causes of Network Outages



Source: Gartner; Copyright © 2001

Failures at the core layer cause widespread outages. It is critical to have written policies and procedures in place to govern how changes are approved, tested, installed, and documented. Plan a back-out strategy to return the network to its previous state in case changes are not successful.

Network Convergence

The choice of a routing protocol for the core layer is determined by the size of the network and the number of redundant links or paths available. A major factor in choosing a protocol is how quickly it recovers from a link or device failure.

Convergence Definition and Factors

Network convergence occurs when all routers have complete and accurate information about the network. The faster the *convergence time*, the quicker a network can react to a change in topology.

Factors that affect convergence time include the following:

- The speed at which the routing updates reach all the routers in the network
- The time that it takes each router to perform the calculation to determine the best paths

Selecting a Routing Protocol for Acceptable Convergence Time

Most dynamic routing protocols offer acceptable convergence times in small networks. In larger networks, protocols such as Routing Information Protocol Version 2 (RIPv2) may converge too slowly to prevent disruption of network services if a link fails. Generally, in a large enterprise network, EIGRP or OSPF provide the most stable routing solution.

Design Considerations with Convergence in Mind

Most networks contain a combination of dynamic and static routes. Network designers need to consider the number of routes required to ensure that all destinations in the network are reachable. Large routing tables can take significant time to converge. The design of network addressing and summarization strategies in all layers affects how well the routing protocol can react to a failure.

Packet Tracer
☐ **Activity**

Observing Network Convergence (1.2.3)

In this activity, you use the existing topology and add a new LAN segment to observe network convergence. Use file d4-123.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Investigating Distribution Layer Design Considerations

The next layer of the Cisco hierarchical model is the distribution layer. This layer is associated with routing, filtering, and is the communication point between the core layer and the access layer. A network designer must create a distribution layer design that complements the needs of the other two layers.

What Happens at the Distribution Layer?

The distribution layer represents a routing boundary between the access layer and the core layer. It also serves as a connection point between remote sites and the core layer.

Distribution Layer Routing

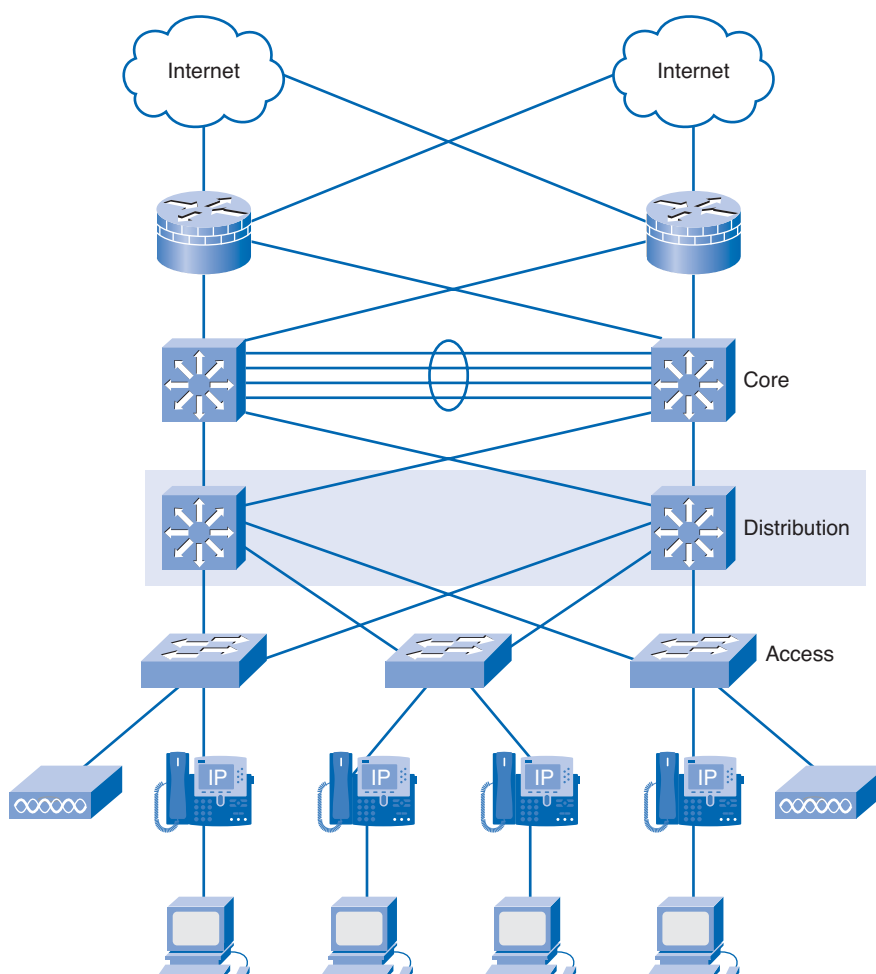
The access layer is commonly built using Layer 2 switching technology. The distribution layer (see Figure 1-10) is built using Layer 3 devices. Routers or multilayer switches, located at the distribution layer, provide many functions critical for meeting the goals of the network design, including the following:

- Filtering and managing traffic flows
- Enforcing access control policies

- Summarizing routes before advertising the routes to the Core
- Isolating the core from access layer failures or disruptions
- Routing between access layer VLANs

Distribution layer devices are also used to manage queues and prioritize traffic before transmission through the campus core.

Figure 1-10 Distribution Layer



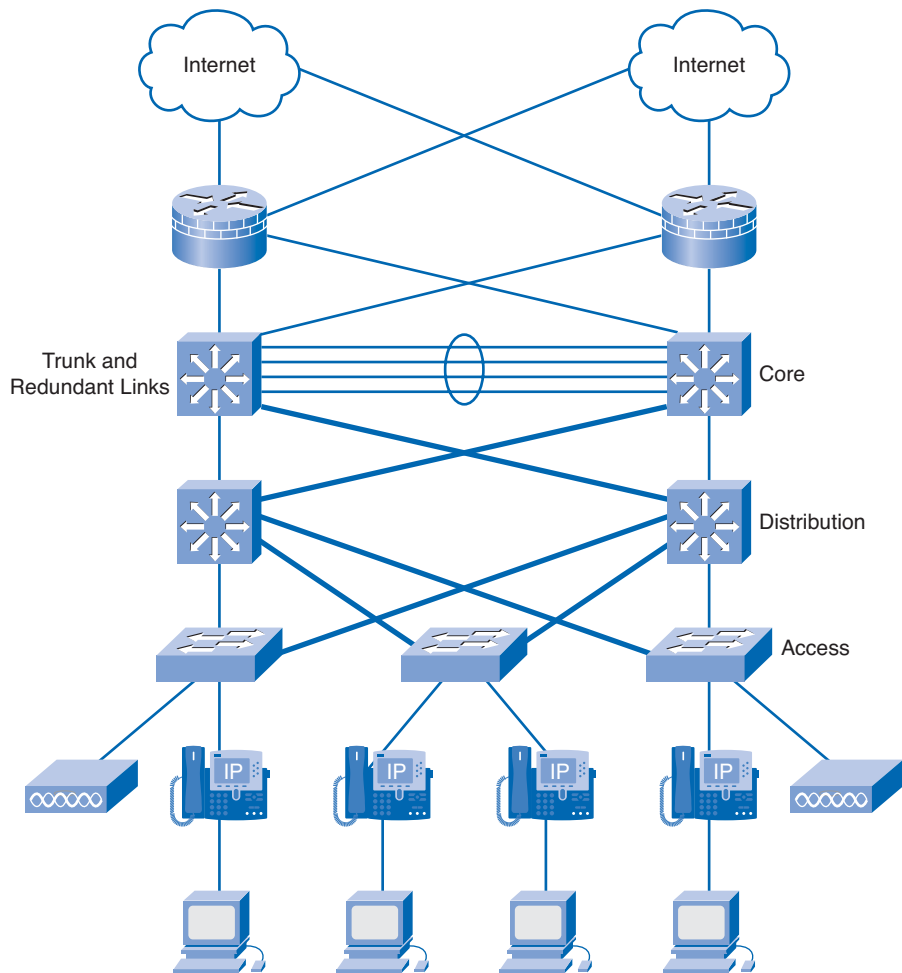
Trunks

Trunk links are often configured between access and distribution layer networking devices. Trunks are used to carry traffic that belongs to multiple VLANs between devices over the same link. The network designer considers the overall VLAN strategy and network traffic patterns when designing the trunk links.

Redundant Links

When redundant links exist between devices in the distribution layer, the devices can be configured to load balance the traffic across the links. Figure 1-11 shows the redundant links at the distribution layer. Load balancing is another option that increases the bandwidth available for applications.

Figure 1-11 Redundancy at the Distribution Layer



Distribution Layer Topology

Distribution layer networks are usually wired in a partial-mesh topology. This topology provides enough redundant paths to ensure that the network can survive a link or device failure. When the distribution layer devices are located in the same wiring closet or data center, they are interconnected using gigabit links. When the devices are separated by longer distances, fiber cable is used. Switches that support multiple high-speed fiber connections can be expensive, so careful planning is necessary to ensure that enough fiber ports are available to provide the desired bandwidth and redundancy.

Packet Tracer

Activity

Demonstrating Distribution Layer Functions (1.3.1)

In this activity, you demonstrate the functions performed by the distribution layer devices. Use file d4-131 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

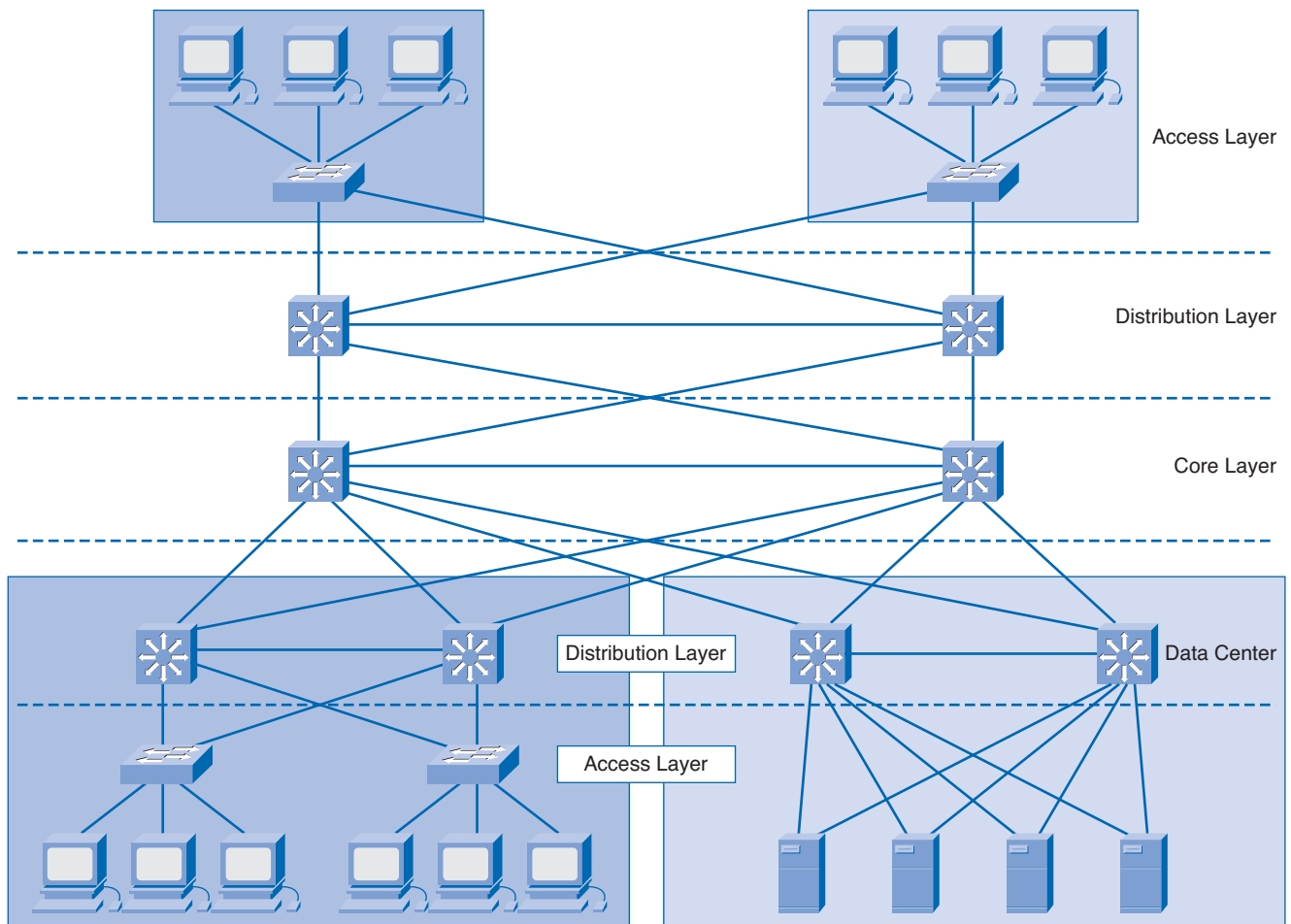
Limiting the Scope of Network Failure

A failure domain defines the portion of the network affected when either a device or network application fails.

Limiting the Size of Failure Domains

Because failures at the core layer of a network have a large impact, the network designer often concentrates on efforts to prevent failures. These efforts can greatly increase the cost to implement the network. In the hierarchical design model, it is easiest and usually least expensive to control the size of a failure domain in the distribution layer. In the distribution layer, network errors can be contained to a smaller area, thus affecting fewer users. When using Layer 3 devices at the distribution layer, every router functions as a gateway for a limited number of access layer users. Figure 1-12 shows the manner in which redundant cabling and devices can be configured to limit the effects of a link or device failure.

Figure 1-12 Protection Against Single Device Failures



Switch Block Deployment

Routers, or multilayer switches, are usually deployed in pairs, with access layer switches evenly divided between them. This configuration is referred to as a building or departmental switch block. Each **switch block** acts independently of the others. As a result, the failure of a single device does not cause the network to go down. Even the failure of an entire switch block does not impact a significant number of end users.

Packet Tracer
Activity
Investigating Failure Domains (1.3.2)

In this activity, you turn off the devices and disable interfaces to see the resulting network failures. Use file d4-132.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Building a Redundant Network at the Distribution Layer

To reduce downtime, the network designer deploys redundancy in the network.

Devices at the distribution layer have redundant connections to switches at the access layer and to devices at the core layer. If a link or device fails, these connections provide alternate paths. Using an appropriate routing protocol at the distribution layer, the Layer 3 devices react quickly to link failures so that they do not impact network operations.

Providing multiple connections to Layer 2 switches can cause unstable behavior in a network unless STP is enabled. Without STP (see Figure 1-13), redundant links in a Layer 2 network can cause broadcast storms. Switches are unable to correctly learn the ports, so traffic ends up being flooded throughout the switch. By disabling one of the links, STP guarantees that only one path is active between two devices (see Figure 1-14). If one of the links fails, the switch recalculates the spanning-tree topology and automatically begins using the alternate link.

Rapid Spanning Tree Protocol (RSTP), as defined in IEEE 802.1w, builds upon the IEEE 802.1d technology and provides rapid convergence of the spanning tree.

Figure 1-13 Traffic Patterns Without STP

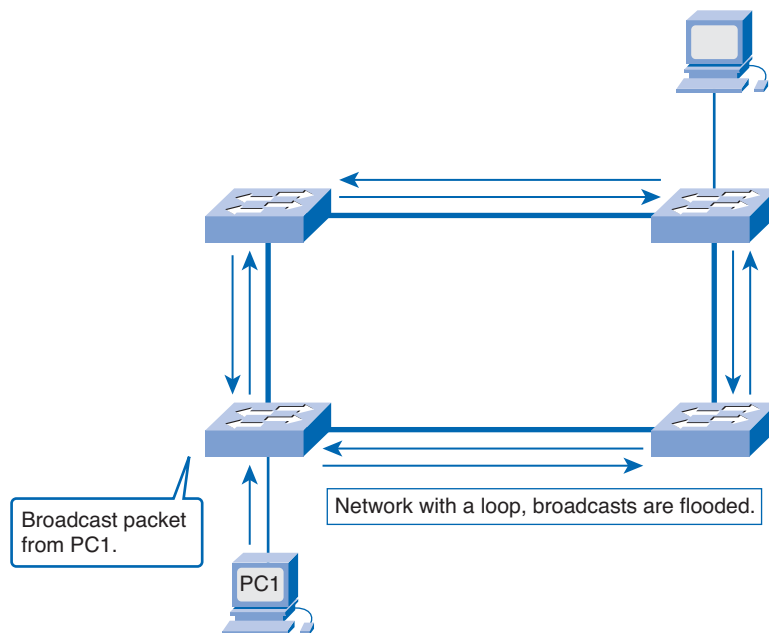
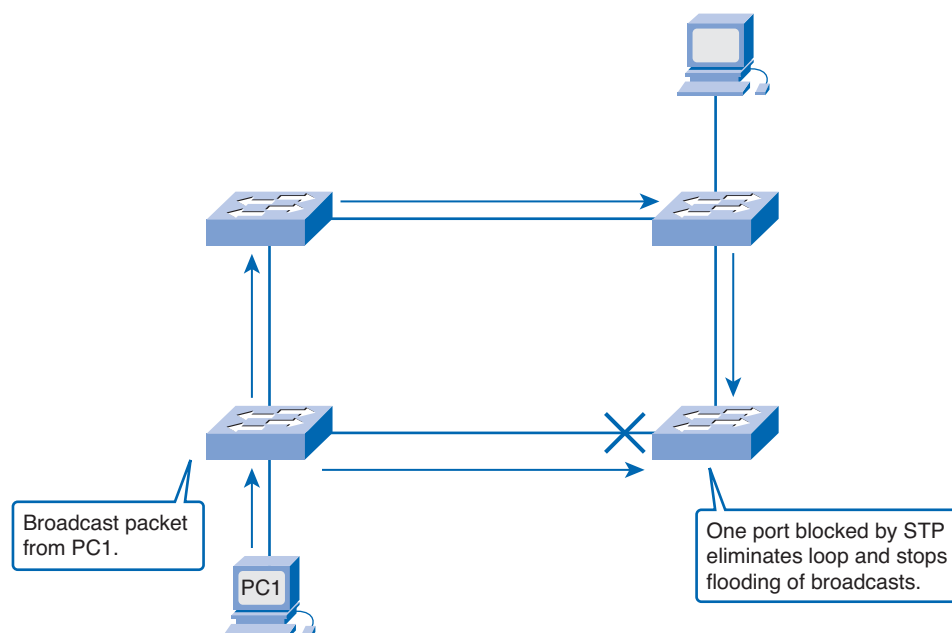


Figure 1-14 Traffic Patterns with STP

Consider the case in which a high-volume, enterprise server is connected to a switch port. If that port recalculates because of STP, the server is down for 50 seconds. It would be difficult to imagine the number of transactions lost during that timeframe.

In a stable network, STP recalculations are infrequent. In an unstable network, it is important to check the switches for stability and configuration changes. One of the most common causes of frequent STP recalculations is a faulty power supply or power feed to a switch. A faulty power supply causes the device to reboot unexpectedly.

Traffic Filtering at the Distribution Layer

Access control lists (ACL) are a tool that can be used at the distribution layer to limit access and to prevent unwanted traffic from entering the core network. An ACL is a list of conditions used to test network traffic that attempts to travel through a router interface. ACL statements identify which packets to accept or which to deny.

Filtering Network Traffic

To filter network traffic, the router examines each packet and then either forwards or discards it, based on the conditions specified in the ACL. There are different types of ACLs for different purposes. Standard ACLs filter traffic based on the source address. Extended ACLs can filter based on multiple criteria, including the following:

- Source address
- Destination address
- Protocols
- Port numbers or applications
- Whether the packet is part of an established TCP stream

Both standard and extended ACLs can be configured as either numbered or named access lists.

Complex ACLs

Standard and extended ACLs serve as the basis for other, more complex types of ACLs. With Cisco IOS Software, you can configure three complex ACL features:

- **Dynamic ACL:** Requires a user to use telnet to connect to the router and authenticate. Once authenticated, traffic from the user is permitted. Dynamic ACLs are sometimes referred to as “lock and key” because the user is required to log in to obtain access.
- **Reflexive ACL:** Allows outbound traffic and then limits inbound traffic to only responses to those permitted requests. This is similar to the established keyword used in extended ACL statements, except that these ACLs can also inspect User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) traffic, in addition to TCP.
- **Time-based ACL:** Permits and denies specified traffic based on the time of day or day of the week.

Placing ACLs

Traffic that travels into an interface is filtered by the inbound ACL. Traffic going out of an interface is filtered by the outbound ACL. The network designer must decide where to place ACLs within the network to achieve the desired results.

It is important to remember the following rules for designing and applying ACLs:

- There can be one ACL per protocol per direction per interface.
- Standard ACLs should be applied closest to the destination.
- Extended ACLs should be applied closest to the source.
- The inbound or outbound interface should be referenced as if looking at the port from inside the router.
- Statements are processed sequentially from the top of the list to the bottom until a match is found. If no match is found, the packet is denied and discarded.
- There is an implicit “deny any” at the end of all ACLs. This statement does not appear in the configuration listing.
- The network administrator should configure ACL entries in an order that filters from specific to general. Specific hosts should be denied first, and groups or general filters should come last.
- The match condition is examined first. The “permit” or “deny” is examined only if the match is true.
- Never work with an ACL that is actively applied.
- Use a text editor to create comments that outline the logic. Then fill in the statements that perform the logic.
- The default behavior is that new lines are always added to the end of the ACL. A **no access-list x** command removes the whole list.
- An IP access control list sends an ICMP host unreachable message to the sender of the rejected packet and discards the packet in the bit bucket.
- An ACL should be removed carefully. Removing an access list immediately stops the filtering process.
- Outbound filters do not affect traffic that originates from the local router.

By following these simple rules, an administrator can ensure the proper functioning of an ACL.



Interactive Activity 1-3: Match ACLs to the Appropriate Statements (1.3.4)

In this interactive activity, you determine which ACL has been applied to the correct statement. Use file ia-134 on the CD-ROM that accompanies this book to perform this interactive activity.



Placing ACLs (1.3.4)

In this activity, you place the ACLs onto the appropriate interface in the topology. Use file d4-134.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.



Lab 1-1: Creating an ACL (1.3.4)

In this lab, you create an ACL to meet the conditions specified in the lab. Refer to the hands-on lab in Part II of this Learning Guide. You may perform this lab now or wait until the end of the chapter.

Routing Protocols at the Distribution Layer (1.3.5)

Another important function that occurs at the distribution layer is route summarization, also called route aggregation or supernetting.

Route Summarization

Route summarization has several advantages for the network, such as the following:

- One route in the routing table that represents many other routes, creating smaller routing tables
- Less routing update traffic on the network
- Lower overhead on the router

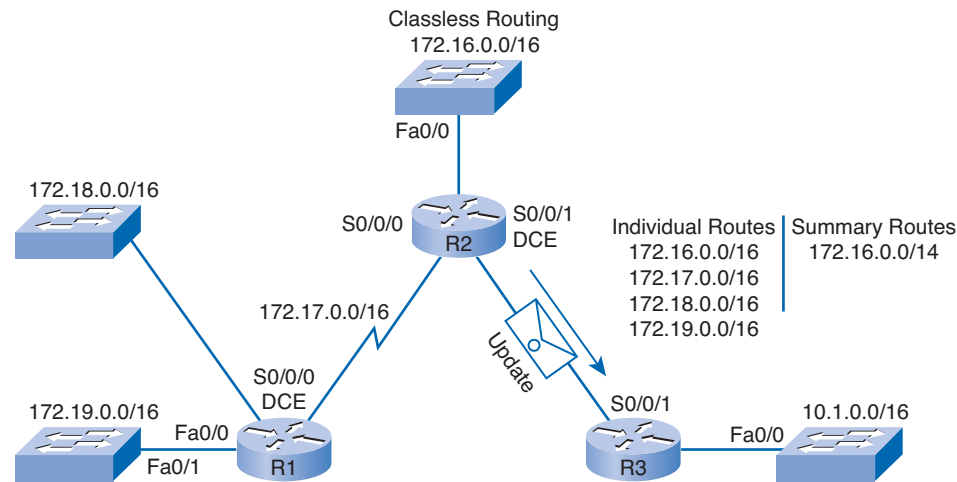
Summarization can be performed manually or automatically, depending on which routing protocols are used in the network.

Classless routing protocols such as RIPv2, EIGRP, OSPF, and *Intermediate System-to-Intermediate System (IS-IS) Protocol* support route summarization based on subnet addresses on any boundary.

Classful routing protocols such as RIPv1 automatically summarize routes on the classful network boundary, but do not support summarization on any other boundaries.

Figure 1-15 shows information on individual and summarized routes.

Figure 1-15 Individual and Summarized Routes



Interactive Activity 1-4: Identify Summary Routes (1.3.5)

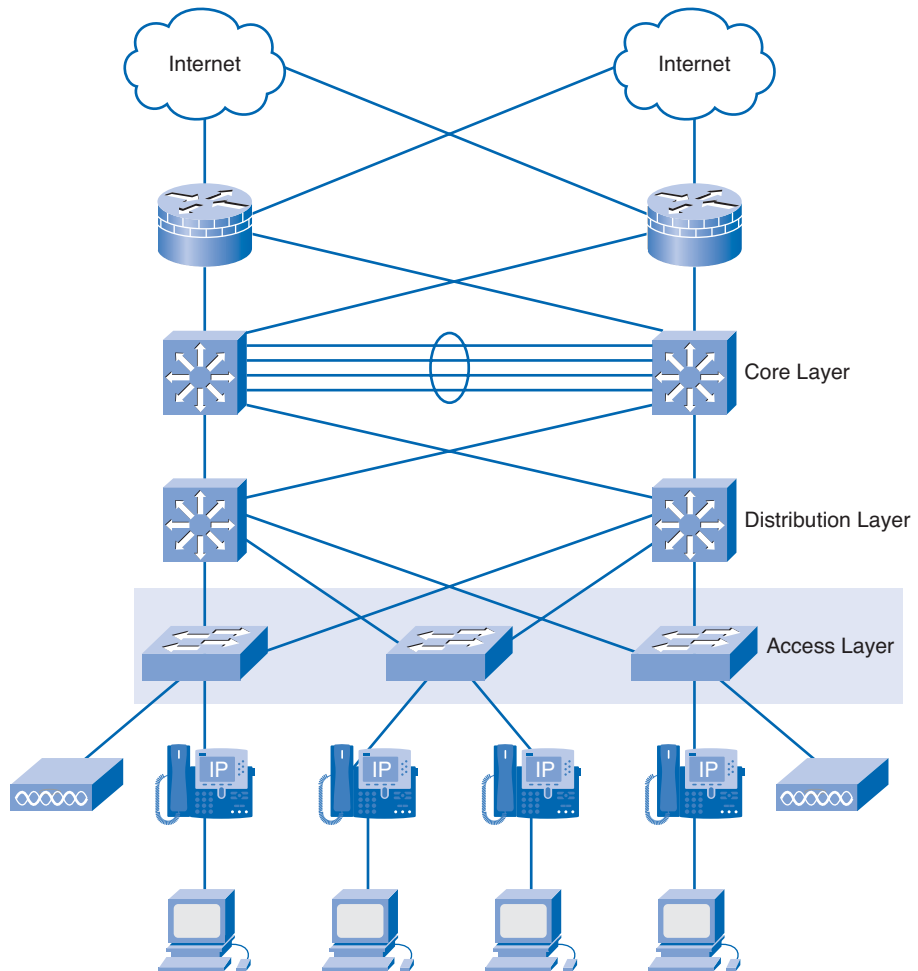
In this interactive activity, you select the appropriate summary route from the distribution router to the core in a given topology. Use file ia-135 on the CD-ROM that accompanies this book to perform this interactive activity.

Investigating Access Layer Design Considerations

The access layer is used to control user access to the internetwork resources. The network designer has to facilitate the traffic generated from the access layer as it is bound for other segments or other layers within the network. Without an appropriate design, the access layer could quickly become inundated with traffic, resulting in less-than-acceptable performance for the end users.

What Happens at the Access Layer?

The access layer, as illustrated in Figure 1-16, represents the edge of the network where end devices connect. Access layer services and devices reside inside each building of a campus, each remote site and server farm, and at the enterprise edge.

Figure 1-16 Access Layer

Access Layer Physical Considerations

The access layer of the campus infrastructure uses Layer 2 switching technology to provide access into the network. The access can be either through a permanent wired infrastructure or through wireless access points. Ethernet over copper wiring poses distance limitations. Therefore, one of the primary concerns when designing the access layer of a campus infrastructure is the physical location of the equipment.

Wiring Closets

Wiring closets can be actual closets or small telecommunication rooms that act as the termination point for infrastructure cabling within buildings or within floors of a building. The placement and physical size of the wiring closets depends on network size and expansion plans.

The wiring closet equipment provides power to end devices such as IP phones and wireless access points. Many access layer switches have *Power-over-Ethernet (PoE)* functionality.

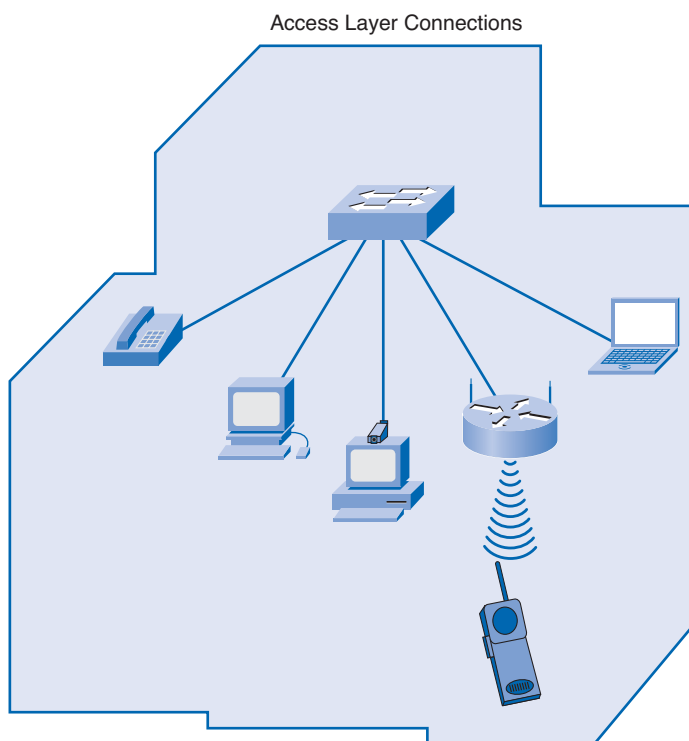
Unlike a typical wiring closet, inside a server farm or data center the access layer devices are typically redundant multilayer switches that combine the functionality of both routing and switching. Multilayer switches can provide firewall and intrusion protection features and Layer 3 functions.

The Impact of Converged Networking at the Access Layer

The modern computer network consists of more than just personal computers and printers connecting to the access layer. Many different devices, as shown in Figure 1-17, can connect to an IP network, including the following:

- IP telephones
- Video cameras
- Videoconferencing systems

Figure 1-17 Access Layer Connections



All of these services can be converged onto a single physical access layer infrastructure. However, the logical network design to support them becomes more complex because of considerations such as quality of service (QoS), traffic segregation, and filtering. These new types of end devices, and the associated applications and services, change the requirements for scalability, availability, security, and manageability at the access layer.

The Need for Availability at the Access Layer

In early networks, high availability was usually present only at the network core, enterprise edge, and data center networks. With IP telephony, there is now an expectation that every individual telephone should be available 100 percent of the time.

Redundant components and *failover* strategies can be implemented at the access layer to improve reliability and increase availability for the end devices.

Access Layer Management

Improving the manageability of the access layer is a major concern for the network designer. Access layer management is crucial because of the following:

- The increase in the number and types of devices connecting at the access layer
- The introduction of wireless access points into the LAN

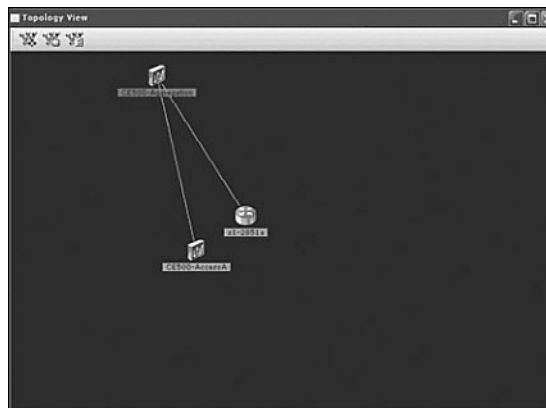
Designing for Manageability

In addition to providing basic connectivity at the access layer, the designer needs to consider the following:

- Naming structures
- VLAN architecture
- Traffic patterns
- Prioritization strategies

Configuring and using network management systems for a large converged network are very important. Figure 1-18 shows an example of network management software. It is also important to standardize configurations and equipment when possible.

Figure 1-18 Network Management Software: Cisco Assistant



Following good design principles improves the manageability and ongoing support of the network by

- Ensuring that the network does not become too complex
- Allowing easy troubleshooting when a problem occurs
- Making it easier to add new features and services in the future

Packet Tracer Activity

Exploring Access Layer Functions (1.4.1)

In this activity, you explore different access layer functions. Use file d4-141.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Network Topologies at the Access Layer

Most recent Ethernet networks use a star topology, which is sometimes called a hub-and-spoke topology. In a star topology, each end device has a direct connection to a single networking device. This single networking device is usually a Layer 2 or multilayer switch. A wired star topology in the access layer typically has no redundancy from individual end devices to the switch. For many businesses, the cost of additional wiring to create redundancy is usually too high. However, if costs are not a factor, the network can be configured as a full-mesh topology (see Figure 1-19) to ensure redundancy.

Figure 1-19 Star and Full-Meshed Topologies

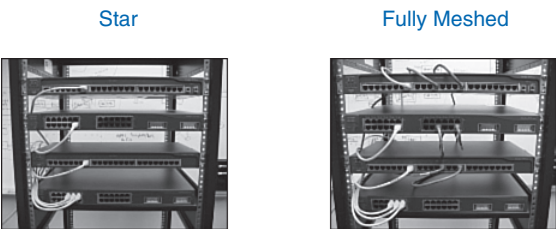


Table 1-1 documents the advantages, disadvantages, and wiring of a star topology.

Table 1-1 Star Topology Advantages, Disadvantages, and Wiring

Advantages	Disadvantages	Ethernet Wiring
Easy installation	The central device represents a single point of failure.	Twisted-pair wiring to connect to the individual end devices.
Minimal configuration	The capabilities of the central device can limit overall performance for access to the network. The topology does not recover in the event of a failure when there are no redundant links.	Fiber to interconnect the access switches to the distribution layer devices.

Packet Tracer
Activity

Creating Topologies (1.4.2)

In this activity, you create an access layer star topology. Use file d4-142.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

How VLANs Segregate and Control Network Traffic

Using VLANs and IP subnets is the most common method for segregating user groups and traffic within the access layer network.

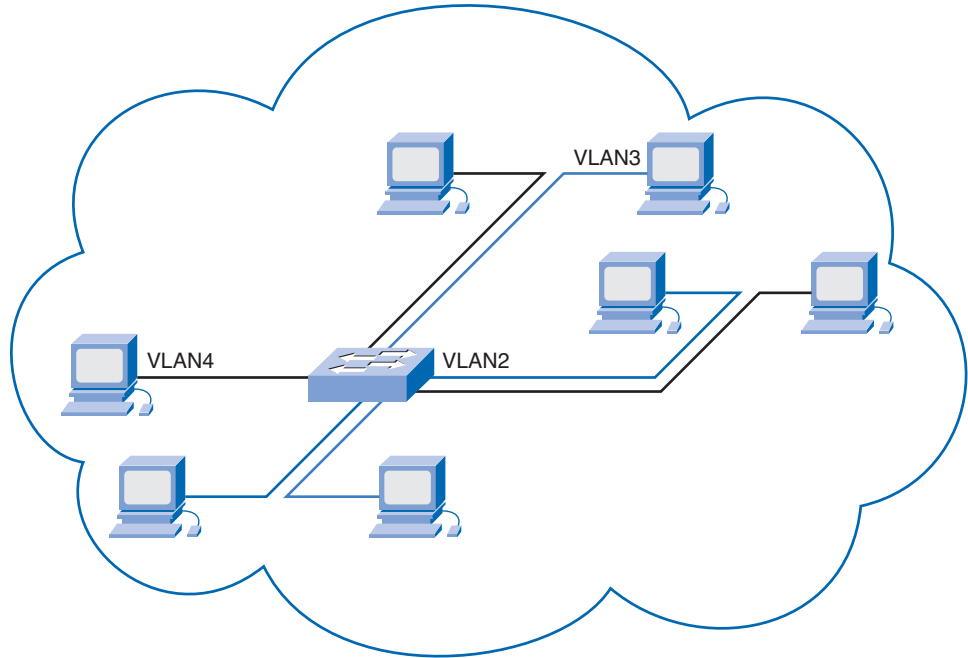
VLANs in the Past

With the introduction of Layer 2 switching, VLANs were used to create end-to-end workgroup networks. The networks connected across buildings or even across the entire infrastructure. End-to-end VLANs are no longer used in this way. The increased number of users and the volume of network traffic that these users generate are too high to be supported.

VLANs Now

Today, VLANs are used to separate and classify traffic streams and to control broadcast traffic within a single wiring closet or building. Figure 1-20 shows VLANs segregating traffic within a network. Although large VLANs that span entire networks are no longer recommended, they may be required to support special applications, such as wireless roaming and wireless IP phones.

Figure 1-20 Segregating VLAN Traffic



The recommended approach is to contain VLANs within a single wiring closet. This approach increases the number of VLANs in a network, which also increases the number of individual IP subnets. It is recommended practice to associate a single IP subnet with a single VLAN. IP addressing at the access layer becomes a critical design issue that affects the scalability of the entire network.



Lab 1-2: Monitoring VLAN Traffic (1.4.3)

In this lab, you monitor various traffic types as it passes through a VLAN. Refer to the hands-on lab in Part II of this Learning Guide. You may perform this lab now or wait until the end of the chapter.

Services at the Network Edge

When creating possible solutions for a client, network designers must consider which services the network will provide, how many users the network will have, and which applications are to be implemented or used. It is expected that the hardware will have the ability to facilitate the demand placed on the network. Realistically, the hardware might be unable to support large quantities of traffic without having another method for prioritizing the traffic being transmitted. The network designer has to design the QoS mechanisms as a complement to the hardware.

Providing QoS to Network Applications

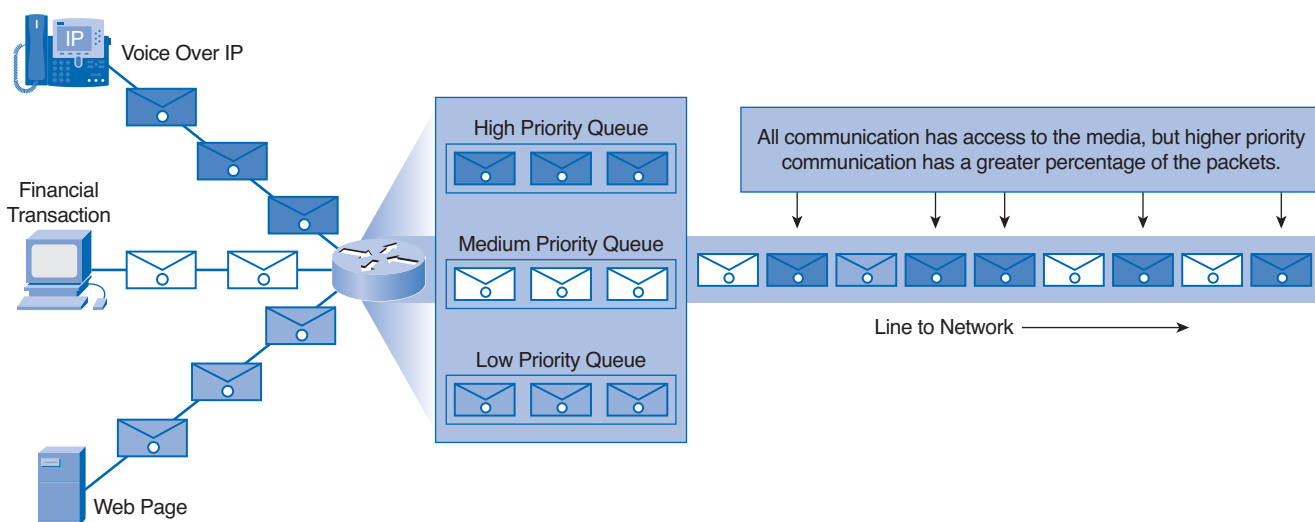
Networks must provide secure, predictable, measurable, and at times, guaranteed services. Networks also need mechanisms to control congestion when traffic increases. Congestion is caused when the demand on the network resources exceeds the available capacity.

All networks have limited resources. For this reason, networks need QoS mechanisms. The ability to provide QoS depends on traffic classification and the assigned priority.

Classification

Before designing QoS strategies, it is necessary to classify applications based on specific delivery requirements. Figure 1-21 shows priority queues used for QoS. Classifying data at or near the source enables the data to be assigned the appropriate priority as it moves through the entire network. Segregating traffic with similar characteristics into classes, and then marking that traffic, is a function of the network devices at the access and distribution layers. An example of this strategy is to place the voice traffic on an access switch into a single VLAN. The device then marks the traffic originating from the voice VLAN with the highest priority.

Figure 1-21 Marking and Prioritizing Traffic



Security at the Network Edge

Many of the security risks that occur at the access layer of the network result from poorly secured end devices. User error and carelessness account for a significant number of network security breaches.

Three types of common security risks that occur at the access layer are as follows:

- Viruses
- Worms
- Trojan horses

Providing adequate security for end devices may not be in the scope of a network design project. Nevertheless, the designer needs to understand the network impact of a security incident, such as a worm or a Trojan, at an end device. The designer can then better determine which network security measures to put in place to limit the effects on the network.

Permitting network access to only known or authenticated devices limits the ability of intruders to enter the network. It is important to apply wireless security measures that follow recommended practices.

**Lab 1-3: Identifying Network Vulnerabilities (1.4.5)**

In this lab, you use the SANS site to identify Internet security threats. Refer to the hands-on lab in Part II of this Learning Guide. You may perform this lab now or wait until the end of the chapter.

Security Measures

The vulnerabilities previously identified show that, for the most part, a network is an extremely unsecure environment. Network designers must place security as a top priority in their designs. Antivirus software is one way to prevent an attack, but software cannot prevent physical breaches of the network or its applications. Consideration must be taken when designing any network to secure the facilities and hardware from unauthorized access.

Providing Physical Security

Physical security of a network is important. Most network intruders gain physical entry at the access layer. On some network devices, such as routers and switches, physical access can provide the opportunity to change passwords and obtain full access to devices.

Obvious measures, such as locking wiring closets and restricting access to networking devices, are often the most effective ways to prevent security breaches. In high-risk or easily accessible areas, it might be necessary to equip wiring closets with additional security, such as cameras or motion-detection devices and alarms. Figure 1-22 shows an area visibly marked to forbid unauthorized personnel from entering the area. Some devices, such as keypad locks, can record which codes are used to enter the secured areas.

Figure 1-22 Unauthorized Entry



Securing Access Layer Networking Devices

The measures listed here can provide additional security to networking devices at the access layer:

- Setting strong passwords
- Using Secure Shell (SSH) to administer devices
- Disabling unused ports

Switch port security and *network access control* can ensure that only known and trusted devices have access to the network.

Recommended Practice on Security

Security risks cannot be eliminated or prevented completely. Effective risk management and assessment can significantly minimize the existing security risks. When considering security measures, it is important to understand that no single product can make an organization secure. True network security comes from a combination of products, services, and procedures and a thorough *security policy* and a commitment to adhere to that policy.



Lab 1-4: Gaining Physical Access to the Network (1.4.6.2)

In this lab, you learn the risks associated with allowing physical access to the network by unauthorized persons. Refer to the hands-on lab in Part II of this Learning Guide. You may perform this lab now or wait until the end of the chapter.



Lab 1-5: Implementing Switch Port Security (1.4.6.3)

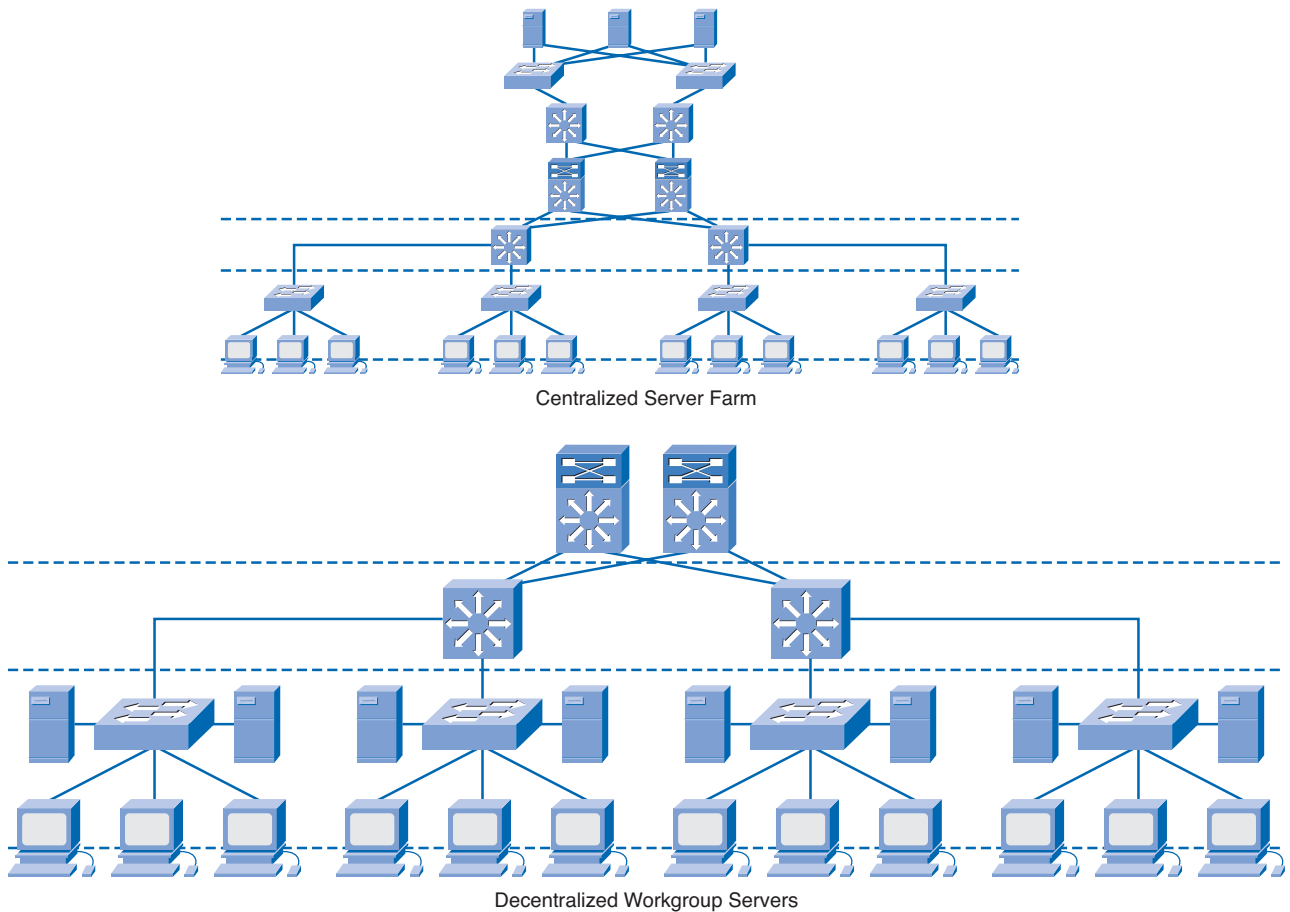
In this lab, you implement port security to prevent unauthorized users. Refer to the hands-on lab in Part II of this Learning Guide. You may perform this lab now or wait until the end of the chapter.

Investigating Server Farms and Security

Most enterprise networks provide users with Internet-accessible services, such as e-mail and e-commerce. The availability and security of these services are crucial to the success of a business.

What Is a Server Farm?

Managing and securing numerous distributed servers at various locations within a business network is difficult. Recommended practice centralizes servers in *server farms*. Server farms are typically located in computer rooms and *data centers*. Figure 1-23 shows the difference between centralized and decentralized server configurations.

Figure 1-23 Centralized and Decentralized Server Farms

Creating a server farm results in the following benefits:

- Network traffic enters and leaves the server farm at a defined point. This arrangement makes it easier to secure, filter, and prioritize traffic.
- Redundant, high-capacity links can be installed to the servers and between the server farm network and the main LAN. This configuration is more cost-effective than attempting to provide a similar level of connectivity to servers distributed throughout the network.
- Load balancing and failover can be provided between servers and between networking devices.
- The number of high-capacity switches and security devices is reduced, helping to lower the cost of providing services.

Packet Tracer
Activity

Observing and Recording Server Traffic (1.5.1)

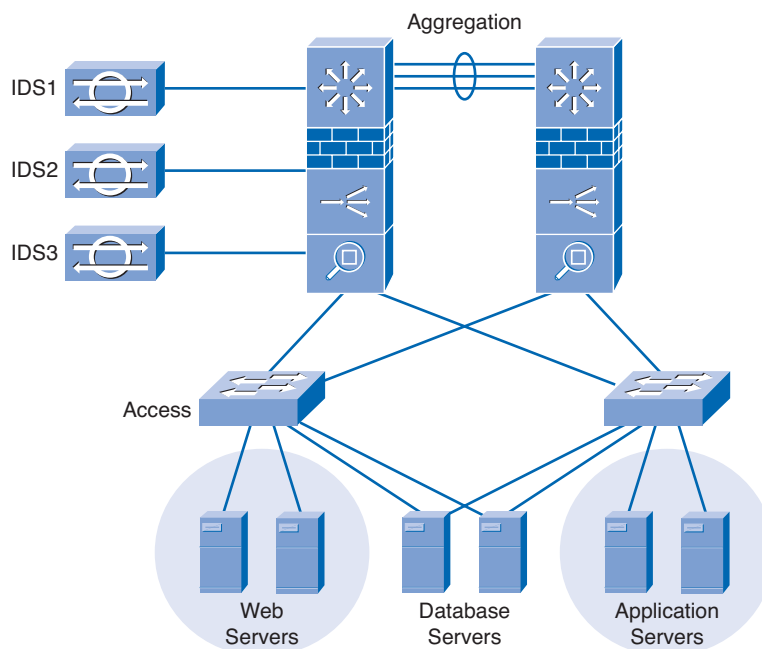
In this activity, you observe and record the way in which traffic moves to and from the servers on the network. Use file d4-151.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Security, Firewalls, and Demilitarized Zones

Data center servers can be the target of malicious attacks and must be protected.

Attacks against server farms can result in lost business for e-commerce and business-to-business applications and in information theft. Both LANs and *storage-area networks (SAN)* must be secured to reduce the chances of such attacks. Hackers use a variety of tools to inspect networks and to launch intrusion and *denial-of-service (DoS)* attacks. Figure 1-24 shows the devices and possible security solutions for a network.

Figure 1-24 Security Solutions



Protecting Server Farms Against Attack

Firewalls are often deployed to provide a basic level of security when internal and external users attempt to access the Internet via the server farm. To properly secure server farms, a more thorough approach must be followed. Such an approach takes advantage of the strengths of the following network products that can be deployed in a server farm:

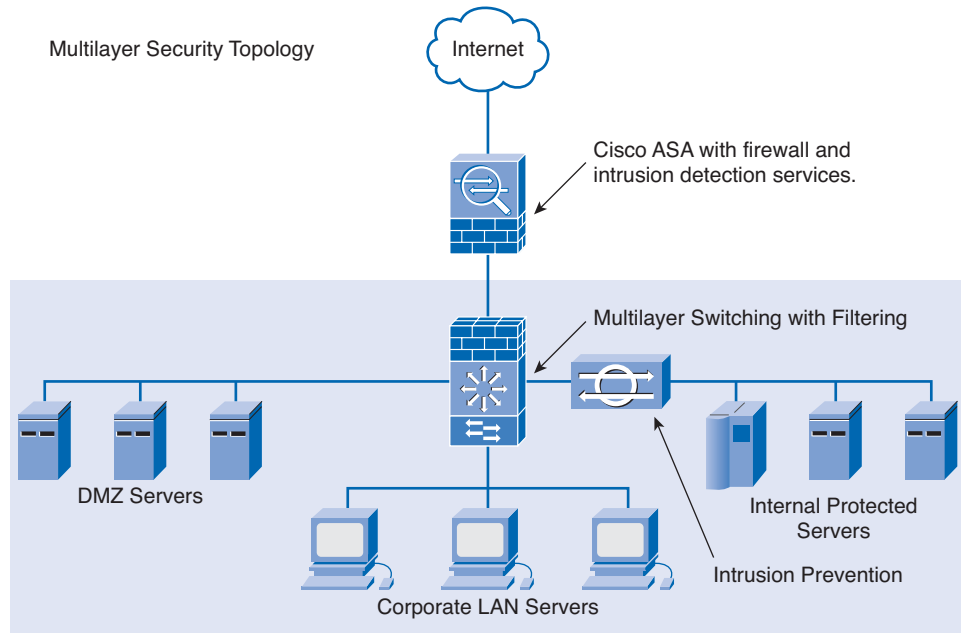
- Firewalls
- LAN switch security features
- Host-based and network-based intrusion detection and prevention systems
- Load balancers
- Network analysis and management devices

Although these devices and solutions are not all inclusive, they do go far in protecting the network from the adverse effects of possible intrusions.

Demilitarized Zones

In the traditional network firewall design, servers that needed to be accessed from external networks were located on a *demilitarized zone (DMZ)*. Users accessing these servers from the Internet or other untrusted external networks were prevented from seeing resources located on the internal LAN. LAN users were treated as trusted users and usually had few restrictions imposed when they accessed servers on the DMZ. Figure 1-25 shows a multilayer security topology. Designing a multilayer approach to security limits traffic and the potential for the entire network from being breached by an intrusion.

Figure 1-25 Multilayer Security



Protecting Against Internal Attacks

Today's networks are more likely to face an attack originating from the access layer of the internal network than from external sources. As a result, the design of server farm security is different from the older DMZ model. A layer of firewall features and intrusion protection is required between the servers and the internal networks, and between the servers and the external users. An additional security layer between the servers may also be required.

The sensitivity of data stored on the servers and contained in the transactions traveling the network determines the appropriate security policy for the design of the server farm.

High Availability

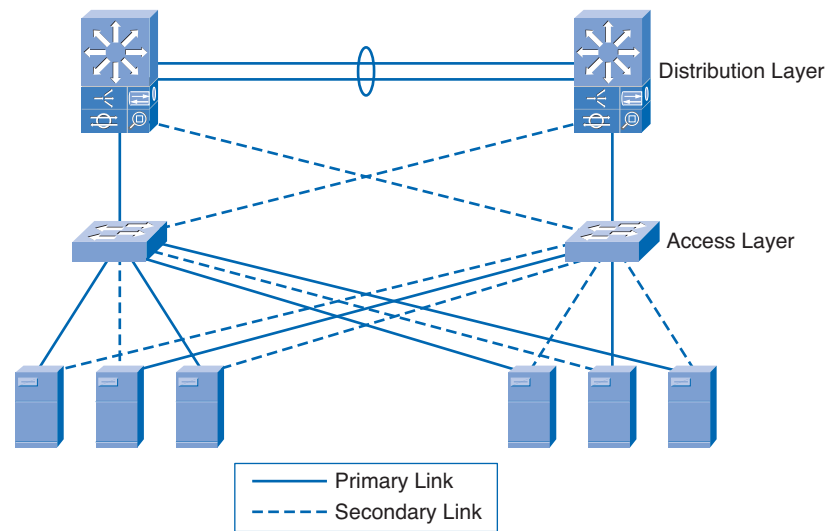
In addition to providing an extra layer of security, server farms are usually required to provide high availability for network applications and services. A highly available network is one that eliminates or reduces the potential impact of failures. This protection enables the network to meet requirements for access to applications, systems, and data from anywhere, at any time.

Building In Redundancy

To achieve high availability, servers are redundantly connected to two separate switches at the access layer. This redundancy provides a path from the server to the secondary switch if the primary switch fails (see Figure 1-26). Devices at the distribution and core layers of the server farm network are also

redundantly connected. Spanning-tree protocols, such as *Rapid Spanning Tree Protocol Plus (RSTP+)*, manage redundant Layer 2 links. Hot Standby Router Protocol (HSRP) and routing protocols provide support for Layer 3 redundancy and failover.

Figure 1-26 Network Redundancy



Virtualization

Many separate logical servers can be located on one physical server. The physical server uses an operating system specifically designed to support multiple virtual images. This feature is known as virtualization. This technology reduces the cost of providing redundant services, load balancing, and failover for critical network services.

Packet Tracer Activity

Using Redundant Links on Server Farm Devices (1.5.3)

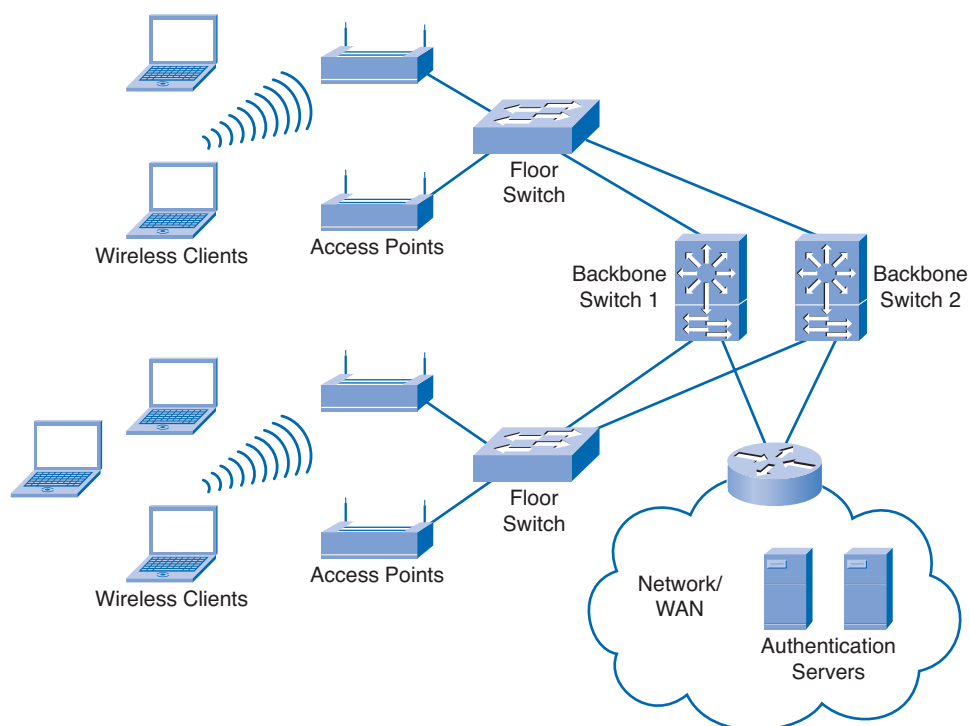
In this activity, you set up redundant switch links in a server farm and observe what happens when one device fails. Use file d4-153.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Investigating Wireless Network Considerations

Wireless networks are becoming more and more common. Coffee shops, bookstores, and public parks are adding wireless networking for their customers. The seamless integration of wireless does, however, pose a challenge to the network designer. Implementing wireless networking while maintaining functionality, manageability, and security of the wired network can introduce new issues that the designer must address.

Network Design Considerations Unique to WLANs

Before designing an indoor *wireless LAN (WLAN)* implementation, the network designer needs to fully understand how the customer intends to use the wireless network. Figure 1-27 shows a sample WLAN topology.

Figure 1-27 WLAN Topology

The designer learns about the network requirements by asking the customer questions. The answers to these questions affect how a wireless network is implemented. Examples of some of these questions include the following:

- Will wireless roaming be required?
- What authentication for users is needed?
- Will open access (hotspots) be provided for the guests?
- Which network services and applications are available to wireless users?
- What encryption technique can be used?
- Are wireless IP telephones planned?
- Which coverage areas need to be supported?
- How many users are in each coverage area?

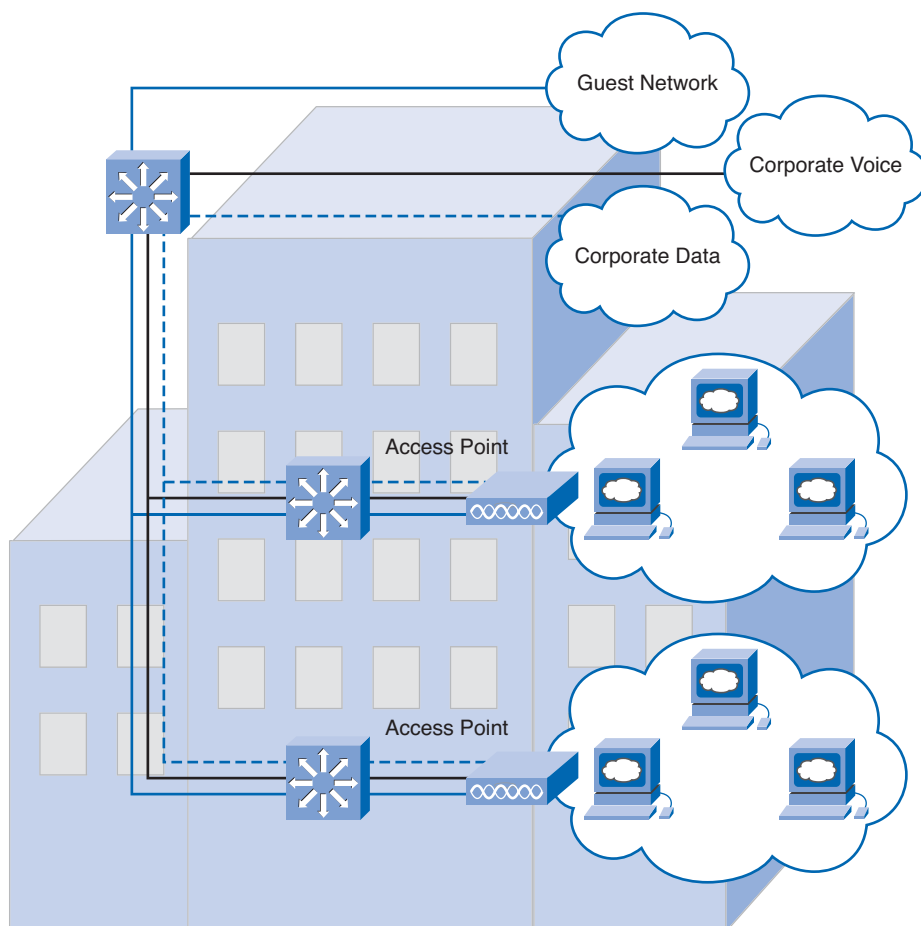
If the designer does not get answers to the questions or fully understand the customer requirements, implementing a wireless LAN will be difficult, if not impossible. For example, the requirements to provide unsecured hotspots are significantly less complex to design than authenticated access to protected internal servers.

Physical Network Design

In typical wireless network designs, most of the effort focuses on the physical coverage areas of the network.

The network designer conducts a site survey to determine the coverage areas for the network and to find the optimum locations for mounting wireless access points. The site survey results help determine the access point hardware, types of antennas, and the desired wireless feature sets. The designer determines that roaming between overlapping coverage areas can be supported. Figure 1-28 shows a physical WLAN topology.

Figure 1-28 Physical WLAN Topology



Logical Network Design

Designing the logical network usually causes network designers the most difficulty. Customers often want to provide different levels of access to different types of wireless users. In addition, wireless networks must be both easy to use and secure. Resolving both the desired features and the constraints presents many different ways to design and configure wireless LANs.

An example of a complex wireless network design is a business that needs to offer the following services:

- Open wireless access for their visitors and vendors
- Secured wireless access for their mobile employees
- Reliable connectivity for wireless IP phones

Network Access Considerations Unique to WLANs

Each type of wireless access requires unique design considerations.

Open Guest Access

When visitors and vendors are at a business site, they often require access to e-mail and websites. This type of access must be convenient to use, and typically is not *Wired Equivalent Privacy (WEP)* or *Wi-Fi Protected Access (WPA)* encrypted. To help guest users connect to the network, the Access Point *service set identifier (SSID)* is broadcast.

Many hotspot guest systems use DHCP and a logging server to register and record wireless use. Guest users typically access the wireless network by opening a browser window and agreeing to a specified usage policy. The guest registration system records the user information and hardware address and then begins logging the IP traffic. These systems require an application server to be installed on the same network or VLAN as the access points.

Secured Employee Access

Some WLAN devices do not support isolated guest access. To secure employee access, use an entirely separate WLAN infrastructure that does not include guest access. The recommended practice is to separate the internal users on a different VLAN. Figure 1-29 shows open guest and secured employee access WLANs. This setup allows for guests to access the Internet or other permitted area without providing total access to the network.

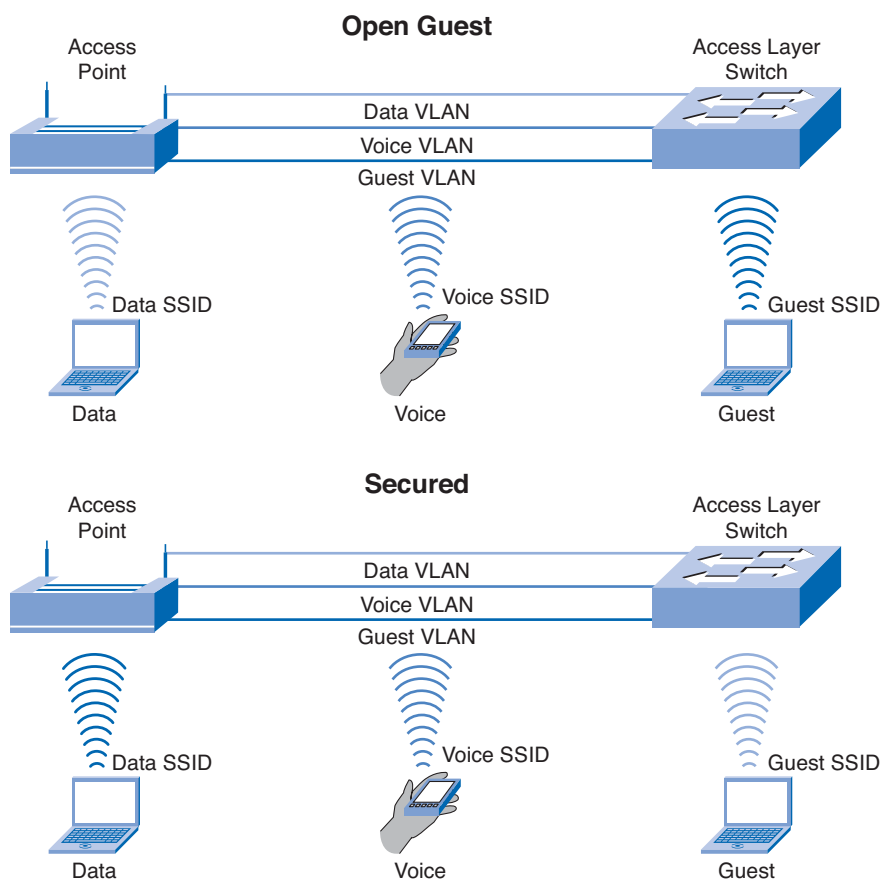
Best Practice Guidelines for WLAN Access

Other wireless implementation recommended practices include the following:

- Nonbroadcast SSID
- Strong encryption
- User authentication
- VPN tunneling for sensitive data
- Firewall and intrusion prevention

In areas where secured wireless is restricted to a few devices, MAC address filtering can be used to limit access.

One of the primary benefits of wireless networking is ease and convenience of connecting devices. Unfortunately, that ease of connectivity, and the fact that the information is transmitted through the air, makes a wireless network vulnerable to interception and attacks.

Figure 1-29 Open Guest and Secured Employee Access WLANs

Standard best practices for securing a wireless access point and the associated wireless transmissions include the following procedures:

- Modify the default SSID, and do not broadcast it unless necessary.
- Use strong encryption.
- Deploy mutual authentication between the client and the network using pre-shared keys or an implementation of Extensible Authentication Protocol (EAP).
- Use VPNs or WPA combined with MAC ACLs to secure business-specific devices.
- Use VLANs to restrict access to network resources.
- Ensure that management ports are secured.
- Deploy lightweight access points, because they do not store security information locally.
- Physically hide or secure access points to prevent tampering.
- Monitor the exterior building and site for suspicious activity.

Some of these factors affect network design (for example, the location and type of authentication servers and VPN endpoints and the choice of lightweight access points).

Supporting WANs and Remote Workers

In many companies, not every employee works on the main site premises. Employees who work offsite can include the following:

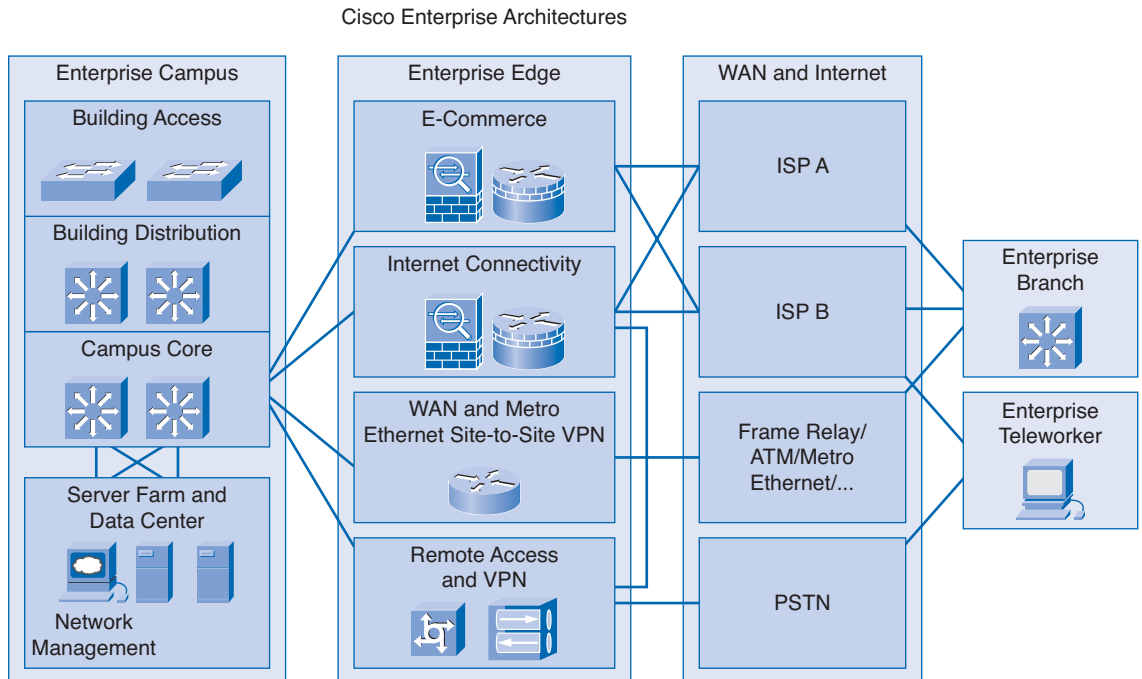
- Remote workers
- Mobile workers
- Branch employees

Remote workers usually work one or more days a week from home or from another location. Mobile workers may be constantly traveling to different locations or be permanently deployed at a customer site. Some workers are employed at small branch offices. In any case, these employees need to have connectivity to the enterprise network. As the Internet has grown, businesses have turned to it as a means of extending their own networks.

Design Considerations at the Enterprise Edge

The enterprise edge is the area of the network where the enterprise network connects to external networks. Routers at the enterprise edge provide connectivity between the internal campus infrastructure and the Internet. They also provide connectivity to remote WAN users and services. The design requirements at the enterprise edge differ from those within the campus network. Figure 1-30 shows the Cisco Enterprise Architecture with an emphasis on the enterprise edge.

Figure 1-30 Cisco Enterprise Architecture



Cost of Bandwidth

Most campus networks are built on Ethernet technology. However, WAN connectivity at the enterprise edge is usually leased from a third-party telecommunications service provider. Because these leased services can be expensive, the bandwidth available to WAN connections is often significantly less than the bandwidth available in the LAN.

QoS

The difference in bandwidth between the LAN and the WAN can create bottlenecks. These bottlenecks cause data to be queued by the edge routers. Anticipating and managing the queuing of data requires a QoS strategy. As a result, the design and implementation of WAN links can be complicated.

Security

Because the users and services accessed through the edge routers are not always known, security requirements at the enterprise edge are critical. Intrusion detection and stateful firewall inspection must be implemented to protect the internal campus network from potential threats.

Remote Access

In many cases, the campus LAN services must extend through the enterprise edge to remote offices and workers. This type of access has different requirements than the level of public access provided to users coming into the LAN from the Internet.

Integrating Remote Sites into the Network Design

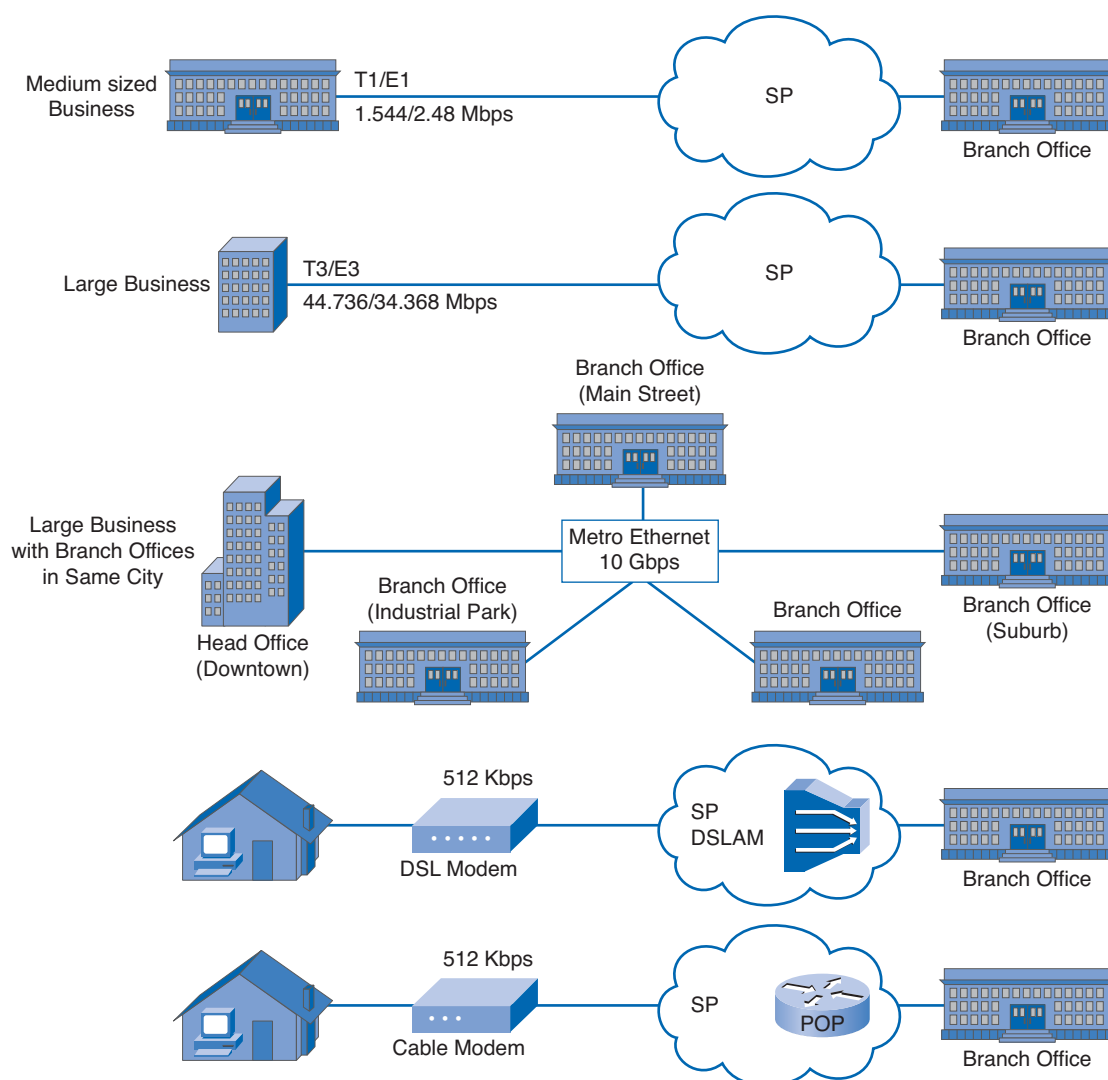
Designing a network to support branch locations and remote workers requires the network designer to be familiar with the capabilities of the various WAN technologies. Traditional WAN technologies include the following:

- Leased lines
- Circuit-switched networks
- Packet-switched networks, such as Frame Relay networks
- *Cell-switched networks* such as *Asynchronous Transfer Mode (ATM)* networks

In many locations, newer WAN technologies are available, such as the following:

- Digital subscriber line (DSL)
- Metro Ethernet
- Cable modem
- Long-range wireless
- Multiprotocol Label Switching (MPLS)

Most WAN technologies are leased on a monthly basis from a telecommunications service provider. Depending on the distances, this type of connectivity can be quite expensive. WAN contracts often include *service level agreements (SLA)*. These agreements guarantee the service level offered by the service provider. SLAs support critical business applications, such as IP telephony and high-speed transaction processing to remote locations. Figure 1-31 shows several WAN technologies.

Figure 1-31 WAN Technologies

MPLS

Cisco IOS MPLS enables enterprises and service providers to build next-generation intelligent networks. MPLS encapsulates packets with an additional header containing “label” information. The labels are used to switch the packets through the MPLS network. MPLS can be integrated seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet. MPLS is independent of access technologies.

MPLS technology is critical to scalable VPNs and end-to-end QoS. MPLS enables efficient use of existing networks to meet future growth and rapid fault correction of link and node failure. The technology also helps deliver highly scalable, end-to-end IP services with simpler configuration, management, and provisioning for both Internet providers and subscribers.

VPNs

One common connectivity option, especially for remote workers, is a VPN through the Internet. A VPN is a private network that uses a public network to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased lines, a VPN uses virtual connections routed through the Internet from the company private network to the remote router or PC.



Interactive Activity 1-5: Select WAN or VPN Connection Types (1.7.2.3)

In this interactive activity, you select the type of WAN or VPN connectivity appropriate for a specific remote worker's situation. Use file ia-172 on the CD-ROM that accompanies this book to perform this interactive activity.

Redundancy and Backup Links

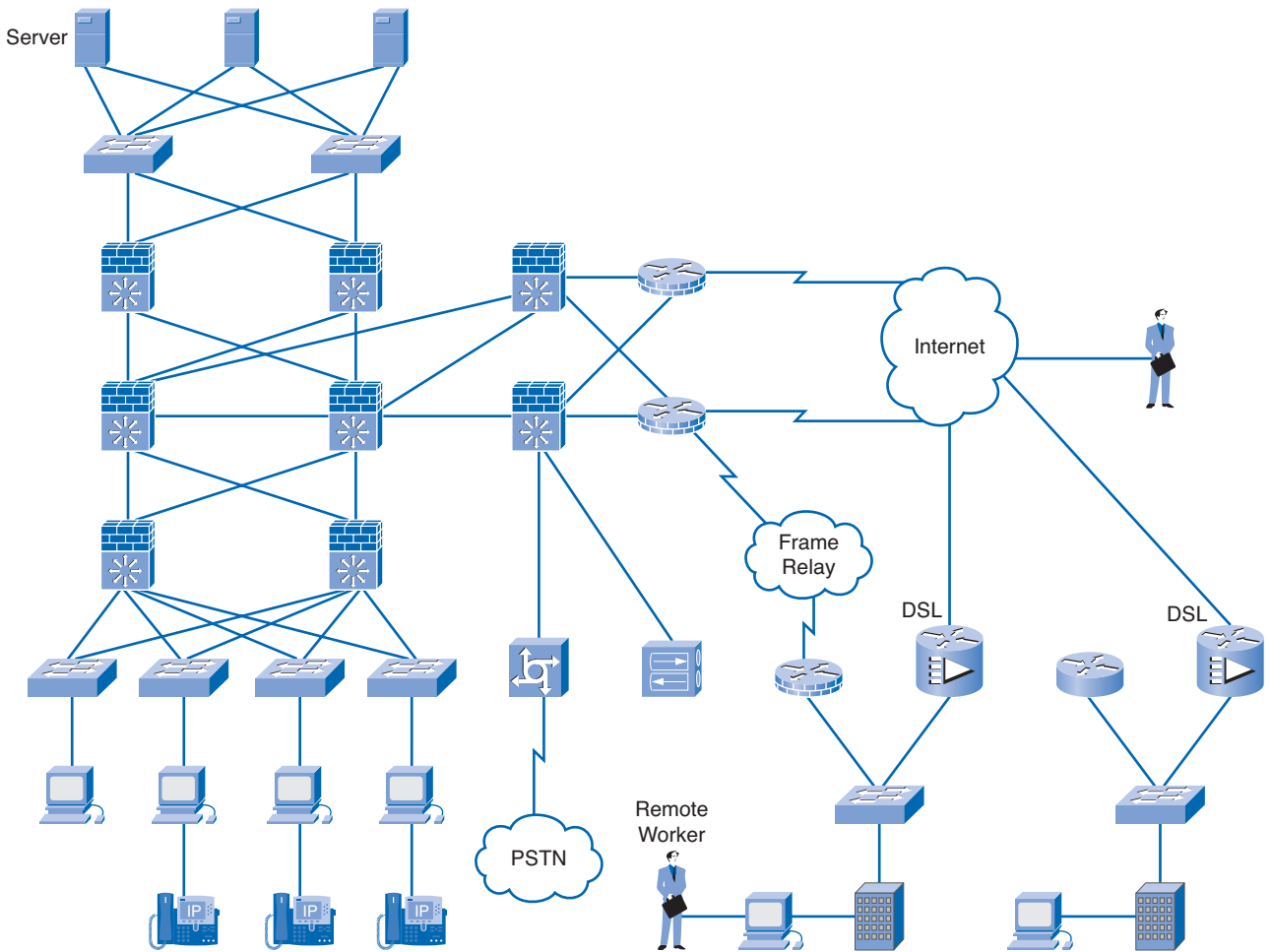
Redundancy is required on WAN links and is vitally important to ensure reliable connectivity to remote sites and users.

Some business applications require that all packets be delivered in a timely fashion. For these applications, dropped connectivity is not an option. Providing redundancy on the WAN and throughout the internetwork ensures high availability for end-to-end applications.

For a WAN, backup links provide the required redundancy. Backup links often use different technologies than the primary connection. This method ensures that if a failure occurs in one system, it does not necessarily affect the backup system.

For example, a business that uses point-to-point WAN connections to remote sites can use VPNs through the Internet as an alternative strategy for redundancy. DSL, ISDN, and dialup modems are other connectivity options used to provide backup links in the event of a WAN failure. Although the backup links are frequently slower than the primary connections, they can be configured to forward only high-priority data and transactions. Figure 1-32 shows how a redundant DSL connection acts as a backup for a point-to-point WAN connection.

In addition to providing a backup strategy, redundant WAN connections can provide additional bandwidth through load sharing. The backup link can be configured to provide additional bandwidth all the time or during peak traffic time only.

Figure 1-32 Redundancy in a Point-to-Point WAN Connection**Interactive Activity 1-6: Identify Connectivity Options (1.7.3.2)**

In this interactive activity, you select the appropriate connectivity option to its correct network location. Use file ia-173 on the CD-ROM that accompanies this book to perform this interactive activity.

Summary

The process of designing a good network requires concerted efforts by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business. The four fundamental technical requirements of network design are scalability, availability, security, and manageability.

The Cisco Enterprise Architectures can be used to further divide the three-layer hierarchical design into modular areas. The modules represent areas that have different physical or logical connectivity. Large network design projects are normally divided into three distinct steps:

Step 1. Identify the network requirements.

Step 2. Characterize the existing network.

Step 3. Design the network topology and solutions.

Failure to correctly estimate the scope of a network upgrade project can greatly increase the cost and time required to implement the new design. The goals of the core layer design are a difficult concept for most to grasp. Identification of the design goals makes this task easier. Goals of the core layer design include the following:

- Provide 100% uptime.
- Maximize throughput.
- Facilitate network growth.
- Redundancy at the core layer enables the network to keep functioning even when a device or link fails.
- Layer 3 devices, including multilayer switches, are usually deployed at the core layer of the network.
- Most core layers in a network are wired in either a full-mesh or partial-mesh topology.
- Devices at the core layer usually contain redundant power supplies and hot-swappable components.
- Fast-converging routing protocols, such as OSPF and EIGRP, are the appropriate choice for the core layer.

The distribution layer represents a routing boundary between the access layer and the core layer. As with the core layer, the distribution layer goals must also be met. The design goals for the distribution layer are as follows:

- Filtering and managing traffic flows
- Enforcing access control policies
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions
- Routing between access layer VLANs

In the hierarchical design model, it is easiest and usually least expensive to control the size of a failure domain in the distribution layer. Redundancy at the distribution layer ensures that failure domains remain small. Providing multiple connections to Layer 2 switches can cause unstable behavior in a network unless STP is enabled. Traffic filtering is one way to ensure the smooth flow of traffic between the access and the core layers. This is accomplished at the distribution layer. ACLs are commonly applied to routers to ensure that traffic flows continue, and they provide an additional level of security

for the network. With ACLs enabled, the router examines each packet, and then either forwards or discards it, based on the conditions specified in the ACL. The criteria for the decisions can include the following:

- Source address
- Destination address
- Protocols
- Upper-layer port numbers
- Whether the packet is part of an established stream

In addition to providing basic connectivity at the access layer, the designer needs to consider the following:

- Naming structures.
- VLAN architecture.
- Traffic patterns.
- Prioritization strategies.
- Most recent Ethernet networks use a star topology, which is sometimes called a hub-and-spoke topology.
- Using VLANs and IP subnets is the most common method for segregating user groups and traffic within the access layer network.
- Networks also need mechanisms to control congestion when traffic increases and queues for delivery.
- Congestion is caused when the demand on the network resources exceeds the available capacity.
- Classifying data at or near the source enables the data to be assigned the appropriate priority as it moves through the entire network.

As a network designer, it is extremely important that these goals and considerations be used from the very beginning of the network design methodology. From the topology used to the level of physical access given to personnel can mean the difference between a successful network implementation and a dismal failure.

Activities and Labs



Interactive Activities on the CD:

Interactive Activity 1-1: Match the Characteristics of the Hierarchical Model and the Cisco Enterprise Architecture (1.1.2)

Interactive Activity 1-2: Determining the Project Scope (1.1.3)

Interactive Activity 1-3: Match ACLs to the Appropriate Statements (1.3.4)

Interactive Activity 1-4: Identify Summary Routes (1.3.5)

Interactive Activity 1-5: Select WAN or VPN Connection Types (1.7.2.3)

Interactive Activity 1-6: Identify Connectivity Options (1.7.3.2)

Packet Tracer
Activity**Packet Tracer Activities on the CD:**

Comparing Mesh Topologies (1.2.1)

Observing Network Convergence (1.2.3)

Demonstrating Distribution Layer Functions (1.3.1)

Investigating Failure Domains (1.3.2)

Placing ACLs (1.3.4)

Exploring Access Layer Functions (1.4.1)

Creating Topologies (1.4.2)

Observing and Recording Server Traffic (1.5.1)

Using Redundant Links on Server Farm Devices (1.5.3)

**Hands-On Labs in Part II of this book:**

Lab 1-1: Creating an ACL (1.3.4)

Lab 1-2: Monitoring VLAN Traffic (1.4.3)

Lab 1-3: Identifying Network Vulnerabilities (1.4.5)

Lab 1-4: Gaining Physical Access to the Network (1.4.6.2)

Lab 1-5: Implementing Switch Port Security (1.4.6.3)

Check Your Understanding

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

1. In today’s Internet-based economy, customer service and business networks should be available what percentage of the time?
 - A. Nearly 100%
 - B. Nearly 75%
 - C. Nearly 50%
 - D. Nearly 25%
2. What are the fundamental design goals for building a successful network? (Choose all that apply.)
 - A. Scalability
 - B. Availability
 - C. Security
 - D. Manageability
 - E. All of the above

3. With a hierarchical network design, which layer is used to connect distribution layer devices?
 - A. Access layer
 - B. Core layer
 - C. Distribution layer
 - D. Network layer
4. When designing a network, what is a common strategy to take?
 - A. Bottom-up approach
 - B. Divide-and-conquer approach
 - C. Top-down approach
 - D. Technical-requirements approach
5. When designing a network, the core layer includes one or more links to the devices at the enterprise edge to support what? (Choose all that apply.)
 - A. Internet connectivity
 - B. VPNs
 - C. Extranet
 - D. WAN access
 - E. All of the above
6. What topology is used when wiring the distribution layer?
 - A. Hub
 - B. Spoke
 - C. Partial mesh
 - D. Full mesh
7. When filtering traffic using extended ACLs at the distribution layer, what filtering criteria can be used?
 - A. Source address
 - B. Destination address
 - C. Protocols
 - D. Port numbers or applications
 - E. All of the above
8. What is a benefit to route summarization?
 - A. Higher router overhead
 - B. Lower router overhead
 - C. More routing updates
 - D. Larger routing tables

9. Which layer of the network represents the edge of the network where end devices are connected?
 - A. Access layer
 - B. Distribution layer
 - C. Core layer
 - D. None of the above
10. What is one method used for segregating and controlling traffic on a network?

Challenge Questions and Activities

These questions are more challenging and require you to bring together knowledge from various parts of the chapter. Answer all questions in this part. Answers are listed in Appendix A, “Check Your Understanding and Challenge Questions Answer Key.”

1. A small drafting company is trying to decide whether they should expand their network infrastructure. Their current network technician has determined that too much traffic from all locations is congesting the network. She believes that if the network were expanded the increase in traffic could potentially create more problems. She contacts you and asks what could be done to filter traffic and control the broadcasts that are currently on the network. What suggestion would you make and why?
2. Company XYZ has a four-floor building in which their administrative, human relations, management, and distribution center employees work. Each section has several servers located in its offices. Production has exceeded their expectations, and the amount of traffic sent to and from the servers has increased 200 percent. This increase has resulted in increased maintenance for the IT technician. The technician spends several hours per day moving from one location to another. As a result, the technician’s productivity has decreased. What suggestion would you make to reduce downtime, provide redundant high-capacity links, and lower the cost of providing services to each department?

NUMERICS

2960 switches, 159

3DES (Triple DES), 259

A

accept-lifetime command, 192

access

- employee, 37
- multi-access WANs, 250
- open guest, 37
- remote, WANs, 40
- remote-access VPNs, 259
- users, adding, 65
- WPA, 37

access control lists. *See* ACLs

access layer, 3

- design, 22, 25-30
- topologies, designing, 158-160

access points. *See* APs

account managers, role of, 61

ACLs (access control lists), 120

- implementing, 175
- testing, 231
- traffic, filtering at distribution layers, 19-21

Active Directory Services, 126

Adaptive Security Appliances (ASA) devices, 260

adding

- hashes to messages, 260
- modules. *See also* scalability, 6
- user access, 65
- services, 6
- WAN connections, 164-165
- wireless network coverage, 168

addressing

- blocks
 - assigning, 195-197*
 - determining, 189-190*
- IP. *See also* IP addressing
 - formatting, 200-202*
 - implementing on Cisco devices, 202-204*
 - migrating, 202*
- prefix and summarization, 187
- reserved, 202
- schemes, 182-183

administrative distance, 240, 252

AES (Advanced Encryption Standard), 259

agents

- call, 133
- management, 70

aggregate links, 11

agreements, SMARTnet, 280-281

AH (Authentication Header), 261

algorithms

- data integrity, 260
- encryption, 260

alternate paths, 228

analysis, 55. *See also* planning

- existing networks, 7
- requirements, 150-158
- traffic, 116

analyzers, protocol, 216

antennas, types of, 99

appliances, security, 173-174

applications

- documentation, 106, 139
 - external traffic diagrams, 143-144*
 - internal traffic diagrams, 140-141*
 - remote site traffic diagrams, 142-143*
 - traffic flow, 139-140*
- existing, 279
- NBAR, 116
- networks, 114
 - characterization, 115-116*
 - hardware, 117-118*
 - Microsoft domain services, 125-127*
 - performance, 114*
 - QoS, 27, 127-131*
 - traffic flow, 116-117*
 - types, 118-127*
- SAS (Software Application Support) services, 282
- servers, 133
- support, defining, 165-166
- transaction-processing, 119-121
- WAN connectivity, 239

applying

- ACLs, 20-21
- Feature Navigator, 91-92
- integrated services, 174
- show version command, 89-90
- top-down or bottom-up approach, 69
- VLSM, 185
- wireless site surveys, 100-101

approval, customer, 272-273

APs (access points)

- wireless, locating, 170-171
- wireless site surveys, 98

architecture

- Cisco Enterprise Network Architectures, 5-6, 85
- hierarchical network design, 3, 5-6
- logical diagrams, 82-84
- network design methodologies, 6-7, 9

arp, 216

ASA (Adaptive Security Appliances) devices, 260

assembling existing proposal information, 270-271

assessment of business case, 50

assigning address blocks, 195-197
ATM (Asynchronous Transfer Mode) networks, 40
atomic transactions, 119
attacks, 32, 173. *See also* security
auditing networks, 116
authentication, 192
Authentication Header (AH), 261
autogeneration of QoS policies, 130
automatic summarization, disabling, 185
AutoQoS, 130
availability, 51, 183

- 2960 switches, 159
- access layers, 24
- applications, 114
- Distribution layer, 160
- documenting, 105
- Frame Relay connections, 244
- networks, 3
- requirements for, 153-155
- server farms, 33, 227, 230
- wireless networks, 170

B

backbones

- networks, 9

background of FilmCompany, 310-311
backups

- links
 - configuring, 252-253*
 - WANs, 42-43*
- paths, 228

backward-explicit congestion notification (FECN), 248
bandwidth

- commands, 240
- cost of, 39
- file transfers, 123
- limitations of, 224

baselines

- networks, 56
- server farms, 227

BECN (backward-explicit congestion notification), 248
behavioral questions, 290
benefits

- of prototyping, 214
- of SMARTnet agreements, 280

best practices, WLAN access, 37-38
bill-of-materials (BOM), creating, 276-279
bits, DE, 247
blocks

- addresses
 - assigning, 195-197*
 - determining, 189-190*
- switches, 17, 160

BOM (bill-of-materials), creating, 276-279
boot process, 93

bottlenecks, 217
bottom-up approach, 69
BPDU (bridge protocol data unit), 228
branch workers, 39-43
bridge protocol data unit. *See* BPDU
building prototype networks, 212-213
business applications, 279
business case, 50
business goals, 7

- analyzing, 150-152
- defining technical requirements, 66-69
- documenting, 104-106
- identifying, 65-66

business growth, 65

C

cables

- applications, 118
- crossover, 240
- V.35, serial connectivity simulation, 241-242

call agents, 133
campus networks

- Cisco Enterprise Architectures, 5

campus network prototypes, 211-213

- creating test plans, 213
- identifying design weaknesses, 217-218
- redundancy and resiliency, 216
- validating devices, 215-216
- verifying goals and requirements, 214-215

careers, 289-291. *See also* interviews
case studies, Cisco Lifecycle Services, 51

- Design phase, 54-55
- Implement phase, 55
- Operate phase, 56
- Optimize phase, 56
- Plan phase, 53
- Prepare phase, 52
- project plan, 53

catalogs, 119
CCNP (Cisco Certified Networking Professional), 289

- preparing for exams, 291

cell-switched networks, 40
centralized servers, 30
channel communications, 61
characterization of applications, 115-116
CIDR (Classless InterDomain Routing), 185

- and summarization, 186-187

cipher strings, 259
Cisco Catalyst 2960 switches, upgrading, 279
Cisco Certified Networking Professional (CCNP), 289

- preparing for exams, 291

Cisco devices, implementing IPv6 on, 202-204
Cisco EasyVPN, 258
Cisco Enterprise Network Architectures, 5-6, 85
Cisco Focused Technical Support Services, 281-282

Cisco IOS

- commands, 215
- file-naming conventions, 90

Cisco Lifecycle Services, 50-51

- case studies. *See* case studies
- Design phase, 54-55
- Implement phase, 55
- Operate phase, 56
- Optimize phase, 56
- Plan phase, 53
- Prepare phase, 52
- project plans, 53

Cisco Networking Academy, 289, 291**Cisco SDM interfaces, 258****Cisco switch clustering, 159****Cisco Unified Communications Manager, 122****class of service (CoS), 131****classful subnets, 184-185****classification**

- QoS, 130-131
- traffic, 28

Classless InterDomain Routing. *See* CIDR**clear frame-relay-inarp command, 252****client-to-client application communication, 115****client-to-distributed server application communication, 115****client-to-enterprise edge application communication, 115****client-to-server farm application communication, 115****clients**

- e-mail, 124
- interaction, 7
- network designer, interaction with, 63-66

clock rate command, 241**closets, wiring, 23, 29, 189-190****clusters of devices, 152****co-located servers, 151****commands**

- accept-lifetime, 192
- bandwidth, 240
- clear frame-relay-inarp, 252
- clock rate, 241
- copy, 92
- copy flash tftp, 92
- copy tftp flash, 92-93
- debug, 215
- debug frame-relay lmi, 254-255
- dir flash, 93
- ip name-server, 203
- ip subnet-zero, 196
- ipv6 address, 203
- ipv6 hostname, 203
- ipv6 rip name enable, 204
- ipv6 rip RTO enable, 204
- ipv6 rip tag enable, 204
- ipv6 router rip, 204
- ipv6 unicast-routing, 202
- maximum-paths, 191
- network, 204
- no access-list, 20
- send-lifetime, 192

- show, 81, 214, 215, 250
- show cdp neighbors, 214
- show cdp neighbors detail, 82, 151
- show frame-relay lmi, 251, 254
- show frame-relay map, 251
- show frame-relay pvc, 253
- show frame-relay pvc [interface interface] [dlci], 251
- show interface serial, 253-254
- show interfaces serial, 250
- show ip arp, 214
- show ipv6 rip, 204
- show ipv6 route rip, 204
- show tech-support, 81
- show version, 89-90
- variance, 192

communications

- channels, 61
- client-to-client, 115
- client-to-distributed server, 115
- client-to-enterprise edge, 115
- client-to-server farm, 115
- interpersonal skills, 63-64

complete network replacements, 274**components**

- bill-of-materials, creating, 276-279
- hot-swappable, 13
- VPNs, 259-260

concentrators, VPN, 259**concessions**

- registers, 114
- vendors, StadiumCompany network upgrade, 306

configuration

- backup links, 252-253
- clock rate, 241
- Etherchannels, 153
- fixed, 159
- Frame Relay, 249, 252
- interfaces, 240
- keys, managing, 192-193
- networks
 - access layer*, 22, 25-30
 - analyzing requirements*, 150-158
 - convergence*, 14
 - core layer*, 9-11, 14
 - design*, 2
 - distribution layer*, 14-22
 - hierarchical*, 3, 5-6
 - methodologies (design)*, 6-7, 9
 - overview of design*, 2-3
- primary links, 253-256
- proposals, 283-284
- PVRST+, 228
- QoS, 130-131
- RIPng, 204-205
- WANs, 163-168
- wireless networks, 34-38

congestion, control, 248**connections**

- DLCI, 247
- DSL, 95
- E1, 244
- fiber, limitations of, 224

- Frame Relay, 165, 244
- ISPs, troubleshooting, 223
- monitoring, 248
- physical, 87
- prototype VPN for remote workers, 261-262
- PVC, 250
- remote
 - lab environment simulations*, 240-242
 - prototypes*, 239
 - testing*, 239
- remote sites, determining, 163-165
- RSTP, troubleshooting, 228, 230
- security, 174
- serial, simulating, 241-242
- T1, 244
- testing, 214
- VPNs. *See* VPNs
- WAN, adding, 164-165
- consistency**
 - of QoS, 130
 - of transactions, 119
- constraints, 66**
 - defining, 66, 68-69
 - design, affect on, 150
 - Distribution layer, 160
- content networking, 8**
- contracts for services, 280**
- control**
 - congestion, 248
 - of network simulation software, 239
 - traffic, 139
- controlling network traffic, 26-27**
- conventions, file naming, 90**
- convergence**
 - networks, 13
 - at access layers*, 24
 - design*, 14
 - selecting routing protocols*, 14
 - time, 14
 - voice/video, 131-136
- copy command, 92**
- copy flash tftp command, 92**
- copy tftp flash command, 92-93**
- core layer**
 - design, 9-11, 13-14
 - topologies, designing, 161
- CoS (class of service), 131**
- cost**
 - of bandwidth, 39
 - estimates, 270
 - network simulation software, 239
- counters, Invalid, 254**
- coverage options, wireless networks, 168**
- CPE (customer premises equipment) routers, 244**
- CQ (custom queuing), 128**
- CRM (customer relationship management) software, 279**
- crossover cables, 240**
- cryptography, 260**

- CSUs/DSUs, 240-241**
- current network environment, 270-271**
- custom queuing (CQ), 128**
- customer premises equipment (CPE) routers, 244**
- customer relationship management (CRM) software, 279**
- customer-caused delays, 275**
- customers. *See also* clients**
 - approval, 272-273
 - defining, 64-65
 - queries, 119
 - satisfaction, 65
 - working with, 63-64
- customization of VPN endpoints, 166-167**

D

- data centers, 30, 87**
- Data Encryption Standard (DES), 259**
- data integrity algorithms, 260**
- data rates, guaranteed, 247**
- data-link connection identifier (DLCI), 247**
- databases**
 - MIB, 72
 - updating, 119
- DCE functions, 241**
- DE (discard eligible) bits, 247**
- debug commands, 215**
- debug frame-relay lmi command, 254-255**
- debugging, LMI, 254-255**
- decentralized servers, 30**
- decryption, 259**
- defense, 174**
- defining**
 - application support, 165-166
 - customers, 64-65
 - policies and procedures, 56
 - technical requirements, 66-69
 - traffic patterns, 165-166
- delay, 155**
 - customer-caused, 275
- DELETED status, 253**
- delivery**
 - services, 289
 - transactions, 119
- demarcation points**
 - deterministic networks, 5
- demilitarized zones (DMZs), 33**
- denial-of-service (DoS) attacks, 32, 173**
- deployment**
 - Cisco Lifecycle Services, 50-56
 - switch blocks, 17
- DES (Data Encryption Standard), 259**
- description of wiring closets, 189-190**

design

- documentation, 175-176
- enterprise edge, 39-40
- FilmCompany, 314
- IP addressing, 182
 - applying VLSM, 185*
 - CIDR and summarization, 186-187*
 - classful subnets and summarization, 184-185*
 - hierarchical routing and addressing schemes, 182-183*
 - IPv4 and IPv6, 199-205*
 - naming schemes, 187-198*
- logical LAN IP addressing schemes, 187-188
- naming schemes, 197-198
- networks
 - access layer, 22-30, 158-160*
 - analyzing requirements, 150-158*
 - campus network prototypes, 212-218*
 - convergence, 14*
 - core layer, 9-11, 14, 161*
 - distribution layer, 14-22, 160-161*
 - documenting, 102-106*
 - existing network characterization, 107-108*
 - goals, 3*
 - hierarchical, 3, 5-6*
 - implementing, 272*
 - logical, 36, 162*
 - managing, 69-71, 73*
 - methodologies, 6-7, 9*
 - overview of, 2-3*
 - physical, 36*
 - placing security functions and appliances, 173-174*
 - security, 173*
 - selecting LAN topologies, 158-162*
 - topologies, 7-9*
 - trade-offs, 157-158*
 - wireless, 168-173*
 - WLANs, 172-173*
- process, preparing, 63-66
- proof-of-concept, 212
- proposals, assembling existing information, 270-271
- remote worker support, 163-168
- stadium networks, implementing, 272-273
- VPNs, customizing endpoints, 166-167
- WANs, 163-168
- wireless networks, 34-38

Design phase, 51-55**designated paths, 228****designating routing strategies, 191-193****detection of threats, 174****deterministic networks, 5****development of implementation plans, 272-273**

- maintenance, 276
- selecting installation methods, 273-275

devices

- ASA, 260
- clusters, 152
- DTE, 241
- information, obtaining information about, 81-82
- IPv6, implementing on, 202-204
- LAN prototypes, validating, 222

- naming, 197

- QoS, 131

- SDM, 56

- security, 30

- server farms, 228-230

- show version command, 89-90

- StadiumCompany network upgrade, 304

- validating, 215-216

- VPNs, 259-260

- WANs, 245-248

DH (Diffie-Hellman) key agreements, 260**diagrams**

- external traffic, 143-144

- internal traffic, 140-141

- networks

- creating, 80-82*

- logical architecture, 82-84*

- modular block, 85-86*

- remote sites, 142-143

diameter, network, 156**Differentiated Services Code Point (DSCP), 131****Diffie-Hellman (DH) key agreements, 260****digital subscriber line (DSL), 95****digits, hexadecimal, 199****dir flash command, 93****disabling**

- automatic summarization, 185

- ports, 229

discard eligible (DE) bits, 247**discontiguous networks, 184****distribution**

- route summarization and, 193-194

- video, 156

distribution layer, 3

- design, 14-22

- topologies, designing, 160-161

DLCI (data-link connection identifier), 247**DMZs (demilitarized zones), 33****DNS (Domain Name System), 8****DNS Services, 126****documentation**

- applications, 139

- external traffic diagrams, 143-144*

- internal traffic diagrams, 140-141*

- remote site traffic diagrams, 142-143*

- traffic flow, 139-140*

- bill-of-materials, creating, 276-279

- design, updating, 175-176

- existing networks, 80

- creating diagrams, 80-82*

- logical architecture diagrams, 82-84*

- modular block diagrams, 85-86*

- strengths and weaknesses of, 86-88*

- network design, 102-106

- existing network characterization, 107-108*

- proposals, creating, 283-284

- response, 57-58

- sale process, 57-63

Domain Name Service. *See* DNS

domains

- large failure, 217
- Microsoft network applications, 125-127

DoS (denial-of-service) attacks, 32, 173

downloading Cisco IOS software, 92-93

downtime

- planning, 276
- reducing, 18-19

DRAM (dynamic random-access memory), 92

DSCP (Differentiated Services Code Point), 131

DSL (digital subscriber line), 95

DTE devices, 241

dual stack migration, 202

durability of transactions, 120

dynamic ACLs, 20. *See also* ACLs

dynamic channel assignment, 170

dynamic random-access memory (DRAM), 92

E

e-commerce, availability for, 154

e-mail

- file transfers, 123-124
- overview of, 123

E1 connections, 244

edge

- Cisco Enterprise Architecture, 5
- enterprise design, 39-40
- networks
 - security,* 28-29
 - services at,* 27

EIGRP (Enhanced Interior Gateway Routing Protocol), 11, 222

- load balancing, 191

emergency services, 114

employee access, 37

Encapsulating Security Payload (ESP), 261

encryption, 120, 259. *See also* security

- algorithms, 260

endpoints

- video, 133
- VPNs, customizing, 166-167

Enhanced Interior Gateway Routing Protocol. *See* EIGRP

enterprise architectures, 5-6

enterprise edge design, 39-40

environments, current network, 270-271

equipment inventory lists, 89

ESP (Encapsulating Security Payload), 261

estimates

- costs, 270
- timelines and resources, 275

Etherchannels, configuring, 153

exams, preparing for, 291

executive summary, 270-271

existing applications, 279

existing equipment, limitations of, 159

existing facilities, StadiumCompany network upgrade, 304

existing networks

- analyzing, 7
- characterization, 107-108
- documentation, 80
 - creating diagrams,* 80-82
 - logical architecture diagrams,* 82-84
 - modular block diagrams,* 85-86
 - strengths and weaknesses of,* 86-88
- phased installations, 273-274
- updating, 88, 90-94
- upgrading, 95-96

existing staff capabilities, 217

extending services to remote locations, 163

external names, 197

external traffic, 117

- diagrams, 143-144

extranets, 9

F

faceplates, 96

facilities, StadiumCompany network upgrade, 304

failover, 24, 31

failure, preventing network, 12

failures, 217

farms, server. *See* server farms

Feature Navigator, applying, 91-92

FECN (forward-explicit congestion notification), 248

fiber connectivity, limitations of, 224

files

- naming, 90
- sharing, 115
- transfers, 123-124

FilmCompany network upgrade story, 309

- background, 310-311
- design, 314
- networks, 313-314
- organization, 311-313

filtering traffic at distribution layers, 19-21

finalizing proposals, 283

firewalls, 121. *See also* security

- rule sets, 175
- server farms, 230

fixed configurations, 159

flash memory, 92

flat networks. *See also* networks, 4

flat topologies, 222

flexibility of network simulation software, 239

floating static routes, 252

flow, traffic, 139-140

- external traffic diagrams, 143-144
- internal traffic diagrams, 140-141
- remote site diagrams, 142-143

formatting

- IP addresses, 200, 202
- proposals, 283-284

forward-explicit congestion notification (FECN), 248**Frame Relay, 246**

- administrative distance configuration, 252
- configuring, 249
- congestion control, 248
- connections, 165, 244
- DLCI, 247
- guaranteed data rates, 247
- interfaces, checking status, 253
- LMI, 248
- local loops, 246
- maps, 249-252
- risk and weaknesses, 256
- troubleshooting, 252-256
- zero CIR, 247

full-meshed topologies, 11-12, 26**functionality**

- commands, 216
- Layer 3, 255-256
- network simulation software, 239
- testing, 213-215

functions

- DCE, 241
- security, 173-174

G**gateways, 133****gathering information, 116****generic routing encapsulation (GRE), 259****global unicast addresses, 202****goals**

- analyzing, 150-152
- business, 7
 - defining technical requirements, 66-69*
 - documenting, 104-106*
 - identifying, 65-66*
- design, verifying, 214-215
- Frame Relay connections, 244
- LANs prototypes, 219
- of core layers, 10
- projects, 102-103
- server farms, 225-226
- VPNs, 256-257

goals, network design, 3**GRE (generic routing encapsulation), 259****guaranteed data rates, 247****guidelines, naming, 198****H****hardware**

- applications, 117-118
- bill-of-materials (BoM), creating, 276-279
- Cisco Focused Technical Support Services, 281-282
- existing, 89

- queues, 128
- replacement times, 280
- SAS (Software Application Support) services, 282
- show version command, 89-90
- SMARTnet services, 280-281
- upgrading, 95-96

Hashed Message Authentication Code (HMAC), 260**hashes, adding to messages, 260****headers**

- AH, 261
- IP, 200

hexadecimal digits, 199**hierarchies**

- routing, 182-183
- three-layer, simulating, 221-222

hierarchical network design, 3, 5-6**high availability**

- access layers, 24
- server farms, 33

high-capacity switches, 31**high-priority packets, 129****high-speed links, 11****high-speed WAN interface cards (HWICs), 95****HMAC (Hashed Message Authentication Code), 260****HMAC-Message Digest 5 (MD5), 260****HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1), 260****hosts**

- per network, 190
- reachability of, 188

Hot Standby Routing Protocol (HSRP), 120**hot-swapping**

- components, 13
- options, 96

HSRP (Hot Standby Routing Protocol), 120**HTTP (Hypertext Transfer Protocol), 124-125****hub-and-spoke topology, 26. *See also* networks; topologies****human error, reducing, 13****HWICs (high-speed WAN interface cards), 95****Hypertext Transfer Protocol. *See* HTTP****hypothetical questions, 290****I****IDS (intrusion detection system), 85****IKE (Internet Key Exchange), 261****Implement phase, 51**

- case study, 55

implementation

- ACLs, 175
- Etherchannels, 153
- planning, 270-273
 - maintenance, 276*
 - selecting installation methods, 273-275*
- QoS, 130-131
- security services, 174

in-band, 159**information**

- gathering, 116
- management, 70

infrastructure

- security, 173
- voice, real-time streaming, 122

installation

- Cisco IOS software, 92-93
- methods, selecting, 273-275
- New Hardware Option (3.3.3), 96
- pilot networks, 165, 212-213
- planning, 55, 276
 - Cisco Focused Technical Support Services, 281-282*
 - creating bill-of-materials, 276-279*
 - SAS (Software Application Support) services, 282*
 - SMARTnet services, 280-281*

integrated services, applying, 174**integrating existing information, 271****interactive kiosk services, 114****interactive voice response (IVR), 133****interfaces**

- cards, 95
- Cisco SDM, 258
- configuring, 240
- Frame Relay, checking status, 253
- LMI, 248
- subinterfaces, 250

interference, APs and, 98**Intermediate System-to-Intermediate System (IS-IS) protocol, 21****internal device names, 197****internal traffic, 117**

- diagrams, 140-141

International Telecommunication Union (ITU-T), 246**Internet bandwidth limitations, 224****Internet Key Exchange (IKE), 261****Internet service provider. *See* ISP****interpersonal skills, 63-64****interviews**

- with FilmCompany, 311-313
- methods, 290-291
- question types in, 290

intrusion detection system (IDS), 85**intrusion prevention systems, 157****Invalid counters, 254****inventory, show version command, 89-90****Inverse ARP (Inverse Address Resolution Protocol), 249-252****IOS**

- commands, 215
- file naming, 90

IP addressing

- design, 182
 - applying VLSM, 185*
 - CIDR and summarization, 186-187*
 - classful subnets and summarization, 184-185*
 - hierarchical routing and addressing schemes, 182-183*
 - IPv4 and IPv6, 199-205*
 - naming schemes, 187-198*
- validating, 223

ip name-server command, 203**IP Phones, 133****IP Security (IPsec), 259-261****IP (Internet Protocol) tools, 216****ip subnet-zero command, 196****IP telephony, 115, 122**

- availability, 154
- QoS, 127
- requirements, 133-136
- voice quality, 156

IPsec (IP Security), 259-261**ipv6 address command, 203****ipv6 hostname command, 203****ipv6 rip name enable command, 204****ipv6 rip RTO enable command, 204****ipv6 rip tag enable command, 204****ipv6 router rip command, 204****ipv6 unicast-routing command, 202****IS-IS (Intermediate System-to-Intermediate System) protocol, 21****isolating**

- traffic, 133
- transactions, 120

ISP (Internet service provider), 151

- troubleshooting, 223

ITU-T (International Telecommunication Union), 246**IVR (interactive voice response), 133**

J-K-L

jitter, 155**job searches, 289-291. *See also* interviews****keepalive messages, 248****key management, 192-193****kiosk services, 114****L2F (Layer 2 Forwarding) protocol, 259****L2TP (Layer 2 Tunneling Protocol), 259****lab environment simulations, WAN connectivity, 240-242****LAN Management Solution (LMS), 71****LANs (local area network)**

- logical LAN IP addressing schemes, 187-188
- logical networks design, 162
- prototypes, 218
 - creating test plans, 220-222*
 - identifying goals and requirements, 219*
 - identifying risks and weaknesses, 223-224*
 - IP addressing schemes, 223*
 - selecting routing protocols, 222-223*
 - validating devices, 222*

simulation, 228
 technologies, validating, 215-216
 topologies
 access layer, 158-160
 core layer, 161
 distribution layer, 160-161
 selecting, 158-162
 VLANs. *See* VLANs
 wireless controllers, 169
 WLANs. *See* WLANs

LAPs (lightweight access points), 169

large failure domains, 217

Layer 2, 131

Layer 2 Forwarding (L2F) protocol, 259

Layer 2 Tunneling Protocol (L2TP), 259

Layer 3
 functionality, 255-256
 QoS, 131

layers
 access, 3, 22-30, 158-160
 core, 3, 13-14, 161
 design, 9-11
 distribution, 3, 14-22, 160-161
 multilayer security, 11, 33
 three-layer hierarchies, simulating, 221-222

leading questions, 290

lifecycles, Cisco Lifecycle Services, 50-56

lightweight access points (LAPs), 169

limitations
 of bandwidth, 224
 of existing equipment, 159
 of fiber connectivity, 224
 of network simulation software, 239
 scalability, 217
 scope of network failure, 16-18

links
 backup
 configuring, 252-253
 WANs, 42-43
 DLCI, 247
 Frame Relay, 246
 primary, configuring, 253-256
 redundancy, 11, 15, 216
 core layer, 11

lists, hardware, 89

live on-demand video, 138

LMI (Local Management Interface), 248
 debugging, 254-255
 verifying, 254

LMS (LAN Management Solution), 71

load balancing, 11, 31
 EIGRP, 191
 EtherChannel configuration, 153
 testing, 217
 unequal-cost, 192

local loops, 246

Local Management Interface. *See* LMI

location

of VPN servers, 263
 of wireless APs, 170-171
 of wiring closets, 189-190
 of VPN servers, 257

logical architecture diagrams, 82-84

logical design, proposal, 270-271

logical LAN IP addressing schemes, 187-188

logical network design, 36

LANs, 162
 WANs, 167-168
 WLANs, 172-173

loops, local, 246

low latency queuing, 122

low-priority packets, 130

luxury restaurants, StadiumCompany network upgrade, 306

luxury skybox support, StadiumCompany network upgrade, 307

M

maintenance, planning, 276

manageability

networks, 3

management

2960 switches, 159
 access layers, 25
 account managers, role of, 61
 applications, 114
 characterization, 115-116
 hardware, 117-118
 performance, 114
 traffic flow, 116-117
 Cisco Lifecycle Services, 51
 convergence, 132
 CRM, 279
 design, 69
 monitoring, 70-73
 top-down approach/bottom-up approach, 69
 Distribution layer, 161
 documenting, 105
 Frame Relay connections, 244
 keys, 192-193
 LMI, 248
 network designers, role of, 62
 postsales field engineers, role of, 63
 presales systems engineers, role of, 61-62
 project software, 275
 proposals, assembling existing information, 270-271
 SAS (Software Application Support) services, 282
 SDM, 56
 security, monitoring, 154
 server farms, 227
 traffic, 129-130, 248
 VPN servers, 257
 wireless networks, 170

Management Information Base (MIB), 72

manual summarization, 194

mapping

- Frame Relay, 249-252
- network topologies, 81

market share, 65**marking QoS, 131****maximum-paths command, 191****MCUs (multipoint control units), 133****MD5 (Message Digest Algorithm Version 5), 192****measurement**

- of application performance, 114
- baselines, 227

medium-priority packets, 129**meetings, prebid, 59****memory**

- DRAM, 92
- flash, 92
- NVRAM, 94
- RAM, 92

mesh topologies, 11-12**Message Digest Algorithm Version 5 (MD5), 192****messages**

- hashes, adding to, 260
- keepalive, 248

methods

- installation, selecting, 273-275
- interviews, 290-291
- testing, selecting, 215

methodologies

- network design, 6-7, 9

MetroEthernets, 164**MIB (Management Information Base), 72****Microsoft domain services, 125-127****migrating from IPv4 to IPv6, 202****mitigation, 174****mobile workers, 39-43****mobility**

- IP, 199
- wireless networks, 168

modems, serial connectivity simulation, 241**modular block diagrams, 85-86****modular design**

- Cisco Enterprise Architectures, 5-6

modules

- adding. *See also* scalability, 6

modularity, network, 183**monitoring**

- connections, 248
- networks, 70-71, 73
- QoS, 130
- security, 154
- video, 156
- VLANs, 27

MPLS technology, 41**MS Visio, 140****multi-access WAN, 250****multicasting, 199****multilayer security, 33, 230****multilayer switches, 11, 160-161****multipoint control units (MCUs), 133****multipoint subinterfaces, 250-252**

N

naming

- files, 90
- guidelines, 198
- IP addressing schemes, 187-198
- schemes, designing, 197-198

NAT-PT (Network Address Translation-Protocol Translation), 202**NBAR (Network-Based Application Recognition), 116****NBMA (nonbroadcast multi-access), 250****neighbor authentication, 192****NetFlow, 116****netstat, 216****Network Address Translation-Protocol Translation (NAT-PT), 202****network command, 204****network designers, role of, 62****network interface cards (NICs), 214****Network Management System (NMS), 70****Network-Based Application Recognition (NBAR), 116****networks**

- applications, 114, 279
 - characterization, 115-116*
 - hardware, 117-118*
 - Microsoft domain services, 125-127*
 - performance, 114*
 - QoS, 27, 127-131*
 - traffic flow, 116-117*
 - types, 118-127*
- ATM, 40
- auditing, 116
- backbones, 9
- baselines, 56
- campus. *See* campus networks
- Cisco Enterprise Architectures, 5-6
- Cisco Lifecycle Services, 50-56
- complete replacements, 274
- convergence, 13
 - at access layers, 24*
 - managing, 132*
 - selecting routing protocols, 14*
- current network, 270-271
- design
 - access layer, 22-30, 158-160*
 - analyzing requirements, 150-158*
 - convergence, 14*
 - core layer, 9-11, 14, 161*
 - distribution layer, 14-22, 160-161*
 - documenting, 102-106*
 - existing network characterization, 107-108*
 - goals, 3*

- hierarchical*, 3, 5-6
- implementing*, 272
- IP addressing*, 182. *See also* *IP addressing*
- logical*, 162
- managing*, 69-73
- methodologies*, 6-7, 9
- overview of*, 2-3
- preparing for*, 63-66
- selecting LAN topologies*, 158-162
- topologies*, 7-9
- trade-offs*, 157-158
- wireless*, 168-173
- WLANs*, 172-173
- deterministic, 5
- diameter, 156
- discontiguous, 184
- edge
 - security at*, 28-29
 - services at*, 27
- existing
 - analyzing*, 7
 - creating diagrams*, 80-82
 - documentation*, 80
 - logical architecture diagrams*, 82-84
 - modular block diagrams*, 85-86
 - phased installations*, 273-274
 - strengths and weaknesses of*, 86-88
 - updating*, 88-94
 - upgrading*, 95-96
- FilmCompany, 313-314
- hosts per, 190
- logical design, 36
- media, HTTP, 124
- modularity, 183
- number of, 190
- physical
 - design*, 36
 - layout of*, 188
- redundancy, building at distribution layers, 18-19
- requirements, 2-3, 270-271
 - for performance*, 155-156
 - identifying*, 7
 - impacting a portion of*, 9
- security, 3, 173
 - placing functions and appliances*, 173-174
 - server farms*, 30-34
 - troubleshooting*, 29-30
- servers, relocating, 226
- simulation tools, 216
- stadium, installation methods, 274-275
- testing, 55
- topologies
 - access layers*, 26
 - mapping*, 81
- traffic
 - prioritization*, 12
- traffic prioritization, 13
- troubleshooting, 12
 - limiting scope of failure*, 16-18
 - reducing human error*, 13
- types, 190

- upgrading*, 55, 80
 - overcoming weaknesses*, 87-88
 - testing*, 91
- virtual*, 259
- VPNs, 42
- WANs, 39-43
- wireless design, 34-38
- wireless networks, 172. *See also* *wireless networks*
- wireless site surveys, 97
 - applying*, 100-101
 - physical network considerations*, 98-100
 - planning*, 100
 - visiting customer sites*, 97-98

new applications, 279

New Hardware Option (3.3.3), installing, 96

new installations, 273

NICs (network interface cards), 214

NMS (Network Management System), 70

no access-list command, 20

nonadjacent subnets, 184

nonbroadcast multi-access. *See* NBMA

nonhierarchical addressing, 183. *See also* hierarchical routing

nonvolatile random-access memory (NVRAM), 94

normal-priority packets, 130

notes, release, 93

nslookup, 216

number of networks, 190

NVRAM (nonvolatile random-access memory), 94

O

on-demand video, 138

online catalogs, 119

open guest access, 37

open-ended questions, 290

Open Shortest Path First. *See* OSPF, 11

Operate phase, 51

- case study, 56

operations, monitoring, 70-73

optimizing applications, 114

- characterization, 115-116

- hardware, 117-118

- traffic flow, 116-117

Optimize phase, 51

- case study, 56

options, VPN endpoints, 166-167

orders

- for tickets, 119

- transactions, 119

organizational input, 116

OSPF (Open Shortest Path First), 11

out-of-band, 159

P

Packet Tracer, 82

packets, file transfers, 123

partial-mesh topologies, 11-12

patterns, traffic, 18

defining, 165-166

PBX (Private Branch Exchange), 135

PCs (personal computers), StadiumCompany network upgrade, 304

Per VLAN Rapid Spanning Tree Plus (PVRST+), 228

performance

applications, 114
network simulation software, 240
network requirements, 155-156
pilot networks, creating, 213

permanent virtual circuits (PVCs), 165, 250

phased installations, 273-274

phases of Cisco Lifecycle Services, 50

phones, StadiumCompany network upgrade, 304

physical connections, 87

physical design proposals, 270-271

physical layout of networks, 188

physical networks, design, 36

physical security, 29. *See also* security

pilot networks, installing, 165, 212-213

creating test plans, 213
identifying design weaknesses, 217-218
redundancy and resiliency, 216
validating devices, 215-216
verifying goals and requirements, 214-215

ping, 216

placement

security functions and appliances, 173-174
of VPN servers, 263

Plan phase, 50-53

planning

downtime, 276
FilmCompany, 311-313
implementation, 270-273
 maintenance, 276
 selecting installation methods, 273-275
installation, 55, 276
 Cisco Focused Technical Support Services, 281-282
 creating bill-of-materials, 276-279
 SAS (Software Application Support) services, 282
 SMARTnet services, 280-281
IP addressing schemes, 183
LAN prototypes, testing, 220-222
networks, testing, 213
remote worker support, 257-258
server farms, testing, 226-227
StadiumCompany network upgrade, 308
WANs
 creating test plans, 242-245
 validating devices, 245-248
wireless site surveys, 100

PoE (Power-over-Ethernet), 23, 122

point-of-sale ticket machines, 114

point-to-point subinterfaces, 250

point-to-point T1, 164

Point-to-Point Tunneling Protocol (PPTP), 259

policies

defining, 56
QoS, 127
 implementation, 130-131
 prioritization, 129-130
 traffic queues, 128-129
routing, IP addressing, 189
security, 30, 189

ports. *See also* connections

disabling, 229
Microsoft domain services, 126
roles, 228

POST (Power-On Self Test), 94

postsales field engineers, role of, 63

power supplies, UPS, 13

Power-On Self-Test (POST), 94

Power-over-Ethernet (PoE), 23, 122

power requirements, 159

PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize), 150, 270

PPTP (Point-to-Point Tunneling Protocol), 259

PQ (priority queuing), 128

prebid meetings, 59

prefixes

addressees and summarization, 187
routing, 202

Prepare phase, 50-52

Prepare, Plan, Design, Implement, Operate, Optimize (PPDIOO), 150, 270

preparing for exams, 291

presales systems engineers, role of, 61-62

presenting proposals, 283-284

press area support, StadiumCompany network upgrade, 307

prevention

network failure, 12

primary links, configuring, 253-256

prioritization

business goals and, 65-66
QoS, 128
traffic, 12, 13
traffic management, 129-130

priority queuing (PQ), 128

Private Branch Exchange (PBX), 135

procedures, defining, 56

processing transactions, 156

profitability, 65

projects

constraints, 150
goals, 102-103
management, 275

- planning, 53
- sales process, 57-61
- scope, 7, 103-104
- proof-of-concept, 212**
- proposals, 57-58**
 - creating, 283-284
 - existing information, assembling, 270-271
 - logical design, 270-271
 - physical design, 270-271
 - TCO, 276
- protocols**
 - analyzers, 216
 - BPDUs, 228
 - EIGRP, 11, 222
 - HSRP, 120
 - HTTP, 124-125
 - Inverse ARP, 249-252
 - IPsec, 261
 - IS-IS, 21
 - L2F, 259
 - L2TP, 259
 - OSPF, 11
 - RIPv2, 185
 - routing
 - at distribution layers, 21-22
 - selecting, 14, 191-193
 - validating, 222-223
 - RSTP, 18, 120, 228, 230
 - RSTP+, 34
 - RTCP, 122
 - RTP, 122
 - SNMPv3, 70
 - STP, 11, 18
 - TFTP, 92
 - VPN tunnel, 259
- prototypes**
 - campus networks, 211-213
 - creating test plans, 213
 - identifying design weaknesses, 217-218
 - redundancy and resiliency, 216
 - validating devices, 215-216
 - verifying goals and requirements, 214-215
 - LANs, 218
 - creating test plans, 220-222
 - identifying goals and requirements, 219
 - identifying risks and weaknesses, 223-224
 - IP addressing schemes, 223
 - selecting routing protocols, 222-223
 - validating devices, 222
 - remote worker support, 256
 - connectivity, 261-262
 - creating test plans, 257-258
 - identifying risks and weaknesses, 264
 - placement of VPN servers, 263
 - validating devices, 259-260
 - VPN goals and requirements, 256-257
 - server farms, 224
 - creating test plans, 226-227
 - identifying goals and requirements, 225-226
 - identifying risks and weaknesses, 232
 - planning security, 230-231
 - validating devices, 228, 230

- WANs, 237-252
 - creating test plans, 242, 244-245
 - identifying risks and weaknesses, 256
 - lab environment simulations, 240-242
 - remote connections, 239
 - testing connections, 239
 - troubleshooting Frame Relay, 252-256
 - validating devices, 245-248

proxying, 202

PSTN (Public Switched Telephone Network), 136

PVCs (permanent virtual circuits), 165, 250

PVRST+ (Per VLAN Rapid Spanning Tree Plus), 228

Q

QoS (Quality of Service)

- applications, 114, 127
 - implementation, 130-131
 - prioritization, 129-130
 - traffic queues, 128-129
- AutoQoS, 130
- convergence, 132
- network applications, 27
- WANs, 40

quality of voice, 156

Quality of Service. *See* QoS

queries, customers, 119

question types (in interviews), 290

queuing

- low latency, 122
- types of, 128
- traffic, 128-129

quotes, 57-58

R

RAM (random-access memory), 92

random-access memory. *See* RAM

Rapid Spanning Tree Protocol (RSTP), 120

Rapid Spanning Tree Protocol Plus (RSTP+), 34

Rapid Spanning Tree Protocol. *See* RSTP

reachability

- of hosts, 188
- testing commands, 216

real-time streaming, voice, 121-122

Real-Time Transport Protocol (RTP), 122

Real-Time Transport Control Protocol (RTCP), 122

Received Signal Strength Indication (RSSI), 172

reduction of network diameter, 156

redundancy

- building in, 33
- co-located servers, 151
- HTTP, 125
- in mesh topologies, 12
- LAN prototypes, 223
- links, 11, 15, 216
 - core layer, 11

- networks, building at distribution layers, 18-19
- testing, 216
- in transaction processing, 120
- WANs, 42-43
- wireless networks, 172

reflexive ACLs, 20. *See also* ACLs

release notes, 93

relevant information, identifying, 64

reliability, 51

- for e-commerce, 154

relocation of servers, 226

remote access

- voice/video, 138-139
- VPNs, 259
- WANs, 40

remote connection prototypes, 239

- lab environment simulations, 240-242
- testing, 239

remote sites

- connections, determining, 163-165
- diagrams, 142-143
- support, StadiumCompany network upgrade, 307

remote worker support, 39-43

- connectivity, 261-262
- design, 163-168
- identifying risks and weaknesses, 264
- placement of VPN servers, 263
- prototypes, 256
 - creating test plans, 257-258*
 - VPN goals and requirements, 256-257*
- validating devices, 259-260

replacement

- of complete networks, 274
- of hardware, 280

reporting, QoS, 130

Request for Proposal (RFP), 57-59, 270

Request for Quote (RFQ), 57-61

requirements

- access layer, 158
- availability, 153-155
 - e-commerce, 154*
 - of server farms, 230*
- core layer, 161
- design, verifying, 214-215
- distribution layer, 160
- Frame Relay connections, 244
- IP telephony, 133, 135-136
- LAN prototypes, 219
- networks, 2-3, 270-271
 - analyzing, 150-158*
 - design, documenting, 102-106*
 - for performance, 155-156*
 - identifying, 7*
 - impacting a portion of, 9*
- power, 159
- for scalability, 152-153
- for security, 156-157
- server farms, 225-226
- technical, 7, 66-69
- VPNs, 256

reserved addresses, 202

resiliency

- testing, 216
- wireless networks, 172

resources, estimating, 275

response documents, 57-58

responsibilities, 61, 289

responsiveness of applications, 114

RFP (Request for Proposal), 57-59, 270

RFQ (Request for Quote), 57-61

RIPng, configuring and verifying, 204-205

RIPv2 (Routing Information Protocol version 2), 185

risks

- design, identifying, 217-218
- LAN prototypes, 223-224
- remote worker support, 264
- server farms, 232
- WANs, 256

Rivest, Shamir, and Adleman (RSA), 259

roles

- of account managers, 61
- of network designers, 62
- of presales systems engineers, 61-62
- of ports, 228
- of postsales field engineers, 63

root switches, 228

routed topologies, 222

routers

- applications, 117
- CPE, 244
- starting, 94

routes

- aggregation, 21-22
- information, obtaining information about, 81-82
- static, floating, 252
- summarization, 21-22, 183, 193-194

routing

- CIDR, 185-187
- distribution layer, 14
- hierarchical, 182-183
- HSRP, 120
- policies, IP addressing, 189
- prefixes, 202
- protocols, 11
 - at distribution layers, 21-22*
 - selecting, 14*
 - validating, 222-223*
- strategies, designating, 191-193

Routing Information Protocol version 2 (RIPv2), 185

RSA (Rivest, Shamir, and Adleman), 259

RSSI (Received Signal Strength Indication), 172

RSTP (Rapid Spanning Tree Protocol), 18, 120, 228-230

RSTP+ (Rapid Spanning Tree Protocol Plus), 34

RTCP (Real-Time Transport Control Protocol), 122

RTP (Real-Time Transport Protocol), 122

S

safety, wireless site surveys, 98

sales process, 57-63

sample topologies, testing, 221

SAN (storage-area networks), 32

SAS (Software Application Support) services, 282

satisfaction of customers, 65

scalability, 183

2960 switches, 159

Cisco Lifecycle Services, 51

Distribution layer, 160

documenting, 105

Frame Relay connections, 244

limitations of, 217

networks, 3

of network simulation software, 239

requirements for, 152-153

server farms, 226

wireless networks, 170

scheduling downtime and maintenance, 276

schemes

addressing, 182-183

IP addressing

naming, 187-198

validating, 223

naming, designing, 197-198

scope

of network failure, limiting, 16-18

of projects, 103-104

of projects, identifying, 7

SDM (Security Device Manager), 56

searching, job searches, 289-291

Secure Shell (SSH), 30

Secure Sockets Layer (SSL), 143

security

2960 switches, 159

ACLs, implementing, 175

Cisco Lifecycle Services, 51

connections, 174

devices, 30

distribution layer, 161

documenting, 105

employee access, 37

Frame Relay connections, 244

HTTP, 125

IDS, 85

infrastructure, 173

internal attacks, 33

IP, 199

monitoring, 154

multilayer, 33

networks, 3, 173

edge, 28-29

placing functions and appliances, 173-174

troubleshooting, 29-30

physical, 29

policies, 30

IP addressing, 189

requirements for, 156-157

server farms, 30-34, 227-231

services, 174

transaction processing, 121

VPNs, 257

WANs, 40

wireless networks, 170

wireless site surveys, 98

Security Device Manager (SDM), 56

segment diagrams, creating network, 83

segregation, VLANs, 26-27

selection

of Cisco IOS versions, 91-92

of installation methods, 273-275

of LAN topologies, 158-162

Access layer, 158-160

Core layer, 161

Distribution layer, 160-161

of pilot or prototype networks, 212-213

of routing protocols, 14, 191-193, 222-223

of server farms, validating devices and topologies, 228, 230

of testing methods, 215

send-lifetime command, 192

serial connectivity, simulating, 241-242

servers

applications, 133

co-located, 151

e-mail, 124

farms, 5

creating test plans, 226-227

identifying goals and requirements, 225-226

identifying risks and weaknesses, 232

planning security, 230-231

security, 30-34

validating devices, 228-230

prototypes, 224

relocation, 226

TFTP, 92

VPNs

locations, 257

managing, 257

placement of, 263

service level agreements (SLAs), 40

service set identifier (SSID), 37

services

adding, 6

applications, 114

characterization, 115-116

hardware, 117-118

performance, 114

traffic flow, 116-117

Cisco Focused Technical Support Services, 281-282

Cisco Lifecycle Services, 50-56

contracts, 280

delivering, 289

domain network applications, 125-127

integrated, applying, 174

network edge, 27

remote locations, extending, 163

SAS (Software Application Support) services, 282

security, 174

SMARTnet, 280-281

sharing files, 115

show cdp neighbors command, 214

show cdp neighbors detail command, 82, 151

show commands, 81, 214-215, 250

show frame-relay lmi command, 251, 254

show frame-relay map command, 251

show frame-relay pvc command, 253

show frame-relay pvc [interface interface] [dlci] command, 251

show interface serial command, 253-254

show interfaces serial command, 250

show ip arp command, 214

show ipv6 rip command, 204

show ipv6 route rip command, 204

show tech-support command, 81

show version command, 89-90

Simple Network Management Protocol version 3 (SNMPv3), 70

simulation, 216

lab environment simulations, 240-242

LANs, 228

serial connectivity, 241-242

three-layer hierarchies, 221-222

WAN connectivity, testing, 239

single points of failure, 217

site-to-site VPNs, 259

skills, interpersonal, 63-64

SLAs (service level agreements), 40

SMARTnet services, 280-281

SNMPv3 (Simple Network Management Protocol version 3), 70

software

Cisco Focused Technical Support Services, 281-282

Cisco IOS, installing, 92-93

CRM, 279

project management, 275

queues, 128

SAS (Software Application Support) services, 282

SMARTnet services, 280-281

telephones, 133

WAN connectivity, testing, 239

Software Application Support (SAS) services, 282

Spanning Tree Protocol (STP), 11, 18

specialized applications, 279

split horizons, 250

split tunnels, 261-262

spoofed, 230

SSH (Secure Shell), 30

SSID (service set identifier), 37

SSL (Secure Sockets Layer), 143

stability, 183

stadium networks

design, implementing, 272-273

installation methods, 274-275

StadiumCompany network upgrade story, 303-304

organization, 304

concession vendors, 306

existing facilities and support, 304

luxury restaurants, 306

luxury skybox support, 307

phones and PCs, 304

press area support, 307

remote site support, 307

Team A, 305

Team B, 306

visiting team support, 306

planning, 308

staff capabilities, existing, 217

standard warranties, 280

star topologies, 26

starting routers, 94

static routes, floating, 252

status, checking Frame Relay interface, 253

storage networking, 8

storage-area networks (SAN), 32

STP (Spanning Tree Protocol), 11, 18

strategies, designating routing, 191-193

streaming video, 138

QoS, 127

strengths of existing networks, 86-88

strings, cipher, 259

subinterfaces, 250

multipoint, 250-252

point-to-point, 250

subnetting

classful, 184-185

with VSLM, 185

summaries, executive, 270-271

summarization

automatic, disabling, 185

CIDR and, 186-187

classful subnets and, 184-185

prefix addresses and, 187

routes, 21-22, 183, 193-194

supernetting, 21-22, 186

support

applications, defining, 165-166

Cisco Focused Technical Support Services, 281-282

StadiumCompany network upgrade, 304

surveys, wireless site, 97

applying, 100-101

physical network considerations, 98-100

planning, 100

visiting customer sites, 97-98

SVCs (switched virtual circuits), 165

switch block deployment, 17

switched virtual circuits (SVCs), 165

switches

2960, 159

applications, 118

blocks, 160

- high-capacity, 31
- multilayer, 11, 160-161
- root, 228
- upgrading, 279

system-level acceptance testing, 55

T

T1 connections, 244

TCO (total cost of ownership), 276

Team A organization, StadiumCompany network upgrade, 305

Team B organization, StadiumCompany network upgrade, 306

team offices, VPN requirements, 256

team scout support, 257

technical requirements, 7, 66

- analyzing, 150-152
- core layers, 11
- defining, 66-69
- documenting, 104-106
- IP telephony, 133-136

technologies, validating LAN, 215-216

telecommunications service provider (TSP), 164, 241

telnet, 216

testing

- ACLs, 231
- campus networks, 212-213
 - creating test plans, 213*
 - identifying design weaknesses, 217-218*
 - redundancy and resiliency, 216*
 - validating devices, 215-216*
 - verifying goals and requirements, 214-215*
- connections, 214
- functionality, 213-215
- LAN prototypes, 220-222
 - identifying risks and weaknesses, 223-224*
 - IP addressing schemes, 223*
 - selecting routing protocols, 222-223*
 - validating devices, 222*
- load balancing, 217
- methods, selecting, 215
- networks, 55, 91
- POST, 94
- proof-of-concept, 212
- redundancy, 222
- remote worker support, 257-258
- sample topologies, 221
- server farms, 226-227
- WANs
 - connectivity, 239-242*
 - creating test plans, 242-245*
 - validating devices, 245-248*

TFTP (Trivial File Transfer Protocol), 92

threats, detection, 174

three-layer hierarchies, simulating, 221-222

tickets, 119

time, convergence, 14

time-based ACLs, 20-12. *See also* ACLs

timelines, estimating, 275

tools

- for network monitoring, 72-73
- IP, 216
- NBAR, 116
- network simulation, 216

top-down approach, 7-9, 69

topologies

- distribution layer, 16
- FilmCompany, 313-314
- flat, 222
- full-meshed, 26
- LANs
 - access layer, 158-160*
 - core layer, 161*
 - distribution layer, 160-161*
 - selecting, 158-162*
- mesh, 11-12
- networks
 - access layers, 26*
 - design, 7-9*
 - mapping, 81*
- routed, 222
- server farms, 228, 230
- star, 26
- testing, 221
- VPNs
 - server tests, 264*
 - validating, 259-260*

WANs, validating, 245-248

WLANS, 34

ToS (type of service), 131

total cost of ownership (TCO), 276

traceroute, 216

tracert, 216

trade-offs in network design, 151-158

traditional telephony, 135. *See also* IP telephony

traffic

- analysis, 116
- classification, 28
- control, 139
- external, 117
- file transfer, 123-124
- filtering at distribution layers, 19-21
- flow, 139-140
 - applications, 116-117*
 - external traffic diagrams, 143-144*
 - internal traffic diagrams, 140-141*
 - remote site diagrams, 142-143*
- Frame Relay, managing, 248
- internal, 117
- isolating, 133
- management, 129-130
- patterns, 18, 165-166
- prioritization, 12-13
- queues, 128-129
- VLANs, 26-27

traffic. *See also* networks, 5

transaction-processing applications, 119-121

transactions, processing, 156

transfers, files, 123-124

translation, 202

transmit power control, 170

transmit queue (TxQ), 128

Triple DES (3DES), 259

Trivial File Transfer Protocol (TFTP), 92

Trojan horses, 28

troubleshooting, 217

application performance, 114

Frame Relay, 252-256

ISPs, 223

networks, 12

limiting scope of failure, 16-18

reducing human error, 13

security, 29-30

RSTP, 228, 230

trunks, distribution layer, 15

TSP (telecommunications service provider), 164, 241

tunnels, 121, 259

split, 261-262

transition methods, 202

VPN protocols, 259

TxQ (transmit queue), 128

type of service (ToS), 131

types

of antennas, 99

of Frame Relay connections, 165

of IP addresses, 201

of network applications, 118-127

of networks, 190

of queuing, 128

of VLANs, 190

U

unauthorized access, physical security, 29

unequal-cost, load balancing, 192

unicast addresses, 201-202

unified wireless and wired solutions, 168-170

uninterruptible power supply. *See* UPS

updating

databases, 119

design documentation, 175-176

existing networks, 88-94

upgrading

existing networks, 95-96

networks, 55, 80

overcoming weaknesses, 87-88

testing, 91

switches, 279

UPS (uninterruptible power supply), 13

users

access, adding, 65

documenting, 106

identifying, 64

utilities

IP, 216

NBAR, 116

V

V.35 cables, serial connectivity simulation, 241-242

validation

devices, 215-216, 222

IP addressing schemes, 223

routing protocols, 222-223

security, 230-231

server farms, 228, 230

VPNs, 259-260

Variable Length Subnet Mask. *See* VLSM

variance command, 192

verification

connections, 214

design goals and requirements, 214-215

LMI, 254

PVRST+, 228

RIPng, 204-205

versions

selecting, 91-92

show version command, 89-90

video, 131

convergence, 131-136

distribution, 156

endpoints, 133

monitoring, 156

QoS, 127

real-time protocols, 122

remote access, 138-139

streaming, 138

videoconference systems, 115

Video on Demand (VoD), 138

viewing PVRST+, 228

virtual LANs. *See* VLANs

virtual networks, 259

virtual private networks. *See* VPNs

virtualization, 34

viruses, 28

Visio (MS), 140

visiting team support, StadiumCompany network upgrade, 306

VLANs (virtual LANs), 26

benefits of separate, 134

traffic, 26-27

types of, 190

VLSM (Variable Length Subnet Mask), 185

VoD (Video on Demand), 138

voice, 131

convergence, 131-136

quality, 156

real-time streaming, 121-122

remote access, 138-139

Voice over IP. *See* VoIP

voice/WAN interface cards (VWICs), 95

VoIP (Voice over IP), 122, 136

VPNs (virtual private networks), 9

- Cisco EasyVPN, 258
- components, 259-260
- concentrators, 259
- endpoints, customizing, 166-167
- goals and requirements, 256-257
- remote-access, 259
- security, 157, 257
- server locations, 257
- servers
 - managing, 257*
 - placement of, 263*
- site-to-site, 259
- tunnel protocols, 259
- WAN connectivity prototypes, 242

VWICs (voice/WAN interface cards), 95

W-X-Y-Z

WAN interface cards (WICs), 95

WANs (wide-area networks), 39-43, 82

- bandwidth limitations, 224
- connections, adding, 164-165
- design, 163-168
- multi-access, 250
- prototypes, 237, 242, 249-252
 - creating test plans, 242-245*
 - identifying risks and weaknesses, 256*
 - lab environment simulations, 240-242*
 - remote connections, 239*
 - testing connections, 239*
 - troubleshooting Frame Relay, 252-256*
 - validating devices, 245-248*

WAPs (wireless access points), 84

warranties, 280

weaknesses

- design, identifying, 217-218
- LAN prototypes, 223-224
- remote worker support, 264
- server farms, 232
- WANs, 256

weaknesses of existing networks, 86-88

WEP (Wired Equivalent Privacy), 37

Wi-Fi Protected Access (WPA), 37

WICs (WAN interface cards), 95

wide-area networks. *See* WANs

windows, planning maintenance, 276

Wired Equivalent Privacy (WEP), 37

wireless access points. *See* WAPs

wireless LANs. *See* WLANs

wireless networks

- APs, locating, 170-171
- design, 34-38, 168-173
 - coverage options and mobility, 168*
 - unified wireless and wired solutions, 168-170*
- redundancy, 172
- resiliency, 172

wireless site surveys, 97

- applying, 100-101
- customer sites, visiting, 97-98
- physical network considerations, 98-100
- planning, 100

wiring closets, 23, 29

- location and description, 189-190

WLANs (wireless LANs), 34, 172-173

worms, 28

WPA (Wi-Fi Protected Access), 37

zero CIR, 247