



Course Booklet

Scaling Networks

Version 6

Scaling Networks v6 Course Booklet

Copyright © 2017 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 May 2017

Library of Congress Control Number: 2017936409

ISBN-13: 978-1-58713-430-2

ISBN-10: 1-58713-430-6

Warning and Disclaimer

This book is designed to provide information about Cisco Networking Academy Scaling Networks 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 author and are not necessarily those of Cisco Systems, Inc.

Editor-in-Chief

Mark Taub

Alliances Manager,

Cisco Press

Ron Fligge

Executive Editor

Mary Beth Ray

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Editorial Assistant

Vanessa Evans

Cover Designer

Chuti Prasertsith

Indexer

Erika Millen

Composition

codeMantra

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.netacad.com



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.

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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Reader Services

Register your copy at www.ciscopress.com/title/9781587134302 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587134302 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

Contents at a Glance

Chapter 1	LAN Design	1
Chapter 2	Scaling VLANs	15
Chapter 3	STP	39
Chapter 4	EtherChannel and HSRP	69
Chapter 5	Dynamic Routing	87
Chapter 6	EIGRP	109
Chapter 7	EIGRP Tuning and Troubleshooting	145
Chapter 8	Single-Area OSPF	165
Chapter 9	Multiarea OSPF	195
Chapter 10	OSPF Tuning and Troubleshooting	209
	Index	231

Contents

Chapter 1 LAN Design 1

1.0 Introduction to LAN Design 1

1.0.1.2 Class Activity - Network by Design 1

1.1 Campus Wired LAN Designs 2

1.1.1 Cisco Validated Designs 2

1.1.1.1 The Need to Scale the Network 2

1.1.1.2 Hierarchical Design Model 2

1.1.2 Expanding the Network 3

1.1.2.1 Design for Scalability 3

1.1.2.2 Planning for Redundancy 4

1.1.2.3 Failure Domains 4

1.1.2.4 Increasing Bandwidth 5

1.1.2.5 Expanding the Access Layer 5

1.1.2.6 Fine-tuning Routing Protocols 5

1.1.2.7 Activity - Identify Scalability Terminology 6

1.2 Selecting Network Devices 6

1.2.1 Switch Hardware 6

1.2.1.1 Switch Platforms 6

1.2.1.2 Port Density 7

1.2.1.3 Forwarding Rates 7

1.2.1.4 Power over Ethernet 8

1.2.1.5 Multilayer Switching 8

1.2.1.6 Activity - Selecting Switch Hardware 8

1.2.1.7 Packet Tracer - Comparing 2960 and 3560 Switches 8

1.2.2 Router Hardware 9

1.2.2.1 Router Requirements 9

1.2.2.2 Cisco Routers 9

1.2.2.3 Router Hardware 10

1.2.2.4 Activity - Identify the Router Category 10

1.2.3 Managing Devices 10

1.2.3.1 Managing IOS Files and Licensing 10

1.2.3.2 In-Band versus Out-of-Band Management 10

1.2.3.3 Basic Router CLI Commands 11

1.2.3.4 Basic Router Show Commands 11

1.2.3.5 Basic Switch CLI commands 12

1.2.3.6 Basic Switch Show Commands 12

1.3 Summary 12

1.3.1.1 Class Activity - Layered Network Design Simulation 12

1.3.1.2 Basic Switch Configuration 13

1.3.1.3 Packet Tracer - Skills Integration Challenge 13

1.3.1.4 Summary 13

Chapter 1 Quiz 14

Chapter 1 Exam 14

Your Chapter Notes 14

Chapter 2 Scaling VLANs 15

2.0 Introduction 15

2.0.1 Welcome 15

2.1 VTP, Extended VLANs, and DTP 15

- 2.1.1 VTP Concepts and Operation 15
 - 2.1.1.1 VTP Overview 15
 - 2.1.1.2 VTP Modes 16
 - 2.1.1.3 VTP Advertisements 17
 - 2.1.1.4 VTP Versions 17
 - 2.1.1.5 Default VTP configuration 18
 - 2.1.1.6 VTP Caveats 19
 - 2.1.1.7 Identify VTP Concepts and Operations 20
- 2.1.2 VTP Configuration 20
 - 2.1.2.1 VTP Configuration Overview 20
 - 2.1.2.2 Step 1 - Configure the VTP Server 20
 - 2.1.2.3 Step 2 - Configure the VTP Domain Name and Password 20
 - 2.1.2.4 Step 3 - Configure the VTP Clients 21
 - 2.1.2.5 Step 4 - Configure VLANs on the VTP Server 21
 - 2.1.2.6 Step 5 - Verify that the VTP Clients Have Received the New VLAN Information 21
- 2.1.3 Extended VLANs 21
 - 2.1.3.1 VLAN Ranges on Catalyst Switches 21
 - 2.1.3.2 Creating a VLAN 22
 - 2.1.3.3 Assigning Ports to VLANs 23
 - 2.1.3.4 Verifying VLAN Information 23
 - 2.1.3.5 Configuring Extended VLANs 24
- 2.1.4 Dynamic Trunking Protocol 24
 - 2.1.4.1 Introduction to DTP 24
 - 2.1.4.2 Negotiated Interface Modes 25
 - 2.1.4.3 Activity - Predict DTP Behavior 25
 - 2.1.4.4 Packet Tracer - Configure VTP and DTP 25
 - 2.1.4.5 Lab - Configure Extended VLANs, VTP and DTP 26

2.2 Troubleshoot Multi-VLAN Issues 26

- 2.2.1 Inter-VLAN configuration issues 26
 - 2.2.1.1 Deleting VLANs 26
 - 2.2.1.2 Switch Port Issues 26
 - 2.2.1.3 Verify Switch Configuration 27
 - 2.2.1.4 Interface Issues 27
 - 2.2.1.5 Verify Routing Configuration 28
- 2.2.2 IP Addressing Issues 28
 - 2.2.2.1 Errors with IP Addresses and Subnet Masks 28
 - 2.2.2.2 Verifying IP Address and Subnet Mask Configuration Issues 29
 - 2.2.2.3 Activity - Identify the Troubleshooting Command for an Inter-VLAN Routing Issue 29
 - 2.2.2.4 Packet Tracer - Troubleshooting Inter-VLAN Routing 29
 - 2.2.2.5 Lab - Troubleshooting Inter-VLAN Routing 30
- 2.2.3 VTP and DTP Issues 30
 - 2.2.3.1 Troubleshoot VTP Issues 30
 - 2.2.3.2 Troubleshoot DTP Issues 31
 - 2.2.3.3 Packet Tracer - Troubleshoot VTP and DTP Issues 31

2.3 Layer 3 Switching 31

- 2.3.1 Layer 3 Switching Operation and Configuration 31
 - 2.3.1.1 Introduction to Layer 3 Switching 31

2.3.1.2	<i>Inter-VLAN Routing with Switch Virtual Interfaces</i>	32
2.3.1.3	<i>Inter-VLAN Routing with Switch Virtual Interfaces (Cont.)</i>	32
2.3.1.4	<i>Inter-VLAN Routing with Routed Ports</i>	33
2.3.1.5	<i>Packet Tracer - Configure Layer 3 Switching and Inter-VLAN routing</i>	34
2.3.2	<i>Troubleshoot Layer 3 Switching</i>	34
2.3.2.1	<i>Layer 3 Switch Configuration Issues</i>	34
2.3.2.2	<i>Example: Troubleshooting Layer 3 Switching</i>	34
2.3.2.3	<i>Activity - Troubleshoot Layer 3 Switching Issues</i>	35
2.4	Summary	35
2.4.1.1	<i>Conclusion</i>	35
Chapter 2 Quiz 37		
Chapter 2 Exam 37		
Your Chapter Notes 37		
 Chapter 3 STP 39		
3.0	LAN Redundancy	39
3.0.1	<i>Introduction</i>	39
3.0.1.2	<i>Class Activity - Stormy Traffic</i>	39
3.1	Spanning Tree Concepts	40
3.1.1	<i>Purpose of Spanning Tree</i>	40
3.1.1.1	<i>Redundancy at OSI Layers 1 and 2</i>	40
3.1.1.2	<i>Issues with Layer 1 Redundancy: MAC Database Instability</i>	41
3.1.1.3	<i>Issues with Layer 1 Redundancy: Broadcast Storms</i>	42
3.1.1.4	<i>Issues with Layer 1 Redundancy: Duplicate Unicast Frames</i>	42
3.1.1.5	<i>Packet Tracer - Examining a Redundant Design</i>	43
3.1.2	<i>STP Operation</i>	43
3.1.2.1	<i>Spanning Tree Algorithm: Introduction</i>	43
3.1.2.2	<i>Spanning Tree Algorithm: Port Roles</i>	45
3.1.2.3	<i>Spanning Tree Algorithm: Root Bridge</i>	46
3.1.2.4	<i>Spanning Tree Algorithm: Root Path Cost</i>	46
3.1.2.5	<i>Port Role Decisions for RSTP</i>	47
3.1.2.6	<i>Designated and Alternate Ports</i>	48
3.1.2.7	<i>802.1D BPDU Frame Format</i>	49
3.1.2.8	<i>802.1D BPDU Propagation and Process</i>	49
3.1.2.9	<i>Extended System ID</i>	50
3.1.2.10	<i>Activity - Identify 802.1D Port Rules</i>	52
3.1.2.11	<i>Video Demonstration - Observing Spanning Tree Protocol Operation</i>	52
3.1.2.12	<i>Lab - Building a Switched Network with Redundant Links</i>	52
3.2	Varieties of Spanning Tree Protocols	52
3.2.1	<i>Overview</i>	52
3.2.1.1	<i>Types of Spanning Tree Protocols</i>	52
3.2.1.2	<i>Characteristics of the Spanning Tree Protocols</i>	53
3.2.1.3	<i>Activity - Identify Types of Spanning Tree Protocols</i>	54
3.2.2	<i>PVST+</i>	54
3.2.2.1	<i>Overview of PVST+</i>	54
3.2.2.2	<i>Port States and PVST+ Operation</i>	55
3.2.2.3	<i>Extended System ID and PVST+ Operation</i>	56
3.2.2.4	<i>Activity - Identifying PVST+ Operation</i>	56

- 3.2.3 Rapid PVST+ 56
 - 3.2.3.1 *Overview of Rapid PVST+* 56
 - 3.2.3.2 *RSTP BPDUs* 57
 - 3.2.3.3 *Edge Ports* 58
 - 3.2.3.4 *Link Types* 58
 - 3.2.3.5 *Activity - Identify Port Roles in Rapid PVST+* 59
 - 3.2.3.6 *Activity - Compare PVST+ and Rapid PVST+* 59

3.3 Spanning Tree Configuration 59

- 3.3.1 PVST+ Configuration 59
 - 3.3.1.1 *Catalyst 2960 Default Configuration* 59
 - 3.3.1.2 *Configuring and Verifying the Bridge ID* 59
 - 3.3.1.3 *PortFast and BPDU Guard* 60
 - 3.3.1.4 *PVST+ Load Balancing* 60
 - 3.3.1.5 *Packet Tracer - Configuring PVST+* 61
- 3.3.2 Rapid PVST+ Configuration 62
 - 3.3.2.1 *Spanning Tree Mode* 62
 - 3.3.2.2 *Packet Tracer - Configuring Rapid PVST+* 62
 - 3.3.2.3 *Lab - Configuring Rapid PVST+, PortFast and BPDU Guard* 63
- 3.3.3 STP Configuration Issues 63
 - 3.3.3.1 *Analyzing the STP Topology* 63
 - 3.3.3.2 *Expected Topology versus Actual Topology* 63
 - 3.3.3.3 *Overview of Spanning Tree Status* 63
 - 3.3.3.4 *Spanning Tree Failure Consequences* 64
 - 3.3.3.5 *Repairing a Spanning Tree Problem* 64
 - 3.3.3.6 *Activity - Troubleshoot STP Configuration Issues* 65
- 3.3.4 Switch Stacking and Chassis Aggregation 65
 - 3.3.4.1 *Switch Stacking Concepts* 65
 - 3.3.4.2 *Spanning Tree and Switch Stacks* 65
 - 3.3.4.3 *Activity - Identify Switch Stacking Concepts* 66

3.4 Summary 66

- 3.4.1.1 *Class Activity - Documentation Tree* 66
- 3.4.1.2 *Summary* 66

Chapter 3 Quiz 68

Chapter 3 Exam 68

Your Chapter Notes 68

Chapter 4 EtherChannel and HSRP 69

4.0 Introduction 69

- 4.0.1.2 *Class Activity - Imagine This* 69

4.1 Link Aggregation Concepts 70

- 4.1.1 Link Aggregation 70
 - 4.1.1.1 *Introduction to Link Aggregation* 70
 - 4.1.1.2 *Advantages of EtherChannel* 70
- 4.1.2 EtherChannel Operation 71
 - 4.1.2.1 *Implementation Restrictions* 71
 - 4.1.2.2 *Port Aggregation Protocol* 71
 - 4.1.2.3 *Link Aggregation Control Protocol* 73
 - 4.1.2.4 *Activity - Identify the PAgP and LACP Modes* 73

4.2 Link Aggregation Configuration 73

- 4.2.1 Configuring EtherChannel 73
 - 4.2.1.1 Configuration Guidelines 73
 - 4.2.1.2 Configuring Interfaces 74
 - 4.2.1.3 Packet Tracer - Configuring EtherChannel 75
 - 4.2.1.4 Lab - Configuring EtherChannel 75
- 4.2.2 Verifying and Troubleshooting EtherChannel 75
 - 4.2.2.1 Verifying EtherChannel 75
 - 4.2.2.2 Troubleshooting EtherChannel 76
 - 4.2.2.3 Packet Tracer - Troubleshooting EtherChannel 76
 - 4.2.2.4 Lab - Troubleshooting EtherChannel 77

4.3 First Hop Redundancy Protocols 77

- 4.3.1 Concept of First Hop Redundancy Protocols 77
 - 4.3.1.1 Default Gateway Limitations 77
 - 4.3.1.2 Router Redundancy 77
 - 4.3.1.3 Steps for Router Failover 78
 - 4.3.1.4 Activity - Identify FHRP Terminology 78
 - 4.3.1.5 First Hop Redundancy Protocols 78
 - 4.3.1.6 Activity - Identify the Type of FHRP 79
- 4.3.2 HSRP Operations 79
 - 4.3.2.1 HSRP Overview 79
 - 4.3.2.2 HSRP Versions 80
 - 4.3.2.3 HSRP Priority and Preemption 80
 - 4.3.2.4 HSRP States and Timers 81
 - 4.3.2.5 Activity - Identify HSRP Terminology and States 81
- 4.3.3 HSRP Configuration 81
 - 4.3.3.1 HSRP Configuration Commands 81
 - 4.3.3.2 HSRP Sample Configuration 81
 - 4.3.3.3 HSRP Verification 82
 - 4.3.3.4 Lab - Configure HSRP 82
- 4.3.4 HSRP Troubleshooting 82
 - 4.3.4.1 HSRP Failure 82
 - 4.3.4.2 HSRP Debug Commands 82
 - 4.3.4.3 Common HSRP Configuration Issues 83
 - 4.3.4.4 Packet Tracer - Troubleshoot HSRP 83

4.4 Summary 84

- 4.4.1.1 Class Activity - Linking Up 84
- 4.4.1.2 Packet Tracer - Skills Integration Challenge 84
- 4.4.1.3 Summary 84

Chapter 4 Quiz 86

Chapter 4 Exam 86

Your Chapter Notes 86

Chapter 5 Dynamic Routing 87

5.0 Introduction 87

- 5.0.1.1 Dynamic Routing 87
- 5.0.1.2 How Much Does This Cost 87

5.1 Dynamic Routing Protocols 88

- 5.1.1 Types of Routing Protocols 88
 - 5.1.1.1 Classifying Routing Protocols 88

5.1.1.2	<i>IGP and EGP Routing Protocols</i>	89
5.1.1.3	<i>Distance Vector Routing Protocols</i>	90
5.1.1.4	<i>Link-State Routing Protocols</i>	90
5.1.1.5	<i>Classful Routing Protocols</i>	91
5.1.1.6	<i>Classless Routing Protocols</i>	92
5.1.1.7	<i>Routing Protocol Characteristics</i>	92
5.1.1.8	<i>Routing Protocol Metrics</i>	93
5.1.1.9	<i>Activity - Classify Dynamic Routing Protocols</i>	94
5.1.1.10	<i>Activity - Compare Routing Protocols</i>	94
5.1.1.11	<i>Activity - Match the Metric to the Protocol</i>	94

5.2 Distance Vector Dynamic Routing 94

5.2.1	Distance Vector Fundamentals	94
5.2.1.1	<i>Dynamic Routing Protocol Operation</i>	94
5.2.1.2	<i>Cold Start</i>	94
5.2.1.3	<i>Network Discovery</i>	95
5.2.1.4	<i>Exchanging the Routing Information</i>	96
5.2.1.5	<i>Achieving Convergence</i>	97
5.2.1.6	<i>Packet Tracer - Investigating Convergence</i>	97
5.2.2	Distance Vector Routing Protocol Operation	97
5.2.2.1	<i>Distance Vector Technologies</i>	97
5.2.2.2	<i>Distance Vector Algorithm</i>	98
5.2.2.3	<i>Activity - Identify Distance Vector Terminology</i>	98
5.2.3	Types of Distance Vector Routing Protocols	98
5.2.3.1	<i>Routing Information Protocol</i>	98
5.2.3.2	<i>Enhanced Interior-Gateway Routing Protocol</i>	99
5.2.3.3	<i>Activity - Compare RIP and EIGRP</i>	100
5.2.3.4	<i>Packet Tracer - Comparing RIP and EIGRP Path Selection</i>	100

5.3 Link-State Dynamic Routing 100

5.3.1	Link-State Routing Protocol Operation	100
5.3.1.1	<i>Shortest Path First Protocols</i>	100
5.3.1.2	<i>Dijkstra's Algorithm</i>	100
5.3.1.3	<i>SPF Example</i>	101
5.3.2	Link-State Updates	101
5.3.2.1	<i>Link-State Routing Process</i>	101
5.3.2.2	<i>Link and Link-State</i>	102
5.3.2.3	<i>Say Hello</i>	103
5.3.2.4	<i>Building the Link-State Packet</i>	103
5.3.2.5	<i>Flooding the LSP</i>	103
5.3.2.6	<i>Building the Link-State Database</i>	104
5.3.2.7	<i>Building the SPF Tree</i>	104
5.3.2.8	<i>Adding OSPF Routes to the Routing Table</i>	105
5.3.2.9	<i>Activity - Building the Link-State Database and SPF Tree</i>	105
5.3.3	Link-State Routing Protocol Benefits	105
5.3.3.1	<i>Why Use Link-State Protocols?</i>	105
5.3.3.2	<i>Disadvantages of Link-State Protocols</i>	105
5.3.3.3	<i>Protocols that Use Link-State</i>	106

5.4 Summary 107

5.4.1	Conclusion	107
-------	------------	-----

Chapter 5 Quiz 108

Chapter 5 Exam 108

Your Chapter Notes 108

Chapter 6 EIGRP 109

6.0 Introduction 109

6.0.1 Welcome 109

6.0.1.2 Class Activity - Classless EIGRP 109

6.1 EIGRP Characteristics 109

6.1.1 EIGRP Basic Features 109

6.1.1.1 Features of EIGRP 109

6.1.1.2 Protocol Dependent Modules 111

6.1.1.3 Reliable Transport Protocol 111

6.1.1.4 Authentication 112

6.1.2 EIGRP Packet Types 112

6.1.2.1 EIGRP Packet Types 112

6.1.2.2 EIGRP Hello Packets 113

6.1.2.3 EIGRP Update and Acknowledgment Packets 113

6.1.2.4 EIGRP Query and Reply Packets 114

6.1.2.5 Activity - Identify the EIGRP Packet Type 115

6.1.2.6 Video Demonstration - Observing EIGRP Protocol Communications 115

6.1.3 EIGRP Messages 115

6.1.3.1 Encapsulating EIGRP Messages 115

6.1.3.2 EIGRP Packet Header and TLV 115

6.2 Implement EIGRP for IPv4 116

6.2.1 Configure EIGRP with IPv4 116

6.2.1.1 EIGRP Network Topology 116

6.2.1.2 Autonomous System Numbers 116

6.2.1.3 The router eigrp Command 117

6.2.1.4 EIGRP Router ID 118

6.2.1.5 Configuring the EIGRP Router ID 118

6.2.1.6 The network Command 119

6.2.1.7 The network Command and Wildcard Mask 120

6.2.1.8 Passive Interface 121

6.2.2 Verify EIGRP with IPv4 122

6.2.2.1 Verifying EIGRP: Examining Neighbors 122

6.2.2.2 Verifying EIGRP: show ip protocols Command 122

6.2.2.3 Verifying EIGRP: Examine the IPv4 routing table 123

6.2.2.4 Packet Tracer - Configuring Basic EIGRP with IPv4 124

6.2.2.5 Lab - Configuring Basic EIGRP with IPv4 124

6.3 EIGRP Operation 125

6.3.1 EIGRP Initial Route Discovery 125

6.3.1.1 EIGRP Neighbor Adjacency 125

6.3.1.2 EIGRP Topology Table 125

6.3.1.3 EIGRP Convergence 126

6.3.1.4 Activity - Identify the Steps in Establishing EIGRP Neighbor Adjacencies 126

6.3.2 EIGRP Metrics 126

6.3.2.1 EIGRP Composite Metric 126

6.3.2.2 Examining Interface Metric Values 127

6.3.2.3 Bandwidth Metric 128

6.3.2.4 Delay Metric 128

6.3.2.5 How to Calculate the EIGRP Metric 129

6.3.2.6	<i>Calculating the EIGRP Metric</i>	129
6.3.2.7	<i>Activity - Calculate the EIGRP Metric</i>	130
6.3.3	DUAL and the Topology Table	130
6.3.3.1	<i>DUAL Concepts</i>	130
6.3.3.2	<i>Introduction to DUAL</i>	130
6.3.3.3	<i>Successor and Feasible Distance</i>	131
6.3.3.4	<i>Feasible Successors, Feasibility Condition, and Reported Distance</i>	131
6.3.3.5	<i>Topology Table: show ip eigrp topology Command</i>	132
6.3.3.6	<i>Topology Table: show ip eigrp topology Command (Cont.)</i>	132
6.3.3.7	<i>Topology Table: No Feasible Successor</i>	133
6.3.3.8	<i>Activity - Determine the Feasible Successor</i>	134
6.3.4	DUAL and Convergence	134
6.3.4.1	<i>DUAL Finite State Machine (FSM)</i>	134
6.3.4.2	<i>DUAL: Feasible Successor</i>	134
6.3.4.3	<i>DUAL: No Feasible Successor</i>	134
6.3.4.4	<i>Packet Tracer - Investigating DUAL FSM</i>	135
6.4	Implement EIGRP for IPv6	135
6.4.1	EIGRP for IPv6	135
6.4.1.1	<i>EIGRP for IPv6</i>	135
6.4.1.2	<i>Compare EIGRP for IPv4 and IPv6</i>	136
6.4.1.3	<i>IPv6 Link-local Addresses</i>	137
6.4.1.4	<i>Activity - Compare EIGRPv4 and EIGRPv6</i>	137
6.4.2	Configure EIGRP for IPv6	137
6.4.2.1	<i>EIGRP for IPv6 Network Topology</i>	137
6.4.2.2	<i>Configuring IPv6 Link-local Addresses</i>	138
6.4.2.3	<i>Configuring the EIGRP for IPv6 Routing Process</i>	138
6.4.2.4	<i>The ipv6 eigrp Interface Command</i>	139
6.4.3	Verifying EIGRP for IPv6	140
6.4.3.1	<i>IPv6 Neighbor Table</i>	140
6.4.3.2	<i>The show ip protocols Command</i>	141
6.4.3.3	<i>The EIGRP for IPv6 Routing Table</i>	141
6.4.3.4	<i>Packet Tracer - Configuring Basic EIGRP with IPv6</i>	142
6.4.3.5	<i>Lab - Configuring Basic EIGRP for IPv6</i>	142
6.5	Summary	142
6.5.1	Conclusion	142
6.5.1.1	<i>Class Activity - Portfolio RIP and EIGRP</i>	142
6.5.1.2	<i>Chapter 6: EIGRP</i>	142
Chapter 6 Quiz		144
Chapter 6 Exam		144
Your Chapter Notes		144

Chapter 7 EIGRP Tuning and Troubleshooting 145

7.0 Introduction 145

7.0.1.2 *Class Activity - EIGRP - Back to the Future* 145

7.1 Tune EIGRP 145

7.1.1 Automatic Summarization 145

7.1.1.1 *Network Topology* 145

7.1.1.2 *EIGRP Automatic Summarization* 146

7.1.1.3 *Configuring EIGRP Automatic Summarization* 147

7.1.1.4 *Verifying Auto-Summary: show ip protocols* 147

7.1.1.5	<i>Verifying Auto-Summary: Topology Table</i>	148
7.1.1.6	<i>Verifying Auto-Summary: Routing Table</i>	148
7.1.1.7	<i>Summary Route</i>	149
7.1.1.8	<i>Summary Route (Cont.)</i>	149
7.1.1.9	<i>Activity - Determine the Classful Summarization</i>	150
7.1.1.10	<i>Activity - Determine the Exit Interface for a Given Packet</i>	150
7.1.2	<i>Default Route Propagation</i>	150
7.1.2.1	<i>Propagating a Default Static Route</i>	150
7.1.2.2	<i>Verifying the Propagated Default Route</i>	150
7.1.2.3	<i>EIGRP for IPv6: Default Route</i>	151
7.1.2.4	<i>Packet Tracer - Propagating a Default Route in EIGRP for IPv4 and IPv6</i>	151
7.1.3	<i>Fine-tuning EIGRP Interfaces</i>	152
7.1.3.1	<i>EIGRP Bandwidth Utilization</i>	152
7.1.3.2	<i>Hello and Hold Timers</i>	152
7.1.3.3	<i>Load Balancing IPv4</i>	153
7.1.3.4	<i>Load Balancing IPv6</i>	154
7.1.3.5	<i>Activity - Determine the EIGRP Fine Tuning Commands</i>	154
7.1.3.6	<i>Lab - Configuring Advanced EIGRP for IPv4 Features</i>	154

7.2 Troubleshoot EIGRP 155

7.2.1	<i>Components of Troubleshooting EIGRP</i>	155
7.2.1.1	<i>Basic EIGRP Troubleshooting Commands</i>	155
7.2.1.2	<i>Components</i>	155
7.2.1.3	<i>Activity - Identify the Troubleshooting Command</i>	156
7.2.2	<i>Troubleshoot EIGRP Neighbor Issues</i>	156
7.2.2.1	<i>Layer 3 Connectivity</i>	156
7.2.2.2	<i>EIGRP Parameters</i>	156
7.2.2.3	<i>EIGRP Interfaces</i>	157
7.2.2.4	<i>Activity - Troubleshoot EIGRP Neighbor Issues</i>	158
7.2.3	<i>Troubleshoot EIGRP Routing Table Issues</i>	158
7.2.3.1	<i>Passive Interface</i>	158
7.2.3.2	<i>Missing Network Statement</i>	158
7.2.3.3	<i>Autosummarization</i>	159
7.2.3.4	<i>Activity - Troubleshoot EIGRP Routing Table Issues</i>	160
7.2.3.5	<i>Packet Tracer - Troubleshooting EIGRP for IPv4</i>	160
7.2.3.6	<i>Lab - Troubleshooting Basic EIGRP for IPv4 and IPv6</i>	160
7.2.3.7	<i>Lab - Troubleshooting Advanced EIGRP</i>	160

7.3 Summary 161

7.3.1.1	<i>Class Activity - Tuning EIGRP</i>	161
7.3.1.2	<i>Packet Tracer - Skills Integration Challenge</i>	161
7.3.1.3	<i>Chapter 7: EIGRP Tuning and Troubleshooting</i>	161

Chapter 7 Quiz 163

Chapter 7 Exam 163

Your Chapter Notes 163

Chapter 8 Single-Area OSPF 165

8.0 Introduction 165

8.0.1.2	<i>Activity - Can Submarines Swim?</i>	165
---------	--	-----

8.1 OSPF Characteristics 165

8.1.1	<i>Open Shortest Path First</i>	165
-------	---------------------------------	-----

8.1.1.1	<i>Evolution of OSPF</i>	165
8.1.1.2	<i>Features of OSPF</i>	166
8.1.1.3	<i>Components of OSPF</i>	167
8.1.1.4	<i>Link-State Operation</i>	167
8.1.1.5	<i>Single-Area and Multiarea OSPF</i>	168
8.1.1.6	<i>Activity - Identify OSPF Features and Terminology</i>	169
8.1.2	<i>OSPF Messages</i>	169
8.1.2.1	<i>Encapsulating OSPF Messages</i>	169
8.1.2.2	<i>Types of OSPF Packets</i>	169
8.1.2.3	<i>Hello Packet</i>	170
8.1.2.4	<i>Hello Packet Intervals</i>	171
8.1.2.5	<i>Link-State Updates</i>	171
8.1.2.6	<i>Activity - Identify the OSPF Packet Types</i>	171
8.1.3	<i>OSPF Operation</i>	171
8.1.3.1	<i>OSPF Operational States</i>	171
8.1.3.2	<i>Establish Neighbor Adjacencies</i>	172
8.1.3.3	<i>OSPF DR and BDR</i>	173
8.1.3.4	<i>Synchronizing OSPF Databases</i>	173
8.1.3.5	<i>Activity - Identify the OSPF States for Establishing Adjacency</i>	174
8.1.3.6	<i>Video Demonstration - Observing OSPF Protocol Communications</i>	174

8.2 Single-Area OSPFv2 174

8.2.1	<i>OSPF Router ID</i>	174
8.2.1.1	<i>OSPF Network Topology</i>	174
8.2.1.2	<i>Router OSPF Configuration Mode</i>	175
8.2.1.3	<i>Router IDs</i>	175
8.2.1.4	<i>Configuring an OSPF Router ID</i>	176
8.2.1.5	<i>Modifying a Router ID</i>	176
8.2.1.6	<i>Using a Loopback Interface as the Router ID</i>	177
8.2.2	<i>Configure Single-Area OSPFv2</i>	177
8.2.2.1	<i>Enabling OSPF on Interfaces</i>	177
8.2.2.2	<i>Wildcard Mask</i>	178
8.2.2.3	<i>The network Command</i>	178
8.2.2.4	<i>Passive Interface</i>	179
8.2.2.5	<i>Configuring Passive Interfaces</i>	179
8.2.2.6	<i>Activity - Calculate the Subnet and Wildcard Masks</i>	180
8.2.2.7	<i>Packet Tracer - Configuring OSPFv2 in a Single-area</i>	180
8.2.3	<i>OSPF Cost</i>	180
8.2.3.1	<i>OSPF Metric = Cost</i>	180
8.2.3.2	<i>OSPF Accumulates Costs</i>	180
8.2.3.3	<i>Adjusting the Reference Bandwidth</i>	181
8.2.3.4	<i>Default Interface Bandwidths</i>	182
8.2.3.5	<i>Adjusting the Interface Bandwidth</i>	182
8.2.3.6	<i>Manually Setting the OSPF Cost</i>	183
8.2.4	<i>Verify OSPF</i>	183
8.2.4.1	<i>Verify OSPF Neighbors</i>	183
8.2.4.2	<i>Verify OSPF Protocol Settings</i>	184
8.2.4.3	<i>Verify OSPF Process Information</i>	184
8.2.4.4	<i>Verify OSPF Interface Settings</i>	184
8.2.4.5	<i>Lab - Configuring Basic Single-Area OSPFv2</i>	185

8.3 Single-Area OSPFv3 185

- 8.3.1 OSPFv2 vs. OSPFv3 185
 - 8.3.1.1 OSPFv3 185
 - 8.3.1.2 Similarities Between OSPFv2 to OSPFv3 186
 - 8.3.1.3 Differences Between OSPFv2 and OSPFv3 186
 - 8.3.1.4 Link-Local Addresses 187
 - 8.3.1.5 Activity - Compare and Contrast OSPFv2 and OSPFv3 187
- 8.3.2 Configuring OSPFv3 187
 - 8.3.2.1 OSPFv3 Network Topology 187
 - 8.3.2.2 Link-Local Addresses 187
 - 8.3.2.3 Assigning Link-Local Addresses 188
 - 8.3.2.4 Configuring the OSPFv3 Router ID 188
 - 8.3.2.5 Modifying an OSPFv3 Router ID 189
 - 8.3.2.6 Enabling OSPFv3 on Interfaces 190
- 8.3.3 Verify OSPFv3 190
 - 8.3.3.1 Verify OSPFv3 Neighbors 190
 - 8.3.3.2 Verify OSPFv3 Protocol Settings 191
 - 8.3.3.3 Verify OSPFv3 Interfaces 191
 - 8.3.3.4 Verify the IPv6 Routing Table 191
 - 8.3.3.5 Packet Tracer - Configuring Basic OSPFv3 191
 - 8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3 192

8.4 Summary 192

- 8.4.1.1 Activity - Stepping Through OSPFv3 192
- 8.4.1.2 Packet Tracer - Skills Integration Challenge 192
- 8.4.1.3 Chapter 8: Single-Area OSPF 192

Chapter 8 Quiz 194

Chapter 8 Exam 194

Your Chapter Notes 194

Chapter 9 Multiarea OSPF 195

9.0 Introduction 195

- 9.0.1.2 Class Activity - Leaving on a Jet Plane 195

9.1 Multiarea OSPF Operation 195

- 9.1.1 Why Multiarea OSPF? 195
 - 9.1.1.1 Single-Area OSPF 195
 - 9.1.1.2 Multiarea OSPF 196
 - 9.1.1.3 OSPF Two-Layer Area Hierarchy 197
 - 9.1.1.4 Types of OSPF Routers 197
 - 9.1.1.5 Activity - Identify the Multiarea OSPF Terminology 198
- 9.1.2 Multiarea OSPF LSA Operation 198
 - 9.1.2.1 OSPF LSA Types 198
 - 9.1.2.2 OSPF LSA Type 1 198
 - 9.1.2.3 OSPF LSA Type 2 199
 - 9.1.2.4 OSPF LSA Type 3 199
 - 9.1.2.5 OSPF LSA Type 4 199
 - 9.1.2.6 OSPF LSA Type 5 200
 - 9.1.2.7 Activity - Identify the OSPF LSA Type 200
- 9.1.3 OSPF Routing Table and Types of Routes 200
 - 9.1.3.1 OSPF Routing Table Entries 200
 - 9.1.3.2 OSPF Route Calculation 200
 - 9.1.3.3 Activity - Order the Steps for OSPF Best Path Calculations 201

9.2 Configuring Multiarea OSPF 201

- 9.2.1 Configuring Multiarea OSPF 201
 - 9.2.1.1 *Implementing Multiarea OSPF* 201
 - 9.2.1.2 *Configuring Multiarea OSPFv2* 202
 - 9.2.1.3 *Configuring Multiarea OSPFv3* 202
- 9.2.2 Verifying Multiarea OSPF 203
 - 9.2.2.1 *Verifying Multiarea OSPFv2* 203
 - 9.2.2.2 *Verify General Multiarea OSPFv2 Settings* 203
 - 9.2.2.3 *Verify the OSPFv2 Routes* 204
 - 9.2.2.4 *Verify the Multiarea OSPFv2 LSDB* 204
 - 9.2.2.5 *Verify Multiarea OSPFv3* 204
 - 9.2.2.6 *Packet Tracer - Configuring Multiarea OSPFv2* 204
 - 9.2.2.7 *Packet Tracer - Configuring Multiarea OSPFv3* 205
 - 9.2.2.8 *Lab - Configuring Multi-area OSPFv2* 205
 - 9.2.2.9 *Lab - Configuring Multi-area OSPFv3* 205

9.3 Summary 205

- 9.3.1.1 *Class Activity - Digital Trolleys* 205
- 9.3.1.2 *Chapter 9: Multiarea OSPF* 206

Chapter 9 Quiz 207**Chapter 9 Exam 207****Your Chapter Notes 207****Chapter 10 OSPF Tuning and Troubleshooting 209****10.0 Introduction 209**

- 10.0.1.2 *Class Activity - DR and BDR Election* 209

10.1 Advanced Single-Area OSPF Configurations 209

- 10.1.1 OSPF in Multiaccess Networks 209
 - 10.1.1.1 *OSPF Network Types* 209
 - 10.1.1.2 *Challenges in Multiaccess Networks* 210
 - 10.1.1.3 *OSPF Designated Router* 210
 - 10.1.1.4 *Verifying DR/BDR Roles* 211
 - 10.1.1.5 *Verifying DR/BDR Adjacencies* 212
 - 10.1.1.6 *Default DR/BDR Election Process* 213
 - 10.1.1.7 *DR/BDR Election Process* 214
 - 10.1.1.8 *The OSPF Priority* 214
 - 10.1.1.9 *Changing the OSPF Priority* 215
 - 10.1.1.10 *Activity - Identify OSPF Network Type Terminology* 216
 - 10.1.1.11 *Activity - Select the Designated Router* 216
 - 10.1.1.12 *Packet Tracer - Determining the DR and BDR* 216
 - 10.1.1.13 *Lab - Configuring OSPFv2 on a Multiaccess Network* 216
- 10.1.2 Default Route Propagation 216
 - 10.1.2.1 *Propagating a Default Static Route in OSPFv2* 216
 - 10.1.2.2 *Verifying the Propagated IPv4 Default Route* 217
 - 10.1.2.3 *Propagating a Default Static Route in OSPFv3* 217
 - 10.1.2.4 *Verifying the Propagated IPv6 Default Route* 217
 - 10.1.2.5 *Packet Tracer - Propagating a Default Route in OSPFv2* 218
- 10.1.3 Fine-tuning OSPF Interfaces 218
 - 10.1.3.1 *OSPF Hello and Dead Intervals* 218
 - 10.1.3.2 *Modifying OSPFv2 Intervals* 218

10.1.3.3	<i>Modifying OSPFv3 Intervals</i>	219
10.1.3.4	<i>Packet Tracer - Configuring OSPFv2 Advanced Features</i>	220
10.1.3.5	<i>Lab - Configuring OSPFv2 Advanced Features</i>	220
10.2	Troubleshooting Single-Area OSPF Implementations	220
10.2.1	Components of Troubleshooting Single-Area OSPF	220
10.2.1.1	<i>Overview</i>	220
10.2.1.2	<i>OSPF States</i>	220
10.2.1.3	<i>OSPF Troubleshooting Commands</i>	221
10.2.1.4	<i>Components of Troubleshooting OSPF</i>	221
10.2.1.5	<i>Activity - Identify the Troubleshooting Command</i>	222
10.2.2	Troubleshoot Single-Area OSPFv2 Routing Issues	222
10.2.2.1	<i>Troubleshooting Neighbor Issues</i>	222
10.2.2.2	<i>Troubleshooting OSPFv2 Routing Table Issues</i>	223
10.2.2.3	<i>Packet Tracer - Troubleshooting Single-Area OSPFv2</i>	223
10.2.3	Troubleshoot Single-Area OSPFv3 Routing Issues	223
10.2.3.1	<i>OSPFv3 Troubleshooting Commands</i>	223
10.2.3.2	<i>Troubleshooting OSPFv3</i>	224
10.2.3.3	<i>Lab - Troubleshooting Basic Single-Area OSPFv2 and OSPFv3</i>	225
10.2.3.4	<i>Lab - Troubleshooting Advanced Single-Area OSPFv2</i>	225
10.2.4	Troubleshooting Multiarea OSPFv2 and OSPFv3	225
10.2.4.1	<i>Multiarea OSPF Troubleshooting Skills</i>	225
10.2.4.2	<i>Multiarea OSPF Troubleshooting Data Structures</i>	225
10.2.4.3	<i>Packet Tracer - Troubleshooting Multiarea OSPFv2</i>	226
10.2.4.4	<i>Packet Tracer - Troubleshooting Multiarea OSPFv3</i>	226
10.2.4.5	<i>Lab - Troubleshooting Multiarea OSPFv2 and OSPFv3</i>	226
10.3	Summary	226
10.3.1.1	<i>Class Activity - OSPF Troubleshooting Mastery</i>	226
10.3.1.2	<i>Packet Tracer - Skills Integration Challenge</i>	227
10.3.1.3	<i>Chapter 10: OSPF Tuning and Troubleshooting</i>	227
Chapter 10 Quiz		229
Chapter 10 Exam		229
Your Chapter Notes		229
Index		231

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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

About This Course Booklet

Your Cisco Networking Academy Course Booklet is designed as a study resource you can easily read, highlight, and review on the go, wherever the Internet is not available or practical:

- The text is extracted directly, word-for-word, from the online course so you can highlight important points and take notes in the “Your Chapter Notes” section.
- Headings with the exact page correlations provide a quick reference to the online course for your classroom discussions and exam preparation.
- An icon system directs you to the online curriculum to take full advantage of the images imbedded within the Networking Academy online course interface and reminds you to perform the labs, Class activities, Interactive activities, Packet Tracer activities, watch videos, and take the chapter quizzes and exams.

Refer to
Online Course
for Illustration

Refer to
Lab Activity
for this chapter

Go to the online
course to take the
quiz and exam.

Refer to
Interactive Graphic
in online course

Refer to **Packet
Tracer Activity**
for this chapter

Refer to **Video**
in online course

The *Course Booklet* is a basic, economical paper-based resource to help you succeed with the Cisco Networking Academy online course.

Companion Guide

Looking for more than the online curriculum? The Companion Guide is fully aligned to Networking Academy’s online course chapters and offers additional book-based pedagogy to reinforce key concepts, enhance student comprehension, and promote retention. Using this full-fledged textbook, students can focus scarce study time, organize review for quizzes and exams, and get the day-to-day reference answers they’re looking for.

The Companion Guide also offers instructors additional opportunities to assign take-home reading or vocabulary homework, helping students prepare more for in-class lab work and discussions.

Available in print and all major eBook formats (book: 9781587134340; eBook: 9780134760896).

LAN Design

Refer to
Online Course
for Illustration

1.0 Introduction to LAN Design

There is a tendency to discount the network as just simple plumbing, to think that all you have to consider is the size and the length of the pipes or the speeds and feeds of the links, and to dismiss the rest as unimportant. Just as the plumbing in a large stadium or high rise has to be designed for scale, purpose, redundancy, protection from tampering or denial of operation, and the capacity to handle peak loads, the network requires similar consideration. As users depend on the network to access the majority of the information they need to do their jobs and to transport their voice or video with reliability, the network must be able to provide resilient, intelligent transport.

As a business grows, so does its networking requirements. Businesses rely on the network infrastructure to provide mission-critical services. Network outages can result in lost revenue and lost customers. Network designers must design and build an enterprise network that is scalable and highly available.

The campus local area network (LAN) is the network that supports devices people use within a location to connect to information. The campus LAN can be a single switch at a small remote site up to a large multi-building infrastructure, supporting classrooms, office space, and similar places where people use their devices. The campus design incorporates both wired and wireless connectivity for a complete network access solution.

This chapter discusses strategies that can be used to systematically design a highly functional network, such as the hierarchical network design model and appropriate device selections. The goals of network design are to limit the number of devices impacted by the failure of a single network device, provide a plan and path for growth, and create a reliable network.

Refer to
Online Course
for Illustration

1.0.1.2 Class Activity - Network by Design

Your employer is opening a new, branch office.

You have been reassigned to the site as the network administrator where your job will be to design and maintain the new branch network.

The network administrators at the other branches used the Cisco three-layer hierarchical model when designing their networks. You decide to use the same approach.

To get an idea of what using the hierarchical model can do to enhance the design process, you research the topic.

1.1 Campus Wired LAN Designs

1.1.1 Cisco Validated Designs

Refer to **Video**
in online course

1.1.1.1 The Need to Scale the Network

Businesses increasingly rely on their network infrastructure to provide mission-critical services. As businesses grow and evolve, they hire more employees, open branch offices, and expand into global markets. These changes directly affect the requirements of a network.

Click the Play button in the figure to view an animation of a small network expanding into a larger network.

A network must support the exchange of various types of network traffic, including data files, email, IP telephony, and video applications for multiple business units. All enterprise networks must:

- Support critical applications
- Support converged network traffic
- Support diverse business needs
- Provide centralized administrative control

The LAN is the networking infrastructure that provides access to network communication services and resources for end users and devices spread over a single floor or building. You create a campus network by interconnecting a group of LANs that are spread over a small geographic area. Campus network designs include small networks that use a single LAN switch, up to very large networks with thousands of connections.

Refer to
Interactive Graphic
in online course

1.1.1.2 Hierarchical Design Model

The campus wired LAN uses a hierarchical design model to break the design up into modular groups or layers. Breaking the design up into layers allows each layer to implement specific functions, which simplifies the network design and therefore the deployment and management of the network.

The campus wired LAN enables communications between devices in a building or group of building, as well as interconnection to the WAN and internet edge at the network core.

A hierarchical LAN design includes the following three layers, as shown in Figure 1:

- Access layer
- Distribution layer
- Core layer

Each layer is designed to meet specific functions.

The access layer provides endpoints and users direct access to the network. The distribution layer aggregates access layers and provides connectivity to services. Finally, the core layer provides connectivity between distribution layers for large LAN environments. User traffic is initiated at the access layer and passes through the other layers if the functionality of those layers is required.

Even though the hierarchical model has three layers, some smaller enterprise networks may implement a two-tier hierarchical design. In a two-tier hierarchical design, the core and distribution layers are collapsed into one layer, reducing cost and complexity, as shown in Figure 2.

In flat or meshed network architectures, changes tend to affect a large number of systems. Hierarchical design helps constrain operational changes to a subset of the network, which makes it easy to manage as well as improve resiliency. Modular structuring of the network into small, easy-to-understand elements also facilitates resiliency via improved fault isolation.

1.1.2 Expanding the Network

Refer to
Online Course
for Illustration

1.1.2.1 Design for Scalability

To support a large, medium or small network, the network designer must develop a strategy to enable the network to be available and to scale effectively and easily. Included in a basic network design strategy are the following recommendations:

- Use expandable, modular equipment or clustered devices that can be easily upgraded to increase capabilities. Device modules can be added to the existing equipment to support new features and devices without requiring major equipment upgrades. Some devices can be integrated in a cluster to act as one device to simplify management and configuration.
- Design a hierarchical network to include modules that can be added, upgraded, and modified, as necessary, without affecting the design of the other functional areas of the network. For example, creating a separate access layer that can be expanded without affecting the distribution and core layers of the campus network.
- Create an IPv4 or IPv6 address strategy that is hierarchical. Careful address planning eliminates the need to re-address the network to support additional users and services.
- Choose routers or multilayer switches to limit broadcasts and filter other undesirable traffic from the network. Use Layer 3 devices to filter and reduce traffic to the network core.

As shown in the figure, more advanced network design requirements include:

- Implementing redundant links in the network between critical devices and between access layer and core layer devices.
- Implementing multiple links between equipment, with either link aggregation (EtherChannel) or equal cost load balancing, to increase bandwidth. Combining multiple Ethernet links into a single, load-balanced EtherChannel configuration increases available bandwidth. EtherChannel implementations can be used when budget restrictions prohibit purchasing high-speed interfaces and fiber runs.
- Using a scalable routing protocol and implementing features within that routing protocol to isolate routing updates and minimize the size of the routing table.
- Implementing wireless connectivity to allow for mobility and expansion.

Refer to
Online Course
for Illustration

1.1.2.2 Planning for Redundancy

Implementing Redundancy

For many organizations, the availability of the network is essential to supporting business needs. Redundancy is an important part of network design for preventing disruption of network services by minimizing the possibility of a single point of failure. One method of implementing redundancy is by installing duplicate equipment and providing failover services for critical devices.

Another method of implementing redundancy is redundant paths, as shown in the figure. Redundant paths offer alternate physical paths for data to traverse the network. Redundant paths in a switched network support high availability. However, due to the operation of switches, redundant paths in a switched Ethernet network may cause logical Layer 2 loops. For this reason, Spanning Tree Protocol (STP) is required.

STP eliminates Layer 2 loops when redundant links are used between switches. It does this by providing a mechanism for disabling redundant paths in a switched network until the path is necessary, such as when failures occur. STP is an open standard protocol, used in a switched environment to create a loop-free logical topology.

More details about LAN redundancy and the operation of STP are covered in the chapter titled “STP”.

Refer to
Online Course
for Illustration

1.1.2.3 Failure Domains

A well-designed network not only controls traffic, but also limits the size of failure domains. A failure domain is the area of a network that is impacted when a critical device or network service experiences problems.

The function of the device that initially fails determines the impact of a failure domain. For example, a malfunctioning switch on a network segment normally affects only the hosts on that segment. However, if the router that connects this segment to others fails, the impact is much greater.

The use of redundant links and reliable enterprise-class equipment minimize the chance of disruption in a network. Smaller failure domains reduce the impact of a failure on company productivity. They also simplify the troubleshooting process, thereby, shortening the downtime for all users.

In the figure, click each highlighted network device to view the associated failure domain.

Limiting the Size of Failure Domains

Because a failure at the core layer of a network can have a potentially large impact, the network designer often concentrates on efforts to prevent failures. These efforts can greatly increase the cost of implementing 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.

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 affect a significant number of end users.

Refer to
Online Course
for Illustration

1.1.2.4 Increasing Bandwidth

Implementing EtherChannel

In hierarchical network design, some links between access and distribution switches may need to process a greater amount of traffic than other links. As traffic from multiple links converges onto a single, outgoing link, it is possible for that link to become a bottleneck. Link aggregation allows an administrator to increase the amount of bandwidth between devices by creating one logical link made up of several physical links. EtherChannel is a form of link aggregation used in switched networks, as shown in the figure.

EtherChannel uses the existing switch ports; therefore, additional costs to upgrade the link to a faster and more expensive connection are not necessary. The EtherChannel is seen as one logical link using an EtherChannel interface. Most configuration tasks are done on the EtherChannel interface, instead of on each individual port, ensuring configuration consistency throughout the links. Finally, the EtherChannel configuration takes advantage of load balancing between links that are part of the same EtherChannel, and depending on the hardware platform, one or more load-balancing methods can be implemented.

EtherChannel operation and configuration will be covered in more detail in the chapter titled “Etherchannel and HSRP”.

Refer to
Online Course
for Illustration

1.1.2.5 Expanding the Access Layer

Implementing Wireless Connectivity

The network must be designed to be able to expand network access to individuals and devices, as needed. An increasingly important aspect of extending access layer connectivity is through wireless connectivity. Providing wireless connectivity offers many advantages, such as increased flexibility, reduced costs, and the ability to grow and adapt to changing network and business requirements.

To communicate wirelessly, end devices require a wireless NIC that incorporates a radio transmitter/receiver and the required software driver to make it operational. Additionally, a wireless router or a wireless access point (AP) is required for users to connect, as shown in the figure.

There are many considerations when implementing a wireless network, such as the types of wireless devices to use, wireless coverage requirements, interference considerations, and security considerations.

Refer to
Interactive Graphic
in online course

1.1.2.6 Fine-tuning Routing Protocols

Managing the Routed Network

Advanced routing protocols, such as OSPF and EIGRP are used in large networks.

Link-state routing protocols such as Open Shortest Path First (OSPF), as shown in Figure 1, works well for larger hierarchical networks where fast convergence is important. OSPF routers establish and maintain neighbor adjacency or adjacencies, with other connected OSPF routers. When routers initiate an adjacency with neighbors, an exchange of link-state updates begins. Routers reach a FULL state of adjacency when they have synchronized

views on their link-state database. With OSPF, link state updates are sent when network changes occur. Single Area OSPF configuration and concepts will be covered in Chapter 8.

Additionally, OSPF supports a two-layer hierarchical design, referred to as multiarea OSPF, as shown in Figure 2. All multiarea OSPF networks must have an Area 0, also called the backbone area. Non-backbone areas must be directly connected to area 0. Chapter 9 titled “Multiarea OSPF” introduces the benefits, operation, and configuration of Multiarea OSPF. Chapter 10, “OSPF Tuning and Troubleshooting”, will cover the more advanced features of OSPF.

Another popular routing protocol for larger networks is Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco developed EIGRP as a proprietary distance vector routing protocol with enhanced capabilities. Although configuring EIGRP is relatively simple, the underlying features and options of EIGRP are extensive and robust. For example, EIGRP uses multiple tables to manage the routing process, as shown in Figure 3. EIGRP contains many features that are not found in any other routing protocols. It is an excellent choice for large, multi-protocol networks that employ primarily Cisco devices.

Chapter 6 titled “EIGRP” introduces the operation and configuration of the EIGRP routing protocol, while chapter 7 titled “EIGRP Tuning and Troubleshooting” covers some of the more advanced configuration options of EIGRP.

Refer to
Interactive Graphic
in online course

1.1.2.7 Activity - Identify Scalability Terminology

1.2 Selecting Network Devices

1.2.1 Switch Hardware

Refer to
Interactive Graphic
in online course

1.2.1.1 Switch Platforms

When designing a network, it is important to select the proper hardware to meet current network requirements, as well as allow for network growth. Within an enterprise network, both switches and routers play a critical role in network communication.

There are five categories of switches for enterprise networks, as shown in Figure 1:

- **Campus LAN Switches** - To scale network performance in an enterprise LAN, there are core, distribution, access, and compact switches. These switch platforms vary from fanless switches with eight fixed ports to 13-blade switches supporting hundreds of ports. Campus LAN switch platforms include the Cisco 2960, 3560, 3650, 3850, 4500, 6500, and 6800 Series.
- **Cloud-Managed Switches** - The Cisco Meraki cloud-managed access switches enable virtual stacking of switches. They monitor and configure thousands of switch ports over the web, without the intervention of onsite IT staff.
- **Data Center Switches** - A data center should be built based on switches that promote infrastructure scalability, operational continuity, and transport flexibility. The data center switch platforms include the Cisco Nexus Series switches and the Cisco Catalyst 6500 Series switches.
- **Service Provider Switches** - Service provider switches fall under two categories: aggregation switches and Ethernet access switches. Aggregation switches are

carrier-grade Ethernet switches that aggregate traffic at the edge of a network. Service provider Ethernet access switches feature application intelligence, unified services, virtualization, integrated security, and simplified management.

- **Virtual Networking** - Networks are becoming increasingly virtualized. Cisco Nexus virtual networking switch platforms provide secure multi-tenant services by adding virtualization intelligence technology to the data center network.

When selecting switches, network administrators must determine the switch form factors. This includes fixed configuration (Figure 2), modular configuration (Figure 3), stackable (Figure 4), or non-stackable. The thickness of the switch, which is expressed in the number of rack units, is also important for switches that are mounted in a rack. For example, the fixed configuration switches shown in Figure 2 are all one rack units (1U).

In addition to these considerations, Figure 5 highlights other common business considerations when selecting switch equipment.

Refer to
Online Course
for Illustration

1.2.1.2 Port Density

The port density of a switch refers to the number of ports available on a single switch. The figure shows the port density of three different switches.

Fixed configuration switches support a variety of port density configurations. The Cisco Catalyst 3850 24 port and 48 port switches are shown on the left in the figure. The 48 port switch has an option for four additional ports for small form-factor pluggable (SFP) devices.

Modular switches can support very high-port densities through the addition of multiple switch port line cards. The modular Catalyst 6500 switch shown on the right in the figure can support in excess of 1,000 switch ports.

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

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

Refer to
Online Course
for Illustration

1.2.1.3 Forwarding Rates

Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. Switch product lines are classified by forwarding rates, as shown in the figure. Entry-level switches have lower forwarding rates than enterprise-level switches. Forwarding rates are important to consider when selecting a switch. If the switch forwarding rate is too low, it cannot accommodate full wire-speed communication across all of its switch ports. Wire speed is the data rate that each Ethernet port on the switch is capable of attaining. Data rates can be 100 Mb/s, 1 Gb/s, 10 Gb/s, or 100 Gb/s.

For example, a typical 48-port gigabit switch operating at full wire speed generates 48 Gb/s of traffic. If the switch only supports a forwarding rate of 32 Gb/s, it cannot run at full wire speed across all ports simultaneously. Fortunately, access layer switches typically do not need to operate at full wire speed, because they are physically limited by their uplinks to the distribution layer. This means that less expensive, lower performing switches can be used at the access layer, and more expensive, higher performing switches can be used at the distribution and core layers, where the forwarding rate has a greater impact on network performance.

Refer to
Interactive Graphic
in online course

1.2.1.4 Power over Ethernet

PoE allows the switch to deliver power to a device over the existing Ethernet cabling. This feature can be used by IP phones and some wireless access points. Click the highlighted icons in Figure 1 to view PoE ports on each device.

PoE allows more flexibility when installing wireless access points and IP phones, allowing them to be installed anywhere that there is an Ethernet cable. A network administrator should ensure that the PoE features are required, because switches that support PoE are expensive.

The Cisco Catalyst 2960-C and 3560-C Series compact switches support PoE pass-through. PoE pass-through allows a network administrator to power PoE devices connected to the switch, as well as the switch itself, by drawing power from certain upstream switches. Click the highlighted icon in Figure 2 to view a Cisco Catalyst 2960-C.

Refer to
Online Course
for Illustration

1.2.1.5 Multilayer Switching

Multilayer switches are typically deployed in the core and distribution layers of an organization's switched network. Multilayer switches are characterized by their ability to build a routing table, support a few routing protocols, and forward IP packets at a rate close to that of Layer 2 forwarding. Multilayer switches often support specialized hardware, such as application-specific integrated circuits (ASICs). ASICs along with dedicated software data structures can streamline the forwarding of IP packets independent of the CPU.

There is a trend in networking toward a pure Layer 3 switched environment. When switches were first used in networks, none of them supported routing; now, almost all switches support routing. It is likely that soon all switches will incorporate a route processor because the cost of doing so is decreasing relative to other constraints.

As shown in the figure, the Catalyst 2960 switches illustrate the migration to a pure Layer 3 environment. With IOS versions prior to 15.x, these switches supported only one active switched virtual interface (SVI). With IOS 15.x, these switches now support multiple active SVIs. This means that the switch can be remotely accessed via multiple IP addresses on distinct networks.

Refer to
Interactive Graphic
in online course

1.2.1.6 Activity - Selecting Switch Hardware

Refer to **Packet Tracer Activity**
for this chapter

1.2.1.7 Packet Tracer - Comparing 2960 and 3560 Switches

In this activity, you will use various commands to examine three different switching topologies and compare the similarities and differences between the 2960 and 3560 switches. You will also compare the routing table of a 1941 router with a 3560 switch.

1.2.2 Router Hardware

Refer to
Online Course
for Illustration

1.2.2.1 Router Requirements

In the distribution layer of an enterprise network, routing is required. Without the routing process, packets cannot leave the local network.

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

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link or path goes down. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway. The ability to route efficiently and recover from network link failures is critical to delivering packets to their destination.

Routers also serve other beneficial functions:

- Provide broadcast containment
- Connect remote locations
- Group users logically by application or department
- Provide enhanced security

Click each highlighted area in the figure for more information on the functions of routers.

Refer to
Online Course
for Illustration

1.2.2.2 Cisco Routers

As the network grows, it is important to select the proper routers to meet its requirements. As shown in the figure, there are three categories of routers:

- **Branch Routers** - Branch routers optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructures. Maximizing service availability at the branch requires networks designed for 24x7x365 uptime. Highly available branch networks must ensure fast recovery from typical faults, while minimizing or eliminating the impact on service, and provide simple network configuration and management.
- **Network Edge Routers** - Network edge routers enable the network edge to deliver high-performance, highly secure, and reliable services that unite campus, data center, and branch networks. Customers expect a high-quality media experience and more types of content than ever before. Customers want interactivity, personalization, mobility, and control for all content. Customers also want to access content anytime and anyplace they choose, over any device, whether at home, at work, or on the go. Network edge routers must deliver enhanced quality of service and nonstop video and mobile capabilities.
- **Service Provider Routers** - Service provider routers differentiate the service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services. Operators must optimize operations, reduce expenses, and improve scalability and flexibility, to deliver next-generation Internet experiences across all devices and locations. These systems are designed to simplify and enhance the operation and deployment of service-delivery networks.

Refer to
Online Course
for Illustration

1.2.2.3 Router Hardware

Routers also come in many form factors, as shown in the figure. Network administrators in an enterprise environment should be able to support a variety of routers, from a small desktop router to a rack-mounted or blade model.

Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built-in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. As an example, a Cisco 1941 router comes with two Gigabit Ethernet RJ-45 interfaces built-in, and two slots that can accommodate many different network interface modules. Routers come with a variety of different interfaces, such as Fast Ethernet, Gigabit Ethernet, Serial, and Fiber-Optic.

[Click here to see a comprehensive list of Cisco routers.](#)

Refer to
Interactive Graphic
in online course

1.2.2.4 Activity – Identify the Router Category

1.2.3 Managing Devices

Refer to
Online Course
for Illustration

1.2.3.1 Managing IOS Files and Licensing

With such a wide selection of network devices to choose from in the Cisco product line, an organization can carefully determine the ideal combination to meet the needs of the employees and the customers.

When selecting or upgrading a Cisco IOS device, it is important to choose the proper IOS image with the correct feature set and version. IOS refers to the package of routing, switching, security, and other internetworking technologies integrated into a single multitasking operating system. When a new device is shipped, it comes preinstalled with the software image and the corresponding permanent licenses for the customer-specified packages and features.

For routers, beginning with Cisco IOS Software release 15.0, Cisco modified the process to enable new technologies within the IOS feature sets, as shown in the figure.

Refer to
Online Course
for Illustration

1.2.3.2 In-Band versus Out-of-Band Management

Regardless of the Cisco IOS network device being implemented, there are two methods for connecting a PC to that network device for configuration and monitoring tasks. These methods include out-of-band and in-band management, as shown in the figure.

Out-of-band management is used for initial configuration or when a network connection is unavailable. Configuration using out-of-band management requires:

- Direct connection to console or AUX port
- Terminal emulation client

In-band management is used to monitor and make configuration changes to a network device over a network connection. Configuration using in-band management requires:

- At least one network interface on the device to be connected and operational
- Telnet, SSH, HTTP, or HTTPS to access a Cisco device

Note Telnet and HTTP are less secure and are not recommended.

Refer to
Interactive Graphic
in online course

1.2.3.3 Basic Router CLI Commands

A basic router configuration includes the hostname for identification, passwords for security, assignment of IP addresses to interfaces for connectivity, and basic routing. Figure 1 shows the commands entered to enable a router with RIPv2. Verify and save configuration changes using the **copy running-config startup-config** command. Figure 2 shows the results of the configuration commands that were entered in Figure 1. To clear the router configuration, use the **erase startup-config** command and then the **reload** command.

Use the Syntax Checker in Figure 3 to practice your basic router configuration skills.

Refer to
Interactive Graphic
in online course

1.2.3.4 Basic Router Show Commands

Here are some of the most commonly used IOS commands to display and verify the operational status of the router and related IPv4 network functionality. Similar commands are available for IPv6 by replacing **ip** with **ipv6**. These commands are divided into several categories.

Routing Related:

- **show ip protocols** - Displays information about the routing protocols configured. If RIP is configured, this includes the version of RIP, networks the router is advertising, whether or not automatic summarization is in effect, the neighbors the router is receiving updates from, and the default administrative distance, which is 120 for RIP. (Figure 1)
- **show ip route** - Displays routing table information, including: routing codes, known networks, administrative distance and metrics, how routes were learned, next hop, static routes, and default routes. (Figure 2)

Interface Related:

- **show interfaces** - Displays interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics. If specified without a specific interface designation, all interfaces will be displayed. If a specific interface is specified after the command, information about that interface only will be displayed. (Figure 3)
- **show ip interfaces** - Displays interface information, including: protocol status, the IPv4 address, if a helper address is configured, and whether an ACL is enabled on the interface. If specified without a specific interface designation, all interfaces will be displayed. If a specific interface is specified after the command, information about that interface only will be displayed. (Figure 4)
- **show ip interface brief** - Displays all interfaces with IPv4 addressing information and interface and line protocols status. (Figure 5)
- **show protocols** - Displays information about the routed protocol that is enabled, and the protocol status of interfaces. (Figure 6)

Other connectivity related commands include the **show cdp neighbors** command (Figure 7). This command displays information on directly connected Cisco devices including Device ID, the local interface the device is connected to, capability (R = router, S = switch), the platform, and Port ID of the remote device. The **details** option includes IP addressing information and the IOS version.

Use the Syntax Checker in Figure 8 to verify router configurations using these **show** commands.

Refer to
Interactive Graphic
in online course

1.2.3.5 Basic Switch CLI commands

Basic switch configuration includes the hostname for identification, passwords for security, and assignment of IP addresses for connectivity. In-band access requires the switch to have an IP address. Figure 1 shows the commands entered to enable a switch.

Figure 2 shows the results of the configuration commands that were entered in Figure 1. Verify and save the switch configuration using the **copy running-config startup-config** command. To clear the switch configuration, use the **erase startup-config** command and then the **reload** command. It may also be necessary to erase any VLAN information using the command **delete flash:vlan.dat**. When switch configurations are in place, view the configurations using the **show running-config** command.

Refer to
Interactive Graphic
in online course

1.2.3.6 Basic Switch Show Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status. Click buttons 1 to 4 for sample outputs of the commands and the important pieces of information that an administrator can gather from it.

Interface / Port Related:

- **show port-security** - Displays any ports with security activated. To examine a specific interface, include the interface ID. Information included in the output: the maximum addresses allowed, current count, security violation count, and action to be taken. (Figure 1)
- **show port-security address** - Displays all secure MAC addresses configured on all switch interfaces. (Figure 2)
- **show interfaces** - Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics. (Figure 3)
- **show mac-address-table** - Displays all MAC addresses that the switch has learned, how those addresses were learned (dynamic/static), the port number, and the VLAN assigned to the port. (Figure 4)

Like the router, the switch also supports the **show cdp neighbors** command.

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

1.3 Summary

Refer to
Online Course
for Illustration

1.3.1.1 Class Activity - Layered Network Design Simulation

As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:

- One 2911 series router
- One 3560 switch
- One 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Refer to
Interactive Graphic
in online course

1.3.1.2 Basic Switch Configuration

Refer to **Packet
Tracer Activity**
for this chapter

1.3.1.3 Packet Tracer - Skills Integration Challenge

Background/Scenario

As a recently hired LAN technician, your network manager has asked you to demonstrate your ability to configure a small LAN. Your tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. You are to use two switches and two hosts/PCs on a cabled and powered network.

Refer to
Online Course
for Illustration

1.3.1.4 Summary

The hierarchical network design model divides network functionality into the access layer, the distribution layer, and the core layer. The campus wired LAN enables communications between devices in a building or group of buildings, as well as interconnection to the WAN and internet edge at the network core.

A well-designed network controls traffic and limits the size of failure domains. Routers and switches can be deployed in pairs so that the failure of a single device does not cause service disruptions.

A network design should include an IP addressing strategy, scalable, and fast-converging routing protocols, appropriate Layer 2 protocols, and modular or clustered devices that can be easily upgraded to increase capacity.

A mission-critical server should have a connection to two different access layer switches. It should have redundant modules when possible, and a power backup source. It may be appropriate to provide multiple connections to one or more ISPs.

Security monitoring systems and IP telephony systems must have high availability and often have special design considerations.

It is important to deploy the appropriate type of routers and switches for a given set of requirements, features and specifications, and expected traffic flow.

Go to the online course to take the quiz and exam.

Chapter 1 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 1 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes

Symbols

? (question mark), 117
802.1D BPDU, 48–50
802.1D-2004, 52

A

ABR (Area Border Router), 197–198
access layer, expanding, 5
Acknowledgement packets, 112
Acknowledgment packets, 114
AD (administrative distance), 166
Address Families (AF) feature, 166
addressing (IP). *See* IPv4; IPv6
adjacencies, 125, 172, 213
administrative distance (AD), 166
advertisements, 17, 198–200
AF (Address Families) feature, 166
alternate ports, 45, 48–49
Area Border Router (ABR), 197–198
ASBR (Autonomous System Boundary Router), 198
authentication (EIGRP), 111, 112
auto-cost reference-bandwidth command, 181
automatic summarization, 145–150, 159–160
Autonomous System Boundary Router (ASBR), 198
autonomous system numbers, 116–117
auto-summary command, 147, 148, 159

B

backbone area, 197
backbone routers, 197
backup designated routers (BDRs), 173, 210–214
backup ports, 45
in-band management, 10
bandwidth, 129–130
 bandwidth metric, 128
 bandwidth parameter, verifying, 129–130
 EIGRP utilization, 152
 increasing, 5
 interface bandwidth, 182
 reference bandwidth, 181–182
bandwidth command, 128, 146, 182
BDRs (backup designated routers), 173, 210–214
BGP (Border Gateway Protocol), 89, 117
BID (bridge ID), 45, 59
blocking state (ports), 55
Border Gateway Protocol (BGP), 89, 117

bounded updates, 99, 113–114
BPDU (bridge protocol data unit), 48–50, 57, 60
branch routers, 9
bridge ID (BID), 45, 59
bridge protocol data unit. *See* BPDU (bridge protocol data unit)
broadcast multiaccess networks, 209
broadcast storms, 42

C

campus LAN switches, 6
campus wired designs, 2–3
Catalyst switches, 21–22, 59. *See also* switches
CEF (Cisco Express Forwarding), 153
channel-group command, 74, 76
chassis aggregation, 65–66
Cisco Express Forwarding (CEF), 153
Cisco validated designs, 2–3
classification of routing protocols, 88–89
classless EIGRP (Enhanced Interior Gateway Routing Protocol), 109
classless routing protocols, 92
clear ip ospf command, 221
clear ip ospf process command, 177, 215
clear ipv6 ospf command, 224
clear ipv6 ospf process command, 190
clients (VTP), 21
cloud-managed switches, 6
cold start, 94–95
Coltun, Rob, 166
composite metric (EIGRP), 126–127
configuration
 EIGRP (Enhanced Interior Gateway Routing Protocol), 116–121, 134–140, 147
 EtherChannel, 5, 71, 73–75
 HSRP (Hot Standby Router Protocol), 81–82
 OSPF (Open Shortest Path First)
 in multiaccess networks, 209–216
 multiarea OSPF (Open Shortest Path First), 202–203
 OSPFv2, 177–180
 OSPFv3, 187–190
 passive interfaces, 179–180
 reference bandwidth, 181–182
 router IDs, 176–177, 188–190
PVST+59–61
Rapid PVST+62
STP (Spanning Tree Protocol), 63–65

- switches, 27
- VLANs, 22–24
- VTP (VLAN Trunking Protocol), 18–21

convergence, 87–88, 99, 126, 134–135, 180–183

copy running-config startup-config command, 11, 12, 22

D

data center switches, 6

data structures, 167

Database Description (DBD) packet, 170

DBD (Database Description) packet, 170

Dead intervals, 218

debug eigrp fsm command, 135

debug standby ? command, 82

debug standby packets command, 82

debug standby terse command, 82–83

debugging HSRP (Hot Standby Router Protocol), 82–83

default gateway limitations, 77

default interface bandwidths, 182

default route propagation, 150–151, 216–218

default-information originate command, 216–217

delay metric, 128–129

delay value, 130

delete flash:vlan.dat command, 12

deleting VLANs, 26

density, port, 7

deployment of switch blocks, 4–5

design (LAN). *See* LAN (local area network) design

designated ports, 45, 48–49

designated routers. *See* DRs (designated routers)

destination IPv6 addresses, 137, 187

devices, 6–12

Diffusing Update Algorithm, 130–135

Dijkstra, Edsger Wybe, 165

Dijkstra's algorithm, 100–101, 167

disabled ports, 45

disabled state (ports), 55

discovery, 95–96

distance vector dynamic routing, 90–98.

See also EIGRP (Enhanced Interior Gateway Routing Protocol)

DMVPN (Dynamic Multipoint Virtual Private Network), 109–110

domains, 4–5, 20–21

DROTHERs, 173, 210–214

DRs (designated routers), 173, 210–214

DTP (Dynamic Trunking Protocol), 15, 24–25, 31

DUAL (Diffusing Update Algorithm), 130–135

duplicate unicast frames, 42–43

Dynamic Multipoint Virtual Private Network (DMVPN), 109–110

dynamic routing, 87, 107. *See also* EIGRP (Enhanced Interior Gateway Routing Protocol); OSPF (Open Shortest Path First)

BGP (Border Gateway Protocol), 89

classful routing protocols, 91–92

classless routing protocols, 92

costs, 87–88

distance vector dynamic routing, 90–98

EGP (Exterior Gateway Protocols), 89

IGP (Interior Gateway Protocols), 89–90

link-state routing protocols, 90–91, 100–105

protocol classification, 88–89

routing protocol characteristics, 92–93

routing protocol metrics, 93

Dynamic Trunking Protocol. *See* DTP (Dynamic Trunking Protocol)

E

e bit (external bit), 199

edge ports, 58

EGP (Exterior Gateway Protocols), 89

EIGRP (Enhanced Interior Gateway Routing Protocol), 6, 98–99, 109–110, 142–143

authentication, 111, 112

classless EIGRP, 109

configuration, 116–121, 134–140

convergence, 126

DUAL (Diffusing Update Algorithm), 130–135

messages, 115–116

metrics, 126–130

named EIGRP, 110

operation, 125–126

packets, 112–114

passive interfaces, 121

PDMs (protocol dependence modules), 111

router IDs, 118–119

RTP (Reliable Transport Protocol), 111

topology table, 125–126

troubleshooting, 155–162

tuning, 145–154, 161–162

verification, 122–124, 140–142

eigrp log-neighbor-changes command, 120

eigrp router-id command, 118–119, 139

election (DR/BDR), 214

encapsulating messages, 115, 169

Enhanced Interior Gateway Routing Protocol. *See* EIGRP (Enhanced Interior Gateway Routing Protocol)

erase startup-config command, 11, 12

EtherChannel, 5, 69–77, 80–85

Ethernet, PoE (Power over Ethernet), 8

expanding network. *See* network expansion

extended system ID, 50–52, 56

extended VLANs, 21–24

Exterior Gateway Protocols (EGP), 89

external bit (e bit), 199

F

failure, 4–5, 64

feasibility condition (FC), 131–132

feasible distance (FD), 131, 148

feasible successor (FS), 131–135, 148
 Ferguson, Dennis, 166
 FHRPs (First Hop Redundancy Protocols)
 default gateway limitations, 77
 GLBP (Gateway Load Balancing Protocol), 79
 HSRP (Hot Standby Router Protocol), 78–83
 IRDP (ICMP Router Discovery Protocol), 79
 router redundancy, 77–78
 VRRP (Virtual Router Redundancy Protocol), 79
 Finite State Machine (FSM), 130, 134
 flooding LSAs (link-state advertisements), 173, 210
 forwarding rates, 7–8
 forwarding state (ports), 55
 frame format, 48–49
 FS (feasible successor), 131–135, 148
 FSM (Finite State Machine), 130, 134

G-H

Gateway Load Balancing Protocol (GLBP), 79
 gateways, 77
 GLBP (Gateway Load Balancing Protocol), 79
 headers (packet), 115–116
 Hello intervals, 152–153, 171, 218
 Hello keepalive mechanism, 99
 Hello packets, 103, 112–113, 170
 hierarchical design model, 2
 Hold times, tuning, 152–153
 HSRP (Hot Standby Router Protocol), 78–83

I

ICMP Router Discovery Protocol (IRDP), 79
 IEEE 802.1w. *See* RSTP (Rapid Spanning Tree Protocol)
 IETF (Internet Engineering Task Force), 165
 IGP (Interior Gateway Protocols), 89–90
 IGRP (Interior Gateway Routing Protocol), 99
 increasing bandwidth, 5
 interface bandwidth, 182
 interface port-channel command, 74
 interface range command, 23, 74
 interface table (OSPF), 225
 Interior Gateway Protocols (IGP), 89–90
 Interior Gateway Routing Protocol (IGRP), 99
 Intermediate System to Intermediate System (IS-IS), 106
 internal routers, 197
 International Organization for Standardization (ISO), 106
 Internet Engineering Task Force (IETF), 165
 intervals
 Hello intervals, 152–153, 171, 218
 OSPF (Open Shortest Path First), 218–220
 inter-VLAN configuration issues, 26–29
 IOS file management, 10
 ip address command, 28–29
 ip bandwidth-percent eigrp command, 152
 ip hello-interval eigrp command, 152
 ip hold-time eigrp command, 152

ip mtu command, 223
 ip ospf cost command, 183
 ip ospf priority command, 215
 IPv4
 EIGRP (Enhanced Interior Gateway Routing Protocol),
 116–124, 136–137, 152
 link-local addresses, 137
 load balancing, 153–154
 troubleshooting, 28–29
 IPv6
 EIGRP (Enhanced Interior Gateway Routing Protocol),
 134–142, 152
 link-local addresses, 137, 187
 load balancing, 154
 ipv6 address command, 138
 ipv6 bandwidth-percent eigrp command, 152
 ipv6 eigrp command, 139–140, 159
 ipv6 hello-interval eigrp command, 153
 ipv6 hold-time eigrp command, 153
 ipv6 ospf command, 190
 ipv6 ospf priority command, 215
 ipv6 router ospf command, 188, 190
 ipv6 unicast-routing command, 138
 IRDP (ICMP Router Discovery Protocol), 79
 IS-IS (Intermediate System to Intermediate System), 106
 ISO (International Organization for Standardization), 106

J-K-L

k values, verifying, 127
 LACP (Link Aggregation Control Protocol), 73
 LAN (local area network) design, 1–13
 Cisco validated designs, 2–3
 device management, 10–12
 network expansion, 3–6
 router hardware, 9–10
 switch hardware, 6–8
 large link-state database (LSDB), 196
 Layer 3 connectivity, 156
 Layer 3 switching, 31–35
 layered network design simulation, 12–13
 learning state (ports), 55
 licensing, 10
 link aggregation, 70
 EtherChannel, 69–77, 80–85
 FHRPs (First Hop Redundancy Protocols), 78–83
 Link Aggregation Control Protocol (LACP), 73
 link-local addresses, 137, 187–188
 links
 Rapid PVST+58
 virtual, 210
 Link-State Acknowledgement (LSAck) packet, 170
 link-state advertisements (LSAs), 173,
 198–200, 210
 link-state database (LSDB), 104, 225
 link-state operation, 167–168
 link-state packets (LSP), 103–104

link-state protocols, 90–91, 100–105. *See also* OSPF (Open Shortest Path First)
Link-State Request (LSR) packet, 170
Link-State Update (LSU) packet, 170
link-state updates, 171
listening state (ports), 55
load balancing, 60–61, 153–154
LSAck (Link-State Acknowledgement) packet, 170
LSAs (link-state advertisements), 173, 198–200, 210
LSDB (large link-state database), 104
LSDB (link-state database), 196, 225
LSP (link-state packets), 103–104
LSR (Link-State Request) packet, 170
LSU (Link-State Update) packet, 170

M

MAC database instability, 41
maximum-paths command, 153
MD5 (Message Digest 5), 166
metric weights command, 127
missing network statement, troubleshooting, 158–159
MISTP (Multiple Instance STP), 53
mode active keywords, 74
modes (VTP), 16
modifying. *See* tuning
Moy, John, 166
MST (Multiple Spanning Tree), 54
MSTP (Multiple Spanning Tree Protocol), 53
multiaccess networks, OSPF (Open Shortest Path First) in, 209–215
multiarea OSPF (Open Shortest Path First), 5–6, 168–169, 195–197, 206
 configuration, 201–203
 LSAs (link-state advertisements), 198–200
 messages, 169–171
 OSPFv2, 202, 203–204
 OSPFv3, 202–203, 204
 route calculation, 200–201
 routers, 197–198
 routing table, 200
 troubleshooting, 225–226
 two-layer area hierarchy, 197
 verification, 203–204
multilayer switching, 8
Multiple Instance STP (MISTP), 53
Multiple Spanning Tree (MST), 54
Multiple Spanning Tree Protocol (MSTP), 53
multi-VLAN issues, 26–29

N

named EIGRP (Enhanced Interior Gateway Routing Protocol), 110
NBMA (nonbroadcast multiaccess), 113, 210
neighbors
 adjacency, 125, 172

EIGRP (Enhanced Interior Gateway Routing Protocol), 122, 125, 140, 156–157
neighbor table (OSPF), 225
troubleshooting, 222–223
verification, 183–184
network command, 102, 119–120, 177–179, 223
network devices, 6–12
network discovery, 95–96
network edge routers, 9
network expansion, 3–6
network link entries, 199
network redundancy, 4, 39–40, 66–67
 802.1D-2004, 52
 MST (Multiple Spanning Tree), 54
 MSTP (Multiple Spanning Tree Protocol), 53
 PVST+, 52–61
 Rapid PVST+, 52–53, 56–57, 62
 routers, 77–78
 RSTP (Rapid Spanning Tree Protocol), 44, 47, 52–53
 STP (Spanning Tree Protocol), 40–52, 63–66
 switch stacking, 65–66
network statements, 202
non-backbone area, 197
nonbroadcast multiaccess (NBMA), 113, 210
NSSA (not-so-stubby area), 197
Null0 interface, 149
numbers, autonomous system numbers, 116–117

O

O designation (OSPF routing table), 200
O E1 designation (OSPF routing table), 200
O E2 designation (OSPF routing table), 200
O IA designation (OSPF routing table), 200
Open Shortest Path First. *See* OSPF (Open Shortest Path First)
OSI layers, redundancy at, 40
OSPF (Open Shortest Path First), 5–6, 106, 209, 226–228. *See also* multiarea OSPF;
 single-area OSPF
 adding to routing table, 105
 components of, 167
 default route propagation, 216–218
 evolution of, 165–166
 features of, 166
 interface bandwidth, 182–183
 intervals, 218–220
 link-local addresses, 187–188
 link-state operation, 167–168
 messages, 169–171
 in multiaccess networks
 BDRs (*backup designated routers*), 210–214
 challenges, 210
 DRs (*designated routers*), 210–214
 network types, 209–210
 priority, 214–215

network topology, 174–175
 reference bandwidth, 181–182
 tuning/troubleshooting, 176–177
 out-of-band management, 10

P

packets

EIGRP (*Enhanced Interior Gateway Routing Protocol*), 112–114
 Hello, 103
 LSP (*link-state packets*), 103–104
 OSPF (*Open Shortest Path First*), 169–171

PAgP (Port Aggregation Protocol), 71–72

partial updates, 113–114

passive interfaces, 121, 158, 179–180

passive-interface command, 121, 158, 179, 222

passwords (VTP), 20–21

PDMs (protocol dependence modules), 111

Perlman, Radia, 44

PoE (Power over Ethernet), 8

point-to-multipoint access, 210

point-to-point links, 58

point-to-point networks, 209

Port Aggregation Protocol (PAgP), 71–72

PortFast, 60

ports

assigning to VLANs, 23
 designated and alternate ports, 48–49
 edge ports, 58
 port density, 7
 roles, 45–47
 routed ports, 33–34
 states, 55–56
 troubleshooting, 26–27

Power over Ethernet (PoE), 8

protocol dependence modules (PDMs), 111

PVST+, 52–61. *See also* Rapid PVST+

Q-R

Query packets, 112, 114

question mark (?), 117

Rapid PVST+, 52, 56–58, 62

Rapid Spanning Tree Protocol. *See* RSTP (Rapid Spanning Tree Protocol)

RD (reported distance), 131, 148

redistribute static command, 150–151

redundancy. *See* network redundancy

reference bandwidth, 181–182

Reliable Transport Protocol (RTP), 111

reload command, 11, 12

repairing STP (Spanning Tree Protocol), 64–65

Reply packets, 112, 114

reported distance (RD), 131, 148

requests, advertisement, 17

Retransmission Timeout (RTO), 122

RIP (Routing Information Protocol), 98–99

root bridges, 45–46

root path cost, 46–47

root ports, 45

route calculation, 200–201

route propagation, 150–151, 216–218

routed network management, 5–6

routed ports, 33–34

router eigrp command, 116–118, 147

router ospf command, 175

router-id command, 175–176, 189, 213

routers, 9

DRs (designated routers), 210–214

hardware, 9–10

router IDs, 118–119, 174–177, 188–190

routing configuration, verifying, 28

routing information exchange, 96–97

Routing Information Protocol (RIP), 98–99

routing protocols. *See also* dynamic routing

BGP (Border Gateway Protocol), 89

classful routing protocols, 91–92

classification, 88–89

classless routing protocols, 92

costs, 87–88

EGP (Exterior Gateway Protocols), 89

fine-tuning, 5–6

IGP (Interior Gateway Protocols), 89–90

link-state routing protocols, 90–91, 100–105

messages, 167

metrics, 93

routing protocol characteristics, 92–93

routing table, 123–124, 148–149, 158–160, 200, 223, 225

RSTP (Rapid Spanning Tree Protocol), 44, 47, 52–53

RSTP PVST+53

RTO (Retransmission Timeout), 122

RTP (Reliable Transport Protocol), 111

S

scalability, 2, 3

Secure Hash Algorithm (SHA), 166

servers (VTP), 20–21

service provider routers, 9

service provider switches, 6–7

SFP (small form-factor pluggable) devices, 7

SHA (Secure Hash Algorithm), 166

shared links, 58

Shortest Path First (SPF), 100–101, 104

show cdp neighbors command, 11, 12, 63

show dtp interface command, 25

show etherchannel port-channel command, 75

show etherchannel summary command, 75

show interfaces command, 11, 12, 27–28, 128, 182

show interfaces etherchannel command, 75

show interfaces port-channel command, 75

show interfaces vlan command, 23

show ip eigrp neighbors command, 122, 155

show ip eigrp topology all-links command, 133, 148
show ip eigrp topology command, 132–133
show ip interface brief command, 11, 156, 221–222
show ip interfaces command, 11
show ip ospf command, 184, 204, 221
show ip ospf database command, 204
show ip ospf interface brief command, 184, 203
show ip ospf interface command, 182, 184, 211, 218, 219, 221–222
show ip ospf neighbor command, 183–184, 212, 218, 219, 221–222
show ip protocols command, 11, 119, 122–123, 147, 147, 153, 155, 158, 176, 177, 179, 184, 203, 221, 222
show ip route command, 11, 123–124, 204, 217
show ip route ospf command, 204, 221, 222
show ipv6 eigrp neighbors command, 140
show ipv6 interface brief command, 138, 140, 187
show ipv6 ospf command, 191, 224
show ipv6 ospf interface brief command, 191
show ipv6 ospf interface command, 191, 212, 220, 224
show ipv6 ospf neighbor command, 190, 219, 224
show ipv6 protocols command, 141, 190, 191, 224
show ipv6 route command, 141, 151
show ipv6 route ospf command, 191, 224
show ipv6 route static command, 217
show mac-address-table command, 12
show port-security address command, 12
show port-security command, 12
show protocols command, 11
show running-config command, 12, 27–28, 60
show spanning-tree command, 47, 59, 61, 63
show spanning-tree vlan command, 64
show standby brief command, 82
show standby command, 82
show vlan brief command, 21, 22, 24
show vlan name student command, 23
show vlan summary command, 23
show vtp password command, 21
show vtp status command, 18, 20
shutdown command, 135
single-area OSPF (Open Shortest Path First), 165, 168–169, 192–193
 costs, 180–183
 messages, 169–171
 operation, 171–174
 OSPFv2 configuration, 177–180
 OSPFv2 router IDs, 174–177
 OSPFv2 versus OSPFv3, 185–187
 OSPFv3 configuration, 187–190
 OSPFv3 verification, 190–192
 troubleshooting, 220–225
 verification, 183–185
size of failure domains, 4
small form-factor pluggable (SFP) devices, 7
Smooth Round Trip Timer (SRTT), 122
source IPv6 addresses, 137, 187

Spanning Tree Algorithm. *See* STA (Spanning Tree Algorithm)
Spanning Tree Protocol. *See* STP (Spanning Tree Protocol)
spanning tree protocols. *See also* STP (Spanning Tree Protocol)
 802.1D-2004, 52
 MST (Multiple Spanning Tree), 54
 MSTP (Multiple Spanning Tree Protocol), 53
 PVST+, 52–61
 Rapid PVST+, 52–53, 56–58, 62
 RSTP (Rapid Spanning Tree Protocol), 52–53
spanning-tree bpduguard enable command, 60
spanning-tree cost command, 47
spanning-tree link-type command, 58
spanning-tree mode rapid-pvst command, 62
spanning-tree portfast bpduguard default command, 60
spanning-tree portfast command, 60
spanning-tree vlan command, 59, 61
SPF (Shortest Path First), 100–101, 104
SRTT (Smooth Round Trip Timer), 122
STA (Spanning Tree Algorithm), 43–47
stack master, 65
standby 1 preempt command, 82
standby preempt command, 80
standby priority command, 80
statements, network, 202
states
 HSRP (Hot Standby Router Protocol), 81
 OSPF (Open Shortest Path First), 171–172, 220
static route propagation, 150–151, 216–218
STP (Spanning Tree Protocol), 4, 39–43
 802.1D BPDU frame format, 48–49
 802.1D BPDU propagation and process, 49–50
 broadcast storms, 42
 designated and alternate ports, 48–49
 duplicate unicast frames, 42–43
 extended system ID, 50–52
 MAC database instability, 41
 redundancy at OSI layers 1 and 2, 40
 STA (Spanning Tree Algorithm), 43–44
 switch stacking, 65–66
 troubleshooting, 63–65
stub area, 197
subnet masks, 28–29
subset advertisements, 17
successor distance, 131
summary advertisements, 17
SVI (switch virtual interface), 8, 31, 32–33
switches
 block deployment, 4–5
 hardware, 6–8
 Layer 3 switching, 31–35
 platforms, 6–7
 ports, 26–27
 stacking, 65–66
 verification, 27

switchport access vlan command, 23
 switchport command, 32
 switchport mode access command, 23, 25
 switchport mode dynamic auto command, 25
 switchport mode dynamic desirable command, 25
 switchport mode trunk command, 24, 25, 27
 switchport nonegotiate command, 24, 25
 synchronizing OSPF (Open Shortest Path First) databases, 173–174

T

timers (HSRP), 81
 TLV (type, length, value) field, 115–116
 topology table, 99, 125–126, 130–133, 148
 totally stubby area, 197
 traffic-share balanced command, 154
 transit area, 197
 troubleshooting
 EIGRP (Enhanced Interior Gateway Routing Protocol), 155–162
 EtherChannel, 76–77
 HSRP (Hot Standby Router Protocol), 82–83
 Layer 3 switching, 34–35
 OSPF (Open Shortest Path First), 209–216, 220–228
 STP (Spanning Tree Protocol), 63–65
 VLANs, 26–29
 VTP (VLAN Trunking Protocol), 30–31
 trunking
 DTP (Dynamic Trunking Protocol), 15, 24–25, 31
 VTP (VLAN Trunking Protocol), 17–21, 30–31
 tuning
 EIGRP (Enhanced Interior Gateway Routing Protocol), 145–153, 161–162
 IETF (Internet Engineering Task Force), 153–154
 OSPF (Open Shortest Path First), 176–177, 188–190, 209–228
 type, length, value (TLV) field, 115–116
 Type 1 LSAs (link-state advertisements), 198
 Type 2 LSAs (link-state advertisements), 199
 Type 3 LSAs (link-state advertisements), 199
 Type 4 LSAs (link-state advertisements), 199
 Type 5 LSAs (link-state advertisements), 200

U

unequal-cost load balancing, 154
 unicast frames, 42–43
 Update packets, 112, 113–114
 updates, link-state, 171

V

variance command, 154
 verification
 bandwidth parameter, 129–130
 EIGRP (Enhanced Interior Gateway Routing Protocol), 122–124, 140–142, 147–149
 EtherChannel, 75
 IP addresses, 28–29
 k values, 127
 OSPF (Open Shortest Path First), 183–185, 190–192, 203–204
 passive interfaces, 121
 propagated default routes, 150–151, 217
 routing configuration, 28
 switch configuration, 27
 VLANs, 23
 VTP (VLAN Trunking Protocol) configuration, 21
 virtual links, 210
 virtual networking, 7
 Virtual Router Redundancy Protocol (VRRP), 79
 VLAN Trunking Protocol. *See* VTP (VLAN Trunking Protocol)
 vlan.dat database, 16
 VLANs, 15–16, 35–36
 assigning ports to, 23
 configuration, 21
 creating, 22–23
 deleting, 26
 DTP (Dynamic Trunking Protocol), 24–25, 31
 extended VLANs, 21–24
 Layer 3 switching, 31–35
 summary, 35–36
 troubleshooting, 26–29
 verification, 23
 VTP (VLAN Trunking Protocol), 15–21, 30–31
 VRRP (Virtual Router Redundancy Protocol), 79
 VTP (VLAN Trunking Protocol)
 advertisements, 17
 cautions, 19–20
 configuration, 18–21
 modes, 16
 troubleshooting, 30–31
 versions, 17
 vtp domain command, 20
 vtp mode server command, 20
 vtp password command, 21

W-X-Y-Z

wildcard masks, 120, 178
 wireless connectivity, 5