



Official Cert Guide

Learn, prepare, and practice for exam success



CCDA

200-310

ciscopress.com

ANTHONY BRUNO, CCIE NO. 2738

STEVE JORDAN, CCIE NO. 11293

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CCDA

200-310

Official Cert Guide

ANTHONY BRUNO, CCIE No. 2738

STEVE JORDAN, CCIE No. 11293

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

CCDA 200-310 Official Cert Guide

Anthony Bruno, CCIE No. 2738
Steve Jordan, CCIE No. 11293

Copyright © 2017 Pearson Education, 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.

Library of Congress Control Number: 2016940168

ISBN-10: 1-58714-454-9

ISBN-13: 978-1-58714-454-7

Warning and Disclaimer

This book is designed to provide information about the CCDA exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

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

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

Feedback Information

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

Reader feedback is a natural continuation of this process. If you have any comments on 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 be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact:

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact:

International Sales

intlcs@pearson.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.

Editor-in-Chief: Mark Taub

Product Line Manager: Brett Bartow

Acquisitions Editor: Michelle Newcomb,
Denise Lincoln

Managing Editor: Sandra Schroeder

Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Indexer: Ken Johnson

Cover Designer: Chuti Praesersith

Business Operation Manager, Cisco Press:
Jan Cornelissen

Technical Editors: Jay McMickle,
Kevin Yudong Wu

Copy Editor: Bart Reed

Editorial Assistant: Vanessa Evans

Composition: Studio Galou



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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, COIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Authors

Anthony Bruno, CCIE No. 2738, is a Consulting Director with BT with more than 20 years of experience in the internetworking field. Previously, he worked for International Network Services, Lucent Technologies, and as a captain in the U.S. Air Force. His other industry certifications include CCDP, PMP, CCNP Security, Cisco Certified Business Value Practitioner, Cisco Data Center Network Infrastructure Specialist, Cisco Security Solutions & Design Specialist, and ITILv3 Foundation. He has consulted for many enterprise and service provider customers in the design, implementation, and optimization of large-scale networks. Anthony leads architecture and design teams in building next-generation networks for his customers. He completed his Master of Science in Electrical Engineering at the University of Missouri–Rolla in 1994 and his Bachelor of Science in Electrical Engineering at the University of Puerto Rico–Mayaguez in 1990. He is also a part-time instructor for the University of Phoenix–Online, teaching networking courses.

Outside of work Anthony enjoys running marathons, Spartan obstacle races, and Olympic and Ironman distance triathlons.

Steve Jordan, CCIE No. 11293, is a Senior Technology Manager with Accudata Systems and has 20 years experience in the field of internetworking. For the last 10 years, Steve has specialized in data center architectures involving compute, network, storage, virtualization, and SDN. Over the years, Steve has worked with many enterprise and service provider customers in both pre-sales and post-sales engineering and architecture roles, along with working at several Cisco Gold Partners. He has extensive experience in data center architecture and design and has implemented solutions in many financial, energy, retail, healthcare, education, and telecommunications industries. Steve is a 10-Year triple CCIE in the tracks of Routing & Switching, Storage Networking, and Data Center. His other certifications include VMware VCIX-NV, VCP-NV, VCP4-DCV, VCP5-DCV, CCDP, CCNP, ACI-SE, and ACI-FE.

Steve lives in Houston, Texas, with his wife and three sons. When he is not working on technology, Steve can be found traveling to new places, finding great food, and listening to live music.

Steve was also the coauthor for the previous editions of the *CCDA Official Cert Guide*.

About the Technical Reviewers

Kevin Yudong Wu, CCIE No. 10697 (Routing & Switching and Security), is a senior network consultant at British Telecom (BT). He has been engaged as a leading engineer in various network design projects, including LAN, WLAN, data center, and network security with BT's customers. Before joining BT, Kevin worked as customer support engineer at Cisco High Touch Technical Support (HTTS) to support both Cisco LAN switching and security products. He holds a master degree in both Computer Science (The University of Texas at Arlington, 2003) and Materials Engineering (Beijing University of Aeronautics and Astronautics, 1995).

Jay McMickle, CCIE No. 35355 (Routing & Switching and Security), is a double CCIE with 20 years of experience in the IT industry. He currently works as a Sr. Network and Security Consultant at Accudata Systems in Houston, Texas. Previously, he worked for Baker Hughes as a Technical Lead—first for the WAN team, followed by the Security team, and finally leading the Solution Architecture team. His other certifications include 3x CCNP (Routing & Switching, Design, and Security), Cisco Advanced Security Architect, Cisco Security Specializations, BCNE, CCSA, MCSE, and CCA. He specializes in routing designs and implementation as well as Security Architecture, implementation, and Security Operations. When he isn't working, you can find him teaching American Karate (ASK) or on the water wakeboarding or wakesurfing with friends and family. A big thank you to God. From the bottom to here, it is only through Him that I have the family, career, and friends that surround me. Thank you to Steve and Anthony. When we met (with you both as consultants) back in 2006, little did I know that we would remain in touch and become friends. Whether it's when I see Anthony at my neighborhood gym or Steve in the office, it goes to show how close our industry is and how you should nurture every relationship and not burn bridges. You might be working for them one day. Thank you to my wife for the patience she has with me in my work. Although I always "have one more thing to do," she understands my passion for IT and the dedication that comes along with it. Much love to both of my daughters, Avery (a.k.a. "The Goose") and Landyn (a.k.a. "The Bits"). I hope you both find a hobby that also serves as a career and funnels your passion for life as well. Much love to you both.

Dedications

This book is dedicated to my wife of 25 years, Yvonne Bruno, Ph.D., and to our daughters, Joanne and Dianne. Thanks for all of your support during the development of this book.

—Anthony Bruno

This book is dedicated to my wife of 22 years, Dorin Jordan, and my three sons, Blake, Lance, and Miles, for their support during the development of this book. I also want to dedicate this book to my mother Frances Brennan and my father-in law John Jordan for supporting me and being an inspiration to me throughout my life.

—Steve Jordan

Acknowledgments

This book would not have been possible without the efforts of many dedicated people. Thanks to Denise Lincoln and Michelle Newcomb for their guidance and support during the book development. Thanks to Chris Cleveland, development editor, for his guidance and special attention to detail. Thanks to Mandie Frank, project editor, for her accuracy. Thanks to Bart Reed, copy editor, for his attention to detail. Thanks to Brett Bartow, executive editor, for his vision. Thanks to all other Cisco Press team members who worked behind the scenes to make this a better book.

A special thanks my coauthor, Steve Jordan, for contributing five chapters. And a special thanks to the technical reviewers, Kevin Wu and Jay McMickle. Their technical advice and careful attention to detail made this book accurate.

—Anthony Bruno

This book would not be possible without all the great people who have assisted me. I would first like to thank Anthony Bruno for inviting me to assist him in this endeavor once more. Thanks to Denise Lincoln and Michelle Newcomb, project editors, for their guidance and support during the book development. Thanks again to Chris Cleveland, development editor, for supporting my schedule delays and keeping me on track.

Special thanks goes to the technical reviewers of this book, Kevin Wu and Jay McMickle, who provided wisdom and helped with keeping the book accurate.

Finally, thanks to all the managers and marketing people at Cisco Press who make all these books possible.

—Steve Jordan

Contents at a Glance

	Introduction	xxxvi
Part I	General Network Design	
Chapter 1	Network Design Methodology	3
Chapter 2	Network Design Models	39
Part II	LAN and WAN Design	
Chapter 3	Enterprise LAN Design	81
Chapter 4	Data Center Design	127
Chapter 5	Wireless LAN Design	167
Chapter 6	WAN Technologies and the Enterprise Edge	215
Chapter 7	WAN Design	249
Part III	The Internet Protocol and Routing Protocols	
Chapter 8	Internet Protocol Version 4 Design	287
Chapter 9	Internet Protocol Version 6 Design	333
Chapter 10	Routing Protocol Characteristics, RIP, EIGRP, and IS-IS	377
Chapter 11	OSPF, BGP, Route Manipulation, and IP Multicast	427
Part IV	Security, Convergence, Network Management	
Chapter 12	Managing Security	485
Chapter 13	Security Solutions	521
Chapter 14	Voice and Video Design	557
Chapter 15	Network Management Protocols	617
Part V	Comprehensive Scenarios and Final Prep	
Chapter 16	Comprehensive Scenarios	641
Chapter 17	Final Preparation	655
Part VI	Appendixes	
Appendix A	Answers to the “Do I Know This Already?” Quizzes and Q&A Questions	663
Appendix B	CCDA 200-310 version 1.0. Exam Updates	699
Appendix C	OSI Model, TCP/IP Architecture, and Numeric Conversion	701
	Glossary	717
	Index	730

Elements Available on the Book Website

Appendix D Memory Tables

Appendix E Memory Tables Answer Key

Appendix F Study Planner

Contents

	Introduction	xxxvi
Part I	General Network Design	
Chapter 1	Network Design Methodology	3
	“Do I Know This Already?” Quiz	3
	Foundation Topics	6
	Cisco Architectures for the Enterprise	6
	Borderless Networks Architecture	7
	Collaboration and Video Architecture	8
	Data Center and Virtualization Architecture	8
	Cisco Design Lifecycle: Plan, Build, Manage	9
	Plan Phase	10
	Build Phase	11
	Manage Phase	11
	Prepare, Plan, Design, Implement, Operate, and Optimize Phases	12
	Prepare Phase	14
	Plan Phase	14
	Design Phase	14
	Implement Phase	15
	Operate Phase	15
	Optimize Phase	15
	Summary of PPDIOO Phases	15
	Project Deliverables	16
	Design Methodology	16
	Identifying Customer Design Requirements	17
	Characterizing the Existing Network	18
	Steps in Gathering Information	19
	Network Audit Tools	19
	Network Checklist	23
	Designing the Network Topology and Solutions	24
	Top-Down Approach	24
	Pilot and Prototype Tests	25
	Design Document	25
	References and Recommended Reading	26
	Exam Preparation Tasks	28

	Review All Key Topics	28
	Complete Tables and Lists from Memory	28
	Define Key Terms	28
	Q&A	28
Chapter 2	Network Design Models	39
	“Do I Know This Already?” Quiz	39
	Foundation Topics	41
	Hierarchical Network Models	41
	Benefits of the Hierarchical Model	41
	Hierarchical Network Design	42
	<i>Core Layer</i>	42
	<i>Distribution Layer</i>	43
	<i>Access Layer</i>	44
	Hierarchical Model Examples	46
	Hub-and-Spoke Design	48
	Collapsed Core Design	49
	Cisco Enterprise Architecture Model	49
	Enterprise Campus Module	50
	Enterprise Edge Area	52
	<i>E-Commerce Module</i>	52
	<i>Internet Connectivity Module</i>	53
	<i>VPN/Remote Access</i>	54
	<i>Enterprise WAN</i>	55
	Service Provider Edge Module	56
	Remote Modules	57
	<i>Enterprise Branch Module</i>	57
	<i>Enterprise Data Center Module</i>	58
	<i>Enterprise Teleworker Module</i>	58
	High Availability Network Services	59
	Workstation-to-Router Redundancy and LAN High Availability	
	Protocols	60
	<i>ARP</i>	60
	<i>Explicit Configuration</i>	60
	<i>RDP</i>	60
	<i>RIP</i>	61
	<i>HSRP</i>	61

VRRP	62
GLBP	62
Server Redundancy	62
Route Redundancy	63
Load Balancing	63
Increasing Availability	63
Link Media Redundancy	65
References and Recommended Reading	66
Exam Preparation Tasks	68
Review All Key Topics	68
Complete Tables and Lists from Memory	68
Define Key Terms	68
Q&A	68

Part II LAN and WAN Design

Chapter 3 Enterprise LAN Design 81

“Do I Know This Already?” Quiz	81
Foundation Topics	83
LAN Media	83
Ethernet Design Rules	83
100Mbps Fast Ethernet Design Rules	84
Gigabit Ethernet Design Rules	85
1000BASE-LX Long-Wavelength Gigabit Ethernet	86
1000BASE-SX Short-Wavelength Gigabit Ethernet	86
1000BASE-CX Gigabit Ethernet over Coaxial Cable	86
1000BASE-T Gigabit Ethernet over UTP	86
10 Gigabit Ethernet Design Rules	87
10GE Media Types	87
EtherChannel	88
Comparison of Campus Media	88
LAN Hardware	89
Repeaters	89
Hubs	89
Bridges	89
Switches	90
Routers	91
Layer 3 Switches	92

Campus LAN Design and Best Practices	93
Best Practices for Hierarchical Layers	94
<i>Access Layer Best Practices</i>	94
<i>Distribution Layer Best Practices</i>	97
<i>Core Layer Best Practices</i>	99
STP Design Considerations	101
Cisco STP Toolkit	103
<i>PortFast</i>	103
<i>UplinkFast</i>	104
<i>BackboneFast</i>	104
<i>Loop Guard</i>	104
<i>Root Guard</i>	104
<i>BPDU Guard</i>	104
<i>BPDU Filter</i>	104
VLAN and Trunk Considerations	105
Unidirectional Link Detection (UDLD) Protocol	105
Large-Building LANs	106
Enterprise Campus LANs	107
<i>Edge Distribution</i>	109
Medium-Size LANs	109
Small and Remote Site LANs	110
Server Farm Module	110
<i>Server Connectivity Options</i>	111
Enterprise Data Center Infrastructure	111
Campus LAN QoS Considerations	111
Multicast Traffic Considerations	113
<i>CGMP</i>	113
<i>IGMP Snooping</i>	114
References and Recommended Readings	114
Exam Preparation Tasks	115
Review All Key Topics	115
Complete Tables and Lists from Memory	115
Define Key Terms	115
Q&A	115
Chapter 4 Data Center Design	127
“Do I Know This Already?” Quiz	127
Foundation Topics	130

Enterprise DC Architecture	130
Data Center Foundation Components	131
Data Center Topology Components	132
Data Center Network Programmability	133
SDN	134
Controllers	134
APIs	135
ACI	135
Challenges in the DC	136
Data Center Facility Aspects	136
Data Center Space	138
Data Center Power	139
Data Center Cooling	140
Data Center Heat	141
Data Center Cabling	141
Enterprise DC Infrastructure	143
Data Center Storage	144
Data Center Reference Architecture	146
Defining the DC Access Layer	147
Defining the DC Aggregation Layer	148
Defining the DC Core Layer	149
Security in the DC	150
Fabric Extenders	151
Virtualization Overview	151
Challenges	151
Defining Virtualization and Benefits	151
Virtualization Risks	152
Types of Virtualization	152
Virtualization Technologies	153
VSS	153
VRF	154
vPC	154
Device Contexts	155
Server Virtualization	155
Server Scaling	155
Virtual Switching	156

Network Virtualization Design Considerations	156
<i>Access Control</i>	156
<i>Path Isolation</i>	156
<i>Services Edge</i>	157
Data Center Interconnect	157
DCI Use Cases	157
DCI Transport Options	158
DCI L2 Considerations	159
Load Balancing in the DC	159
Application Load Balancing	159
Network Load Balancing	160
References and Recommended Readings	160
Exam Preparation Tasks	161
Review All Key Topics	161
Complete Tables and Lists from Memory	162
Define Key Terms	162
Q&A	162
Chapter 5	
Wireless LAN Design	167
“Do I Know This Already?” Quiz	167
Foundation Topics	169
Wireless LAN Technologies	169
WLAN Standards	169
<i>ISM and UNII Frequencies</i>	170
<i>Summary of WLAN Standards</i>	171
Service Set Identifier	171
WLAN Layer 2 Access Method	172
WLAN Security	172
<i>Unauthorized Access</i>	173
<i>WLAN Security Design Approach</i>	173
<i>IEEE 802.1X-2001 Port-Based Authentication</i>	173
<i>Dynamic WEP Keys and LEAP</i>	174
<i>Controlling WLAN Access to Servers</i>	174
Cisco Unified Wireless Network	175
Cisco UWN Architecture	175
Autonomous Access Points	176
Centralized WLAN Architecture	177
LWAPP	177

CAPWAP	178
Cisco Unified Wireless Network Split-MAC Architecture	179
Local MAC	179
AP Modes	180
LAP Discovery of WLC Using CAPWAP	181
WLAN Authentication	182
Authentication Options	183
WLAN Controller Components	183
WLC Interface Types	184
AP Controller Equipment Scaling	185
Roaming and Mobility Groups	186
Intracontroller Roaming	187
Layer 2 Intercontroller Roaming	187
Layer 3 Intercontroller Roaming	188
Mobility Groups	189
WLAN Design	190
Controller Redundancy Design: Deterministic vs. Dynamic	190
N+1 WLC Redundancy	190
N+N WLC Redundancy	191
N+N+1 WLC Redundancy	191
Radio Management and Radio Groups	192
RF Groups	193
RF Site Survey	194
Using EoIP Tunnels for Guest Services	194
Wireless Mesh for Outdoor Wireless	195
Mesh Design Recommendations	196
Campus Design Considerations	196
Power over Ethernet (PoE)	197
Wireless and Quality of Service (QoS)	197
Branch Design Considerations	199
Local MAC	200
REAP	200
Hybrid REAP	200
Branch Office Controller Options	200
References and Recommended Readings	201
Exam Preparation Tasks	203
Review All Key Topics	203

Complete Tables and Lists from Memory	203
Define Key Terms	203
Q&A	204
Chapter 6 WAN Technologies and the Enterprise Edge	215
“Do I Know This Already?” Quiz	215
Foundation Topics	218
WAN and Enterprise Edge Overview	218
WAN Defined	218
WAN Edge Module	219
Enterprise Edge Modules	219
WAN Transport Technologies	220
ISDN	221
<i>ISDN BRI Service</i>	221
<i>ISDN PRI Service</i>	221
Digital Subscriber Line	222
Cable	222
Wireless	223
Frame Relay	224
Time-Division Multiplexing	225
Metro Ethernet	225
SONET/SDH	225
Multiprotocol Label Switching (MPLS)	226
Dark Fiber	227
Dense Wavelength-Division Multiplexing	228
Ordering WAN Technology and Contracts	228
WAN and Edge Design Methodologies	229
Response Time	230
Throughput	231
Reliability	231
Bandwidth Considerations	231
WAN Link Categories	232
Optimizing Bandwidth Using QoS	233
<i>Queuing, Traffic Shaping, and Policing</i>	233
<i>Classification</i>	233
<i>Congestion Management</i>	234
<i>Priority Queuing</i>	234
<i>Custom Queuing</i>	234

	<i>Weighted Fair Queuing</i>	234
	<i>Class-Based Weighted Fair Queuing</i>	234
	<i>Low-Latency Queuing</i>	235
	<i>Traffic Shaping and Policing</i>	235
	<i>Link Efficiency</i>	235
	<i>Window Size</i>	236
	DMZ Connectivity	236
	Segmenting DMZs	237
	DMZ Services	238
	Internet Connectivity	238
	Centralized Internet (Branch) vs. Direct Internet (Branch)	240
	High Availability for the Internet Edge	240
	VPN Network Design	240
	References and Recommended Readings	242
	Exam Preparation Tasks	243
	Review All Key Topics	243
	Complete Tables and Lists from Memory	243
	Define Key Terms	243
	Q&A	244
Chapter 7	WAN Design	249
	“Do I Know This Already?” Quiz	249
	Foundation Topics	252
	Traditional WAN Technologies	252
	Hub-and-Spoke Topology	252
	Full-Mesh Topology	253
	Partial-Mesh Topology	253
	Point-to-Point Topology	254
	Remote Site Connectivity	254
	Enterprise VPN vs. Service Provider VPN	255
	Enterprise Managed VPN: IPsec	255
	<i>IPsec Direct Encapsulation</i>	256
	<i>Generic Routing Encapsulation</i>	257
	<i>IPsec DMVPN</i>	257
	<i>IPsec Virtual Tunnel Interface Design</i>	258
	<i>GETVPN</i>	258
	Service Provider–Managed Offerings	259
	<i>Metro Ethernet</i>	259

<i>Service Provider VPNs: L2 vs. L3</i>	260
<i>Virtual Private Wire Services</i>	260
<i>VPWS L2 VPN Considerations</i>	261
<i>Virtual Private LAN Services</i>	261
<i>VPLS L2 VPN Considerations</i>	262
MPLS	262
<i>MPLS Layer 3 Design Overview</i>	262
<i>MPLS L3 VPN Considerations</i>	262
VPN Benefits	263
WAN Backup Design	263
WAN Backup over the Internet	263
Enterprise WAN Architecture	264
Cisco Enterprise MAN/WAN	265
Enterprise WAN/MAN Architecture Comparison	266
Enterprise WAN Components	268
Comparing Hardware and Software	269
Enterprise Branch Architecture	270
Branch Design	270
Branch Connectivity	271
Redundancy for Branches	271
Single WAN Carrier vs. Dual WAN Carriers	271
Single MPLS Carrier Site	272
Dual MPLS Carriers	272
Hybrid WAN: L3 VPN with IPsec VPN	273
<i>Internet for Branches</i>	274
<i>Flat Layer 2 vs. Collapsed Core</i>	274
Enterprise Branch Profiles	275
<i>Small Branch Design</i>	275
<i>Medium Branch Design</i>	276
<i>Large Branch Design</i>	278
Enterprise Teleworker Design	279
ISRs for Teleworkers	280
References and Recommended Readings	280
Exam Preparation Tasks	281
Review All Key Topics	281
Complete Tables and Lists from Memory	281
Define Key Terms	281
Q&A	282

Part III The Internet Protocol and Routing Protocols

Chapter 8 Internet Protocol Version 4 Design 287

“Do I Know This Already?” Quiz	287
Foundation Topics	289
IPv4 Header	289
ToS	291
IPv4 Fragmentation	295
IPv4 Addressing	296
IPv4 Address Classes	297
Class A Addresses	297
Class B Addresses	298
Class C Addresses	298
Class D Addresses	298
Class E Addresses	298
IPv4 Address Types	299
IPv4 Private Addresses	299
NAT	300
IPv4 Address Subnets	302
Mask Nomenclature	302
IP Address Subnet Design Example	303
Determining the Network Portion of an IP Address	304
Variable-Length Subnet Masks	305
VLSM Address Assignment: Example 1	305
Loopback Addresses	307
IP Telephony Networks	308
VLSM Address Assignment: Example 2	308
IPv4 Addressing Design	310
Goal of IPv4 Address Design	310
Plan for Future Use of IPv4 Addresses	310
Performing Route Summarization	311
Plan for a Hierarchical IP Address Network	311
Private and Public IP Address and NAT Guidelines	313
Steps for Creating an IPv4 Address Plan	313
Case Study: IP Address Subnet Allocation	314
Address Assignment and Name Resolution	316
Recommended Practices of IP Address Assignment	317
BOOTP	317

	DHCP	317
	DNS	319
	ARP	321
	References and Recommended Readings	322
	Exam Preparation Tasks	324
	Review All Key Topics	324
	Complete Tables and Lists from Memory	324
	Define Key Terms	325
	Q&A	325
Chapter 9	Internet Protocol Version 6 Design	333
	“Do I Know This Already?” Quiz	333
	Foundation Topics	336
	Introduction to IPv6	336
	IPv6 Header	337
	IPv6 Address Representation	339
	IPv4-Compatible IPv6 Addresses	339
	IPv6 Prefix Representation	340
	IPv6 Address Scope Types and Address Allocations	340
	IPv6 Address Allocations	341
	IPv6 Unicast Address	342
	<i>Global Unicast Addresses</i>	342
	<i>Link-Local Addresses</i>	343
	<i>Unique Local IPv6 Address</i>	343
	<i>Global Aggregatable IPv6 Address</i>	343
	<i>IPv4-Compatible IPv6 Address</i>	344
	IPv6 Anycast Addresses	344
	IPv6 Multicast Addresses	344
	IPv6 Mechanisms	347
	ICMPv6	347
	IPv6 Neighbor Discovery Protocol	348
	IPv6 Name Resolution	348
	Path MTU Discovery	349
	IPv6 Address-Assignment Strategies	350
	<i>Manual Configuration</i>	350
	<i>SLAAC of Link-Local Address</i>	350
	<i>SLAAC of Globally Unique IPv6 Address</i>	350

<i>DHCPv6</i>	352
<i>DHCPv6 Lite</i>	352
IPv6 Security	352
IPv6 Routing Protocols	353
RIPng	353
EIGRP for IPv6	353
OSPFv3	353
IS-IS for IPv6	353
BGP4 Multiprotocol Extensions (MP-BGP) for IPv6	353
IPv6 Addressing Design	354
Planning for Addressing with IPv6	354
Route Summarization with IPv6	354
IPv6 Private Addressing	355
IPv6 for the Enterprise	355
IPv6 Address Allocation	355
<i>Partly Linked IPv4 Address into IPv6</i>	355
<i>Whole IPv4 Address Linked into IPv6</i>	356
<i>IPv6 Addresses Allocated Per Location and/or Type</i>	356
IPv4-to-IPv6 Transition Mechanisms and Deployment Models	357
Dual-Stack Mechanism	357
IPv6 over IPv4 Tunnels	357
Protocol Translation Mechanisms	359
IPv6 Deployment Models	360
<i>Dual-Stack Model</i>	360
<i>Hybrid Model</i>	361
<i>Service Block Model</i>	362
<i>IPv6 Deployment Model Comparison</i>	363
IPv6 Comparison with IPv4	363
References and Recommended Readings	364
Exam Preparation Tasks	367
Review All Key Topics	367
Complete Tables and Lists from Memory	368
Define Key Terms	368
Q&A	368
Chapter 10 Routing Protocol Characteristics, RIP, EIGRP, and IS-IS	377
“Do I Know This Already?” Quiz	377
Foundation Topics	380

Routing Protocol Characteristics	380
Static Versus Dynamic Route Assignment	380
Interior Versus Exterior Routing Protocols	382
Distance-Vector Routing Protocols	383
<i>EIGRP</i>	383
Link-State Routing Protocols	384
Distance-Vector Routing Protocols Versus Link-State Protocols	384
Hierarchical Versus Flat Routing Protocols	385
Classless Versus Classful Routing Protocols	385
IPv4 Versus IPv6 Routing Protocols	386
Administrative Distance	386
Routing Protocol Metrics and Loop Prevention	388
Hop Count	388
Bandwidth	389
Cost	389
Load	390
Delay	391
Reliability	391
Maximum Transmission Unit	391
Routing Loop-Prevention Schemes	392
<i>Split Horizon</i>	392
<i>Poison Reverse</i>	392
<i>Counting to Infinity</i>	393
Triggered Updates	393
Summarization	393
RIPv2 and RIPv6	393
Authentication	394
<i>MD5 Authentication</i>	394
RIPv2 Routing Database	394
RIPv2 Message Format	394
RIPv2 Timers	396
RIPv2 Design	396
RIPv2 Summary	396
RIPv6	397
<i>RIPv6 Timers</i>	397
<i>Authentication</i>	397
<i>RIPv6 Message Format</i>	397

	<i>RIPng Design</i>	398
	<i>RIPng Summary</i>	398
EIGRP		398
	EIGRP Components	399
	<i>Protocol-Dependent Modules</i>	399
	<i>Neighbor Discovery and Recovery</i>	399
	<i>RTP</i>	400
	<i>DUAL</i>	400
	EIGRP Timers	401
	EIGRP Metrics	401
	EIGRP Packet Types	403
	EIGRP Design	404
	<i>EIGRP Stub Routers</i>	404
	<i>EIGRP Variance Command</i>	405
	EIGRP for IPv4 Summary	406
	EIGRP for IPv6 (EIGRPv6) Networks	406
	<i>EIGRP for IPv6 Design</i>	407
	<i>EIGRP for IPv6 Summary</i>	407
IS-IS		408
	IS-IS Metrics	409
	IS-IS Operation and Design	409
	<i>IS-IS NET Addressing</i>	409
	<i>IS-IS DRs</i>	410
	<i>IS-IS Areas</i>	410
	<i>IS-IS Authentication</i>	411
	IS-IS Summary	411
References and Recommended Readings		412
Exam Preparation Tasks		413
	Review All Key Topics	413
	Complete Tables and Lists from Memory	413
	Define Key Terms	413
Q&A		414
Chapter 11	OSPF, BGP, Route Manipulation, and IP Multicast	427
	“Do I Know This Already?” Quiz	427
	Foundation Topics	430
	OSPFv2	430
	OSPFv2 Metric	430

OSPFv2 Adjacencies and Hello Timers	431
OSPFv2 Areas	432
<i>OSPF Area Design Considerations</i>	433
OSPF Router Types	434
OSPF DRs	435
LSA Types	436
<i>Autonomous System External Path Types</i>	436
OSPF Stub Area Types	437
<i>Stub Areas</i>	437
<i>Totally Stubby Areas</i>	438
<i>NSSAs</i>	438
Virtual Links	438
OSPFv2 Router Authentication	439
OSPFv2 Summary	439
OSPFv3	439
OSPFv3 Changes from OSPFv2	440
OSPFv3 Areas and Router Types	440
OSPFv3 LSAs	441
OSPFv3 Summary	443
BGP	443
BGP Neighbors	444
<i>eBGP</i>	445
<i>iBGP</i>	445
Route Reflectors	446
Confederations	448
BGP Administrative Distance	449
BGP Attributes, Weight, and the BGP Decision Process	449
<i>BGP Path Attributes</i>	449
<i>Next-Hop Attribute</i>	450
<i>Local Preference Attribute</i>	450
<i>Origin Attribute</i>	450
<i>Autonomous System Path Attribute</i>	451
<i>MED Attribute</i>	451
<i>Community Attribute</i>	452
<i>Atomic Aggregate and Aggregator Attributes</i>	452
<i>Weight</i>	453
<i>BGP Decision Process</i>	453
BGP Summary	454

Route Manipulation	455
PBR	455
Route Summarization	455
Route Redistribution	458
<i>Default Metric</i>	460
<i>OSPF Redistribution</i>	460
Route Filtering	461
<i>Transit Traffic</i>	461
Routing Protocols on the Hierarchical Network Infrastructure	462
IP Multicast Review	463
Multicast Addresses	463
Layer 3 to Layer 2 Mapping	464
IGMP	465
<i>IGMPv1</i>	465
<i>IGMPv2</i>	465
<i>IGMPv3</i>	466
<i>CGMP</i>	466
<i>IGMP Snooping</i>	467
Sparse Versus Dense Multicast	467
Multicast Source and Shared Trees	468
PIM	468
<i>PIM-SM</i>	469
<i>PIM DR</i>	469
<i>Auto-RP</i>	469
<i>PIMv2 Bootstrap Router</i>	470
DVMRP	470
IPv6 Multicast Addresses	470
References and Recommended Readings	471
Exam Preparation Tasks	473
Review All Key Topics	473
Complete Tables and Lists from Memory	473
Define Key Terms	474
Q&A	474

Part IV Security, Convergence, Network Management

Chapter 12 Managing Security 485

“Do I Know This Already?” Quiz	485
Foundation Topics	488

Network Security Overview	488
Security Legislation	489
Security Threats	490
<i>Reconnaissance and Port Scanning</i>	491
<i>Vulnerability Scanners</i>	492
<i>Unauthorized Access</i>	493
Security Risks	494
<i>Targets</i>	494
<i>Loss of Availability</i>	495
<i>Integrity Violations and Confidentiality Breaches</i>	496
Security Policy and Process	497
Security Policy Defined	498
Basic Approach of a Security Policy	498
Purpose of Security Policies	499
Security Policy Components	499
Risk Assessment	500
Risk Index	501
Continuous Security	501
Integrating Security Mechanisms into Network Design	502
Trust and Identity Management	503
Trust	503
Domains of Trust	503
Identity	504
<i>Passwords</i>	505
<i>Tokens</i>	505
<i>Certificates</i>	506
Network Access Control	506
Secure Services	506
Encryption Fundamentals	507
Encryption Keys	507
VPN Protocols	508
Transmission Confidentiality	509
Data Integrity	509
Threat Defense	510
Physical Security	510
Infrastructure Protection	512
Security Management Solutions	512
References and Recommended Readings	513

Exam Preparation Tasks	514
Review All Key Topics	514
Complete Tables and Lists from Memory	514
Define Key Terms	514
Q&A	515

Chapter 13 Security Solutions 521

“Do I Know This Already?” Quiz	521
Foundation Topics	524
Cisco SAFE Architecture	524
Network Security Platforms	525
Cisco Security Control Framework	526
Trust and Identity Technologies	527
Firewall Fundamentals	527
<i>Types of Firewalls</i>	528
<i>Next-Gen Firewalls</i>	529
<i>NAT Placement</i>	529
<i>Firewall Guidelines</i>	530
Firewall ACLs	530
Cisco Identity-Based Network Services	531
Identity and Access Control Deployments	532
Detecting and Mitigating Threats	533
IPS/IDS Fundamentals	534
IPS/IDS Guidelines	535
Threat Detection and Mitigation Technologies	536
Threat-Detection and Threat-Mitigation Solutions	536
FirePOWER IPS	538
Cisco ESA	538
Cisco WSA	538
Security Management Applications	539
Security Platform Solutions	540
Security Management Network	540
Integrating Security into Network Devices	541
IOS Security	542
ISR G2 Security Hardware Options	542
Cisco Security Appliances	543
Catalyst 6500 Service Modules	544
Endpoint Security	545

Securing the Enterprise	545
Implementing Security in the Campus	545
Implementing Security in the Data Center	546
Implementing Security in the Enterprise Edge	548
References and Recommended Readings	550
Exam Preparation Tasks	552
Review All Key Topics	552
Complete Tables and Lists from Memory	552
Define Key Terms	552
Q&A	553

Chapter 14 Voice and Video Design 557

“Do I Know This Already?” Quiz	557
Foundation Topics	559
Traditional Voice Architectures	559
PBX and PSTN Switches	559
Local Loop and Trunks	560
Ports	561
Major Analog and Digital Signaling Types	562
<i>Loop-Start Signaling</i>	563
<i>Ground-Start Signaling</i>	563
<i>E&M Signaling</i>	564
<i>CAS and CCS Signaling</i>	565
PSTN Numbering Plan	567
Other PSTN Services	568
<i>Centrex Services</i>	569
<i>Voice Mail</i>	569
<i>Database Services</i>	569
<i>IVR</i>	569
<i>ACD</i>	569
Voice Engineering Terminology	569
<i>Grade of Service</i>	569
<i>Erlangs</i>	569
<i>Centum Call Second</i>	570
<i>Busy Hour</i>	570
<i>Busy-Hour Traffic</i>	570
<i>Blocking Probability</i>	571
<i>Call Detail Records</i>	571

Converged Multiservice Networks	571
VoIP	572
IPT Components	574
<i>Design Goals of IP Telephony</i>	575
IPT Deployment Models	576
<i>Single-Site Deployment</i>	576
<i>Multisite WAN with Centralized Call Processing Model</i>	576
<i>Multisite WAN with Distributed Call Processing Model</i>	577
<i>Unified CallManager Express Deployments</i>	578
Video Deployment Considerations	578
Codecs	580
<i>Analog-to-Digital Signal Conversion</i>	580
<i>Codec Standards</i>	580
VoIP Control and Transport Protocols	581
<i>DHCP, DNS, and TFTP</i>	582
SCCP	582
RTP and RTCP	583
MGCP	584
H.323	584
H.264	587
SIP	588
IPT Design	590
Bandwidth	590
VAD	590
Calculating Voice Bandwidth	591
Delay Components in VoIP Networks	592
Packet Loss	594
Echo Cancellation	595
QoS and Bandwidth Mechanisms for VoIP and Video Networks	595
cRTP	596
IEEE 802.1P	596
Resource Reservation Protocol	597
LFI	597
LLQ	597
Auto QoS	599
IPT Design Recommendations	600
Service Class Recommendations	600

References and Recommended Readings	602
Exam Preparation Tasks	604
Review All Key Topics	604
Complete Tables and Lists from Memory	604
Define Key Terms	605
Q&A	605

Chapter 15 Network Management Protocols 617

“Do I Know This Already?” Quiz	617
Foundation Topics	619
Simple Network Management Protocol	619
SNMP Components	620
MIB	620
SNMP Message Versions	622
<i>SNMPv1</i>	622
<i>SNMPv2</i>	622
<i>SNMPv3</i>	623
Other Network Management Technologies	624
RMON	624
<i>RMON2</i>	625
NetFlow	626
<i>NetFlow Compared to RMON and SNMP</i>	628
CDP	629
LLDP	630
Syslog	630
References and Recommended Reading	631
Exam Preparation Tasks	633
Review All Key Topics	633
Complete Tables and Lists from Memory	633
Define Key Terms	633
Q&A	634

Part V Comprehensive Scenarios and Final Prep

Chapter 16 Comprehensive Scenarios 641

Scenario One: Friendswood Hospital	641
Scenario One Questions	642
Scenario Two: Big Oil and Gas	642
Scenario Two Questions	643

Scenario Three: Video Games Spot	643
Scenario Three Questions	644
Scenario Four: Diamond Communications	645
Scenario Four Questions	646
Scenario Answers	646
Scenario One Answers	646
Scenario Two Answers	650
Scenario Three Answers	651
Scenario Four Answers	652

Chapter 17 Final Preparation 655

Tools for Final Preparation	655
Review Tools on the Companion Website	655
Pearson Cert Practice Test Engine and Questions	655
<i>Download and Install the Software</i>	655
<i>Activate and Download the Practice Exam</i>	656
<i>Activating Other Exams</i>	657
<i>Premium Edition</i>	657
The Cisco Learning Network	657
Memory Tables	657
Chapter-Ending Review Tools	658
Suggested Plan for Final Review/Study	658
Subnetting Practice	658
Using the Exam Engine	659
Summary	660

Part VI Appendixes

Appendix A Answers to the Do I Know This Already?" Quizzes and Q&A Questions 663

Appendix B CCDA 200-310 version 1.0. Exam Updates 699

Appendix C OSI Model, TCP/IP Architecture, and Numeric Conversion 701

OSI Model Overview	701
Physical Layer (OSI Layer 1)	702
Data Link Layer (OSI Layer 2)	703
Network Layer (OSI Layer 3)	703
Transport Layer (OSI Layer 4)	704
Session Layer (OSI Layer 5)	704
Presentation Layer (OSI Layer 6)	705

Application Layer (OSI Layer 7)	705
TCP/IP Architecture	705
Network Interface Layer	706
Internet Layer	706
Host-to-Host Transport Layer	706
Application Layer	706
Example of Layered Communication	706
Numeric Conversion	707
Hexadecimal Numbers	707
Hexadecimal Representation	708
Converting Decimal to Hexadecimal	708
Converting Hexadecimal to Decimal	710
Alternative Method for Converting from Hexadecimal to Decimal	710
Binary Numbers	711
Converting Binary to Hexadecimal	712
Converting Hexadecimal to Binary	712
Converting Binary to Decimal	713
Converting Decimal to Binary Numbers	713
Alternative Method for Converting from Decimal to Binary	714
References and Recommended Readings	715

Glossary 717

Index 730

Elements Available on the Book Website

- Appendix D Memory Tables
- Appendix E Memory Tables Answer Key
- Appendix F Study Planner

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:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold 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.

This page intentionally left blank

Introduction

So, you have worked on Cisco devices for a while, designing networks for your customers, and now you want to get certified? There are several good reasons to do so. The Cisco certification program allows network analysts, design engineers, and network architects to demonstrate their competence in different areas and levels of networking. The prestige and respect that come with a Cisco certification will definitely help you in your career. Your clients, peers, and superiors will recognize you as an expert in networking.

Cisco Certified Design Associate (CCDA) is the associate-level certification that represents knowledge of the design of Cisco internetwork infrastructure. The CCDA demonstrates skills required to design routed and switched networks, LANs, and WANs. The CCDA also has knowledge of campus designs, data centers, network security, voice, and wireless LANs.

Although it is not required, Cisco suggests taking the DESGN 3.0 course before you take the CCDA exam. For more information about the various levels of certification, career tracks, and Cisco exams, go to the Cisco Certifications page at <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html>.

Our goal with this book is to help you pass the 200-310 CCDA exam. This is done by assessment on and coverage of all the exam topics published by Cisco. Reviewing tables and practicing test questions will help you practice your knowledge on all subject areas.

About the 200-310 CCDA Exam

The CCDA exam measures your ability to design networks that meet certain requirements for performance, security, capacity, and scalability. The exam focuses on small- to medium-sized networks. The candidate should have at least one year of experience in the design of small- to medium-sized networks using Cisco products. A CCDA candidate should understand internetworking technologies, including Cisco's enterprise network architecture, IPv4 subnets, IPv6 addressing and protocols, routing, switching, WAN technologies, LAN protocols, security, IP telephony, and network management. The new exam adds topics and updates to virtualization, data centers design, IPv6, voice and video design, wireless LANs, WAN technologies, and security.

The test to obtain CCDA certification is called Designing for Cisco Internetwork Solutions (DESGN) Exam #200-310. It is a computer-based test that has 55 to 65 questions and a 75-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for CCDA course and exam updates at <http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccda.html>.

You can take the exam at Pearson VUE testing centers. You can register with VUE at www.vue.com/cisco/. The CCDA certification is valid for three years. To recertify, you can pass a current CCDA test, pass a CCIE exam, or pass any 300 level, 642 level, or Cisco Specialist exam.

200-310 CCDA Exam Topics

Table I-1 lists the topics of the 200-310 CCDA exam and indicates the part in the book where they are covered.

Table I-1 200-310 CCDA Exam Topics

Exam Topic	Part
1.0 Design Methodologies	
<i>1.1 Describe the Cisco Design lifecycle—PBM (plan, build, manage)</i>	I
<i>1.2 Describe the information required to characterize an existing network as part of the planning for a design change</i>	I
<i>1.3 Describe the use cases and benefits of network characterization tools (SNMP, NBAR, NetFlow)</i>	I
<i>1.4 Compare and contrast the top-down and bottom-up design approaches</i>	I
2.0 Design Objectives	
<i>2.1 Describe the importance and application of modularity in a network</i>	I
<i>2.2 Describe the importance and application of hierarchy in a network</i>	I
<i>2.3 Describe the importance and application of scalability in a network</i>	I
<i>2.4 Describe the importance and application of resiliency in a network</i>	I
<i>2.5 Describe the importance and application of concept of fault domains in a network</i>	I
3.0 Addressing and Routing Protocols in an Existing Network	
<i>3.1 Describe the concept of scalable addressing</i>	
3.1.a Hierarchy	III
3.1.b Summarization	III
3.1.c Efficiency	III
<i>3.2 Design an effective IP addressing scheme</i>	
3.2.a Subnetting	III
3.2.b Summarization	III
3.2.c Scalability	III
3.2.d NAT	III
<i>3.3 Identify routing protocol scalability considerations</i>	
3.3.a Number of peers	III
3.3.b Convergence requirements	III
3.3.c Summarization boundaries and techniques	III

Exam Topic	Part
3.3.d Number of routing entries	III
3.3.e Impact of routing table of performance	III
3.3.f Size of the flooding domain	III
3.3.g Topology	III
3.4 Design a routing protocol expansion	
3.4.a IGP protocols (EIGRP, OSPF, IS-IS)	III
3.4.b BGP (eBGP peering, iBGP peering)	III
4.0 Enterprise Network Design	
4.1 Design a basic campus	
4.1.a Layer 2/Layer 3 demarcation	II
4.1.b Spanning tree	II
4.1.c Ether channels	II
4.1.d First Hop Redundancy Protocols (FHRP)	II
4.1.e Chassis virtualization	II
4.2 Design a basic enterprise network	
4.2.a Layer 3 protocols and redistribution	III
4.2.b WAN connectivity	II
4.2.b(i) Topologies (hub and spoke, spoke to spoke, point to point, full/partial mesh)	II
4.2.b(ii) Connectivity methods (DMVPN, get VPN, MPLS Layer 3 VPN, Layer 2 VPN, static IPsec, GRE, VTI)	II
4.2.b(iii) Resiliency (SLAs, backup links, QoS)	II
4.2.c Connections to the data center	II
4.2.d Edge connectivity	II
4.2.d(i) Internet connectivity	II
4.2.d(ii) ACLs and firewall placements	II
4.2.d(iii) NAT placement	II
4.3 Design a basic branch network	
4.3.a Redundancy	II
4.3.a(i) Connectivity	II
4.3.a(ii) Hardware	II
4.3.a(iii) Service provider	II
4.3.b Link capacity	II
4.3.b(i) Bandwidth	II

Exam Topic	Part
4.3.b(ii) Delay	II
5.0 Considerations for Expanding an Existing Network	
<i>5.1 Describe design considerations for wireless network architectures</i>	
5.1.a Physical and virtual controllers	II
5.1.b Centralized and decentralized designs	II
<i>5.2 Identify integration considerations and requirements for controller-based wireless networks</i>	
5.2.a Traffic flows	II
5.2.b Bandwidth consumption	II
5.2.c AP and controller connectivity	II
5.2.d QoS	II
<i>5.3 Describe security controls integration considerations</i>	
5.3.a Traffic filtering and inspection	IV
5.3.b Firewall and IPS placement and functionality	IV
<i>5.4 Identify traffic flow implications as a result of security controls</i>	
5.4.a Client access methods	IV
5.4.b Network access control	IV
<i>5.5 Identify high-level considerations for collaboration (voice, streaming video, interactive video) applications</i>	IV
5.5.a QoS (shaping vs. policing, trust boundaries, jitter, delay, loss)	IV
5.5.b Capacity	IV
5.5.c Convergence time	IV
5.5.d Service placement	IV
<i>5.6 Describe the concepts of virtualization within a network design</i>	II
<i>5.7 Identify network elements that can be virtualized</i>	
5.7.a Physical elements (chassis, VSS, VDC, contexts)	II
5.7.b Logical elements (routing elements, tunneling, VRFs, VLANs)	II
<i>5.8 Describe the concepts of network programmability within a network design</i>	
5.8.a APIs	II
5.8.b Controllers	II
5.8.c Application Centric Infrastructure (ACI)	II

Exam Topic	Part
<i>5.9 Describe data center components</i>	
5.9.a Server load balancing basics	II
5.9.b Blocking vs. non-blocking Layer 2	II
5.9.c Layer 2 extension	II

About the CCDA 200-310 Official Cert Guide

This book maps to the topic areas of the 200-310 CCDA exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics for which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. This book is designed to help you pass the CCDA exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **“Do I Know This Already?” quiz:** Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
- **Foundation Topics:** This is the core section of each chapter. It explains the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
 - **Review All the Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All the Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.

- **Complete the Tables and Lists from Memory:** To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list.
- **Define Key Terms:** Although the exam may be unlikely to ask a question such as “Define this term,” the CCDA exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Q&A:** Confirm that you understand the content you just covered.

How This Book Is Organized

This book contains 16 core chapters—Chapters 1 through 16. Chapter 17 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCDA exam. The core chapters are organized into parts. They cover the following topics:

Part I: General Network Design

- **Chapter 1: Network Design Methodology** covers Cisco architectures for the enterprise network; the Plan, Design, Manage (PDM) network lifecycle; the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) methodology; and the process of completing a network design.
- **Chapter 2: Network Design Models** covers hierarchical network models, the Cisco Enterprise Architecture model, and high-availability network services.

Part II: LAN and WAN Design

- **Chapter 3: Enterprise LAN Design** covers LAN media, campus LAN design and models, and best practices for campus networks.
- **Chapter 4: Data Center Design** covers enterprise data center design fundamentals, network programmability, data center challenges, virtualization technologies, data center interconnects, and load balancing in the DC.
- **Chapter 5: Wireless LAN Design** covers technologies and design options used for wireless LANs.
- **Chapter 6: WAN Technologies and the Enterprise Edge** examines technologies, design methodologies, DMZ connectivity, Internet connectivity, VPN network design, and requirements for the enterprise WANs.
- **Chapter 7: WAN Design** covers WAN design for the Enterprise WAN and enterprise branch, including remote access and virtual private network (VPN) architectures.

Part III: The Internet Protocol and Routing Protocols

- **Chapter 8: Internet Protocol Version 4 Design** covers the header, addressing, subnet design, and protocols used by IPv4.
- **Chapter 9: Internet Protocol Version 6 Design** covers the header, addressing, design best practices, and protocols used by IPv6.
- **Chapter 10: Routing Protocol Characteristics, RIP, EIGRP, and IS-IS** covers routing protocol characteristics, metrics, RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP), and Intermediate System to Intermediate System (IS-IS) characteristics and design.
- **Chapter 11: OSPF, BGP, Route Manipulation, and IP Multicast** covers Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), route summarization, route redistribution, route filtering, and IP multicast.

Part IV: Security, Convergence, Network Management

- **Chapter 12: Managing Security** examines security management, security policy, threats, risks, security compliance, and trust and identity management.
- **Chapter 13: Security Solutions** covers Cisco SAFE architecture, security technologies, and design options for securing the enterprise.
- **Chapter 14: Voice and Video Design** reviews traditional voice architectures, integrated multiservice networks, Cisco's IPT architecture and call processing deployment models, video deployment considerations, and IPT design.
- **Chapter 15: Network Management Protocols** covers Simple Network Management Protocol (SNMP), Remote Monitor (RMON), NetFlow, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and syslog.

Part V: Comprehensive Scenarios and Final Prep

- **Chapter 16: Comprehensive Scenarios** provides network case studies for further comprehensive study.
- **Chapter 17: Final Preparation** identifies tools for final exam preparation and helps you develop an effective study plan. It contains tips on how to best use the web-based material to study.

Part VI: Appendixes

- **Appendix A: Answers to the "Do I Know This Already?" Quizzes and Q&A Questions** includes the answers to all the questions from Chapters 1 through 15.
- **Appendix B: CCDA Exam Updates: Version 1.0** provides instructions for finding updates to the exam and this book when and if they occur.
- **Appendix C: OSI Model, TCP/IP Architecture, and Numeric Conversion** reviews the Open Systems Interconnection (OSI) reference model to give you a better understanding of internetworking. It reviews the TCP/IP architecture and also reviews the techniques to convert between decimal, binary, and hexadecimal numbers. Although there might not be a specific question on the exam about converting a binary number to decimal, you need to know how to do so to do problems on the test.

- **Appendix D: Memory Tables** (a website-only appendix) contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exam. This appendix is available in PDF format on the companion website; it is not in the printed book.
- **Appendix E: Memory Tables Answer Key** (a website-only appendix) contains the answer key for the memory tables in Appendix D. This appendix is available in PDF format on the companion website; it is not in the printed book.
- **Appendix F: Study Planner** is a spreadsheet, available from the book website, with major study milestones, where you can track your progress through your study.

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the authors that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9781587144547.
3. Answer the challenge question as proof of purchase.
4. Click the Access Bonus Content link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps, please visit www.pearsonITcertification.com/contact and select the “Site Problems / Comments” option. Our customer service representatives will assist you.

Pearson IT Certification Practice Test Engine and Questions

The companion website includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode, or take a simulated exam that mimics real exam conditions. You can also serve up questions in Flash Card Mode, which will display just the question and no answers, challenging you to state the answer in your own words before checking the actual answers to verify your work.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam (the database of exam questions) is not on this site.

Note The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software

The Pearson IT Certification Practice Test is a **Windows-only desktop application**. You can run it on a Mac using a Windows virtual machine, but it was built specifically for the PC platform. The minimum system requirements are as follows:

- Windows 10, Windows 8.1, or Windows 7
- Microsoft .NET Framework 4.0 Client
- Pentium-class 1GHz processor (or equivalent)
- 512 MB of RAM
- 650 MB of disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is routine as compared with other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the access code card sleeve in the back of the book.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to Windows prompts as with any typical software installation process.

The installation process will give you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

1. Start the Pearson IT Certification Practice Test software from the Windows Start menu or from your desktop shortcut icon.

2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate Exam** button.
3. At the next screen, enter the activation key from the paper inside the cardboard sleeve in the back of the book. Once this is entered, click the **Activate** button.
4. The activation process will download the practice exam. Click **Next**, and then click **Finish**.

When the activation process completes, the **My Products** tab should list your new exam. If you do not see the exam, make sure you have selected the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam you have already activated and downloaded, display the **Tools** tab and click the **Update Products** button. Updating your exams will ensure that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, display the Tools tab and click the **Update Application** button. You can then ensure that you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process, and the registration process, only has to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another Pearson IT Certification Cert Guide, extract the activation code from the cardboard sleeve in the back of that book; you do not even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running) and perform Steps 2 through 4 from the previous list.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the “Do I Know This Already?” quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70 percent off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.



This chapter covers the following subjects:

Cisco Architectures for the Enterprise

Plan, Build, and Manage Lifecycle

Prepare, Plan, Design, Implement, Operate, and Optimize Phases

Identifying Customer Requirements

Characterizing the Existing Network

Designing the Network Topology and Solutions

Networks can become complex and difficult to manage. Network architectures and design methodologies help you manage the complexities of networks. This chapter provides an overview of Cisco's architectures for the enterprise and the Plan, Build, Manage (PBM) network lifecycle. This chapter also describes steps in design methodology and contents of design documents.



This chapter covers the following subjects:

Hierarchical Network Models

Cisco Enterprise Architecture Model

High Availability Network Services

This chapter reviews the hierarchical network model and introduces Cisco's Enterprise Architecture model. This architecture model separates network design into more manageable modules. This chapter also addresses the use of device, media, and route redundancy to improve network availability.

CHAPTER 2

Network Design Models

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz helps you identify your strengths and deficiencies in this chapter’s topics.

The eight-question quiz, derived from the major sections in the “Foundation Topics” portion of the chapter, helps you determine how to spend your limited study time.

Table 2-1 outlines the major topics discussed in this chapter and the “Do I Know This Already?” quiz questions that correspond to those topics.

Table 2-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Hierarchical Network Models	1, 3
Cisco Enterprise Architecture Model	2, 5, 6, 7
High Availability Network Services	4, 8

1. In the hierarchical network model, which layer is responsible for fast transport?
 - a. Network layer
 - b. Core layer
 - c. Distribution layer
 - d. Access layer
2. Which Enterprise Architecture model component interfaces with the service provider (SP)?
 - a. Campus infrastructure
 - b. Access layer
 - c. Enterprise edge
 - d. Edge distribution
3. In the hierarchical network model, at which layer do security filtering, address aggregation, and media translation occur?
 - a. Network layer
 - b. Core layer
 - c. Distribution layer
 - d. Access layer

- 4.** Which of the following is (are) a method (methods) of workstation-to-router redundancy in the access layer?
 - a.** AppleTalk Address Resolution Protocol (AARP)
 - b.** Hot Standby Router Protocol (HSRP)
 - c.** Virtual Router Redundancy Protocol (VRRP)
 - d.** Answers b and c
 - e.** Answers a, b, and c
- 5.** The network-management module has tie-ins to which component(s)?
 - a.** Campus infrastructure
 - b.** Server farm
 - c.** Enterprise edge
 - d.** SP edge
 - e.** Answers a and b
 - f.** Answers a, b, and c
 - g.** Answers a, b, c, and d
- 6.** Which of the following is an SP edge module in the Cisco Enterprise Architecture model?
 - a.** Public switched telephone network (PSTN) service
 - b.** Edge distribution
 - c.** Server farm
 - d.** Core layer
- 7.** In which module would you place Cisco Unified Communications Manager (CUCM)?
 - a.** Campus core
 - b.** E-commerce
 - c.** Server farm
 - d.** Edge distribution farm
- 8.** High availability, port security, and rate limiting are functions of which hierarchical layer?
 - a.** Network layer
 - b.** Core layer
 - c.** Distribution layer
 - d.** Access layer

Foundation Topics

With the complexities of network design, the CCDA needs to understand network models used to simplify the design process. The hierarchical network model was one of the first Cisco models that divided the network into core, distribution, and access layers.

The Cisco Enterprise Architecture model provides a functional modular approach to network design. In addition to a hierarchy, modules are used to organize server farms, network management, campus networks, WANs, and the Internet. A modular approach to network design allows for higher scalability, better resiliency, and easier fault isolation of the network.

2

Hierarchical Network Models



Hierarchical models enable you to design internetworks that use specialization of function combined with a hierarchical organization. Such a design simplifies the tasks required to build a network that meets current requirements and can grow to meet future requirements. Hierarchical models use layers to simplify the tasks for internetworking. Each layer can focus on specific functions, allowing you to choose the right systems and features for each layer. Hierarchical models apply to both LAN and WAN design.

Benefits of the Hierarchical Model

The benefits of using hierarchical models for your network design include the following:

- Cost savings
- Ease of understanding
- Modular network growth
- Improved fault isolation

After adopting hierarchical design models, many organizations report cost savings because they are no longer trying to do everything in one routing or switching platform. The model's modular nature enables appropriate use of bandwidth within each layer of the hierarchy, reducing the provisioning of bandwidth in advance of actual need.

Keeping each design element simple and functionally focused facilitates ease of understanding, which helps control training and staff costs. You can distribute network monitoring and management reporting systems to the different layers of modular network architectures, which also helps control management costs.

Hierarchical design facilitates changes and growth. In a network design, modularity lets you create design elements that you can replicate as the network grows—allowing maximum scalability. As each element in the network design requires change, the cost and complexity of making the upgrade are contained to a small subset of the overall network. In large, flat network architectures, changes tend to impact a large number of systems. Limited mesh topologies within a layer or component, such as the campus core or backbone connecting central sites, retain value even in the hierarchical design models.

Structuring the network into small, easy-to-understand elements improves fault isolation. Network managers can easily understand the transition points in the network, which helps identify failure points. It is more difficult to troubleshoot if hierarchical design is not used because the network is not divided into segments.

Today's fast-converging protocols were designed for hierarchical topologies. To control the impact of routing-protocol processing and bandwidth consumption, you must use modular hierarchical topologies with protocols designed with these controls in mind, such as the Open Shortest Path First (OSPF) routing protocol.

Hierarchical network design facilitates route summarization. Enhanced Interior Gateway Routing Protocol (EIGRP) and all other routing protocols benefit greatly from route summarization. Route summarization reduces routing-protocol overhead on links in the network and reduces routing-protocol processing within the routers. It is less possible to provide route summarization if the network is not hierarchical.

Hierarchical Network Design



As shown in Figure 2-1, a traditional hierarchical LAN design has three layers:

- The core layer provides fast transport between distribution switches within the enterprise campus.
- The distribution layer provides policy-based connectivity.
- The access layer provides workgroup and user access to the network.

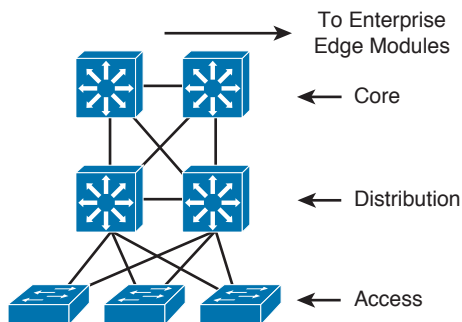


Figure 2-1 Hierarchical network design has three layers: core, distribution, and access

Each layer provides necessary functionality to the enterprise campus network. You do not need to implement the layers as distinct physical entities. You can implement each layer in one or more devices or as cooperating interface components sharing a common chassis. Smaller networks can “collapse” multiple layers to a single device with only an implied hierarchy. Maintaining an explicit awareness of hierarchy is useful as the network grows.

Core Layer

The core layer is the network's high-speed switching backbone that is crucial to corporate communications. It is also referred as the backbone. The core layer should have the following characteristics:

- Fast transport
- High reliability
- Redundancy
- Fault tolerance
- Low latency and good manageability
- Avoidance of CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes
- Limited and consistent diameter
- QoS

When a network uses routers, the number of router hops from edge to edge is called the diameter. As noted, it is considered good practice to design for a consistent diameter within a hierarchical network. The trip from any end station to another end station across the backbone should have the same number of hops. The distance from any end station to a server on the backbone should also be consistent.

Limiting the internetwork's diameter provides predictable performance and ease of troubleshooting. You can add distribution layer routers and client LANs to the hierarchical model without increasing the core layer's diameter. Use of a block implementation isolates existing end stations from most effects of network growth.

Distribution Layer

The network's distribution layer is the isolation point between the network's access and core layers. The distribution layer can have many roles, including implementing the following functions:

- Policy-based connectivity (for example, ensuring that traffic sent from a particular network is forwarded out one interface while all other traffic is forwarded out another interface)
- Redundancy and load balancing
- Aggregation of LAN wiring closets
- Aggregation of WAN connections
- QoS
- Security filtering
- Address or area aggregation or summarization
- Departmental or workgroup access
- Broadcast or multicast domain definition
- Routing between virtual LANs (VLANs)
- Media translations (for example, between Ethernet and Token Ring)
- Redistribution between routing domains (for example, between two different routing protocols)
- Demarcation between static and dynamic routing protocols

You can use several Cisco IOS Software features to implement policy at the distribution layer:

- Filtering by source or destination address
- Filtering on input or output ports
- Hiding internal network numbers by route filtering
- Static routing
- QoS mechanisms, such as priority-based queuing

The distribution layer provides aggregation of routes providing route summarization to the core. In the campus LANs, the distribution layer provides routing between VLANs that also apply security and QoS policies.

Access Layer

The access layer provides user access to local segments on the network. The access layer is characterized by switched LAN segments in a campus environment. Microsegmentation using LAN switches provides high bandwidth to workgroups by reducing the number of devices on Ethernet segments. Functions of the access layer include the following:

- Layer 2 switching
- High availability
- Port security
- Broadcast suppression
- QoS classification and marking and trust boundaries
- Rate limiting/policing
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Spanning tree
- Trust classification
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP
- Network Access Control (NAC)
- Auxiliary VLANs

You implement high availability models at the access layer. The section “High Availability Network Services” covers availability models. The LAN switch in the access layer can control access to the port and limit the rate at which traffic is sent to and from the port. You can implement access by identifying the MAC address using ARP, trusting the host, and using access lists.

Other chapters of this book cover the other functions in the list.

For small office/home office (SOHO) environments, the entire hierarchy collapses to interfaces on a single device. Remote access to the central corporate network is through traditional WAN technologies such as ISDN, Frame Relay, and leased lines. You can implement

features such as dial-on-demand routing (DDR) and static routing to control costs. Remote access can include virtual private network (VPN) technology.

Table 2-2 summarizes the hierarchical layers.

Table 2-2 Cisco Enterprise Architecture Model

Hierarchical Layer	Description
Core	- Fast transport - High reliability - Redundancy - Fault tolerance - Low latency and good manageability - Avoidance of slow packet manipulation caused by filters or other processes - Limited and consistent diameter - QoS
Distribution	- Policy-based connectivity - Redundancy and load balancing - Aggregation of LAN wiring closets - Aggregation of WAN connections - QoS - Security filtering - Address or area aggregation or summarization - Departmental or workgroup access - Broadcast or multicast domain definition - Routing between VLANs - Media translations (for example, between Ethernet and Token Ring) - Redistribution between routing domains (for example, between two different routing protocols) - Demarcation between static and dynamic routing protocols
Access	- Layer 2 switching - High availability - Port security - Broadcast suppression - QoS

Hierarchical Layer	Description
Access (<i>continued</i>)	Rate limiting ARP inspection VACLs Spanning tree Trust classification Network Access Control (NAC) PoE and auxiliary VLANs for VoIP

Hierarchical Model Examples

You can implement the hierarchical model by using a traditional switched campus design or routed campus network. Figure 2-2 is an example of a switched hierarchical design in the enterprise campus. In this design, the core provides high-speed transport between the distribution layers. The building distribution layer provides redundancy and allows policies to be applied to the building access layer. Layer 3 links between the core and distribution switches are recommended to allow the routing protocol to take care of load balancing and fast route redundancy in the event of a link failure. The distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network. Inter-VLAN communications are routed in the distribution layer. Route summarization is configured under the routing protocol on interfaces towards the core layer. The drawback with this design is that Spanning Tree Protocol (STP) allows only one of the redundant links between the access switch and the distribution switch to be active. In the event of a failure, the second link becomes active, but at no point does load balancing occur.

Figure 2-3 shows examples of a routed hierarchical design. In this design, the Layer 3 boundary is pushed toward the access layer. Layer 3 switching occurs in access, distribution, and core layers. Route filtering is configured on interfaces toward the access layer. Route summarization is configured on interfaces toward the core layer. The benefit of this design is that load balancing occurs from the access layer since the links to the distribution switches are routed.

Another solution for providing redundancy between the access and distribution switching is the Virtual Switching System (VSS). VSS solves the STP looping problem by converting the distribution switching pair into a logical single switch. It removes STP and negates the need for Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP).

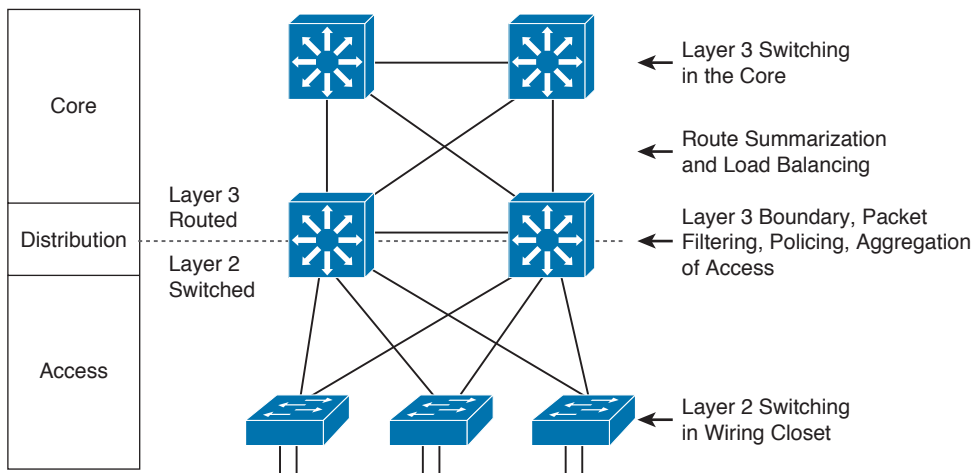


Figure 2-2 *Switched Hierarchical Design*

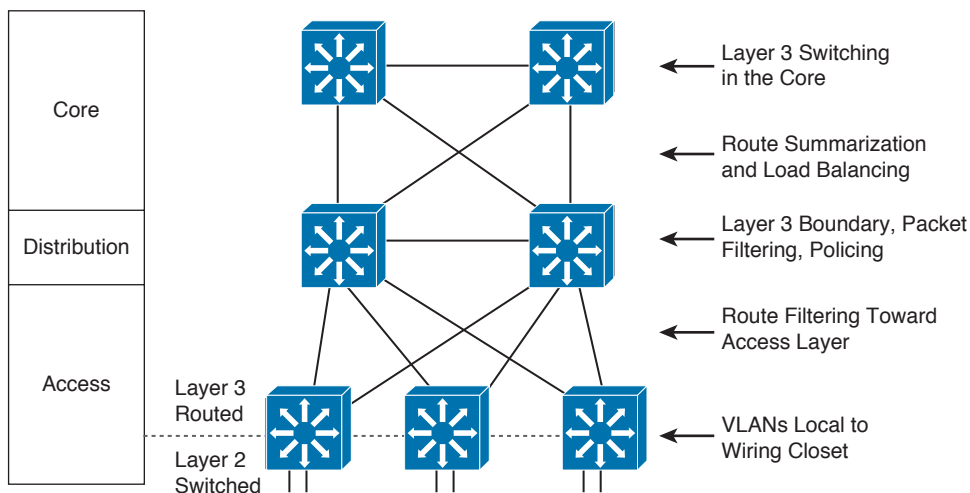
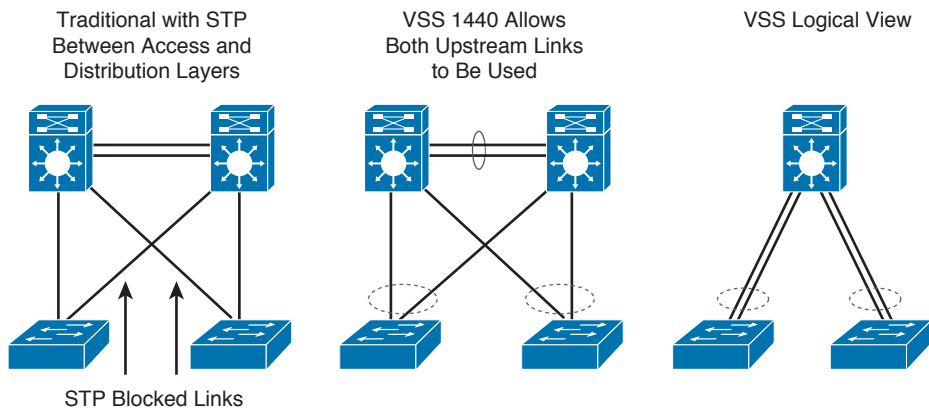


Figure 2-3 *Routed hierarchical design*

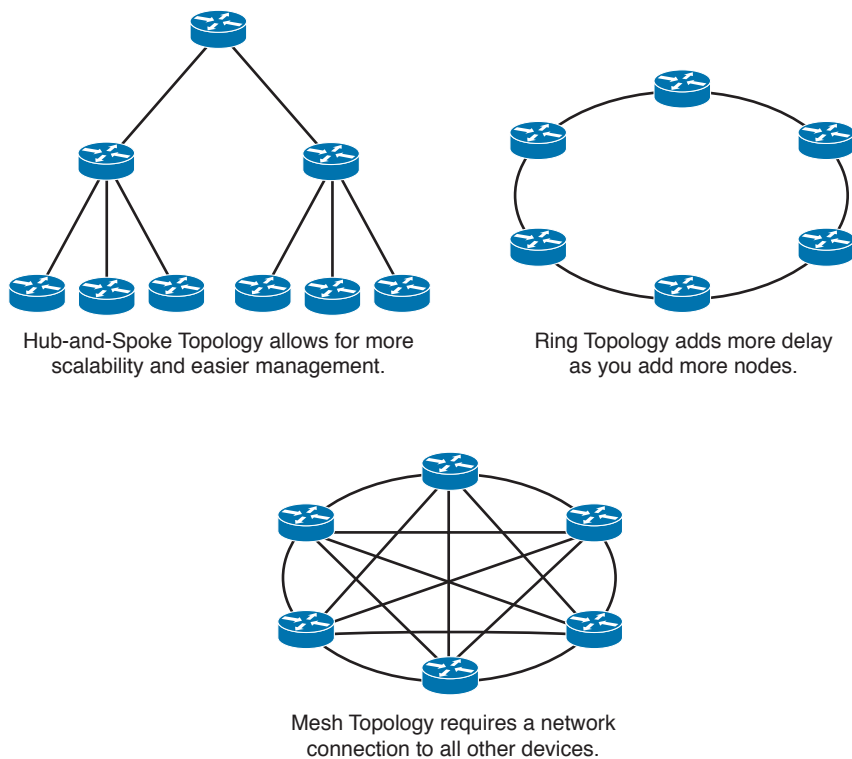
With VSS, the physical topology changes as each access switch has a single upstream distribution switch versus having two upstream distribution switches. VSS is configured only on Cisco 6500 switches using the VSS Supervisor 720-10G. As shown in Figure 2-4, the two switches are connected via 10GE links called virtual switch links (VSLs), which makes them seem as a single switch. The key benefits of VSS include the following:

- Layer 3 switching can be used toward the access layer, enhancing nonstop communication.
- Scales system bandwidth up to 1.44 Tbps.
- Simplified management of a single configuration of the VSS distribution switch.
- Better return on investment (ROI) via increased bandwidth between the access layer and the distribution layer.
- Supported on Catalyst 4500, 6500, and 6800 switches.

**Figure 2-4** VSS

Hub-and-Spoke Design

For designing networks, the hub-and-spoke design provides better convergence times than ring topology. The hub-and-spoke design, illustrated in Figure 2-5, also scales better and is easier to manage than ring or mesh topologies. For example, implementing security policies in a full mesh topology would become unmanageable because you would have to configure policies at each point location.

**Figure 2-5** Hub-and-spoke design

Collapsed Core Design

One alternative to the three-layer hierarchy is the collapsed core design. It is a two-layer hierarchy used with smaller networks. It is commonly used on sites with a single building with just multiple floors. As shown in Figure 2-6, the core and distribution layers are merged, providing all the services needed for those layers. Design parameters to decide if you need to migrate to the three-layer hierarchy include not enough capacity and throughput at the distribution layer, network resiliency, and geographic dispersion.

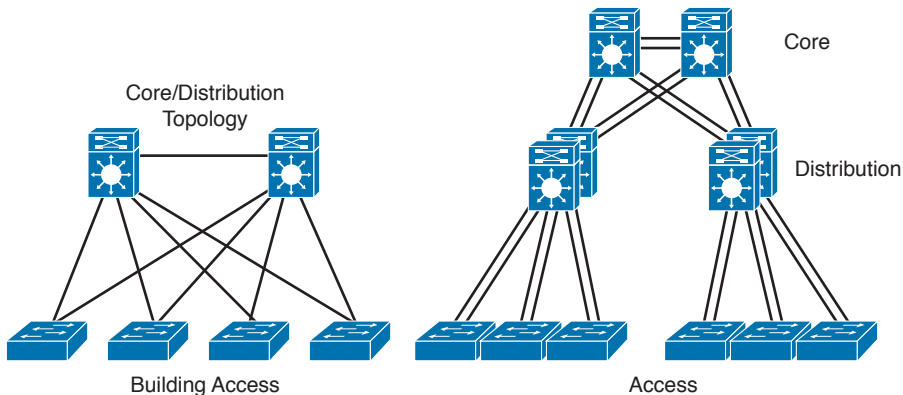


Figure 2-6 *Collapsed core design*

Cisco Enterprise Architecture Model

The Cisco Enterprise Architecture model facilitates the design of larger, more scalable networks.

As networks become more sophisticated, it is necessary to use a more modular approach to design than just WAN and LAN core, distribution, and access layers. The architecture divides the network into functional network areas and modules. These areas and modules of the Cisco Enterprise Architecture are

- Enterprise campus area
- Enterprise data center module
- Enterprise branch module
- Enterprise teleworker module

The Cisco Enterprise Architecture model maintains the concept of distribution and access components connecting users, WAN services, and server farms through a high-speed campus backbone. The modular approach in design should be a guide to the network architect. In smaller networks, the layers can collapse into a single layer, even a single device, but the functions remain.

Figure 2-7 shows the Cisco Enterprise Architecture model. The enterprise campus area contains a campus infrastructure that consists of core, building distribution, and building access layers, with a data center module. The enterprise edge area consists of the Internet,

e-commerce, VPN, and WAN modules that connect the enterprise to the service provider's facilities. The SP edge area provides Internet, public switched telephone network (PSTN), and WAN services to the enterprise.

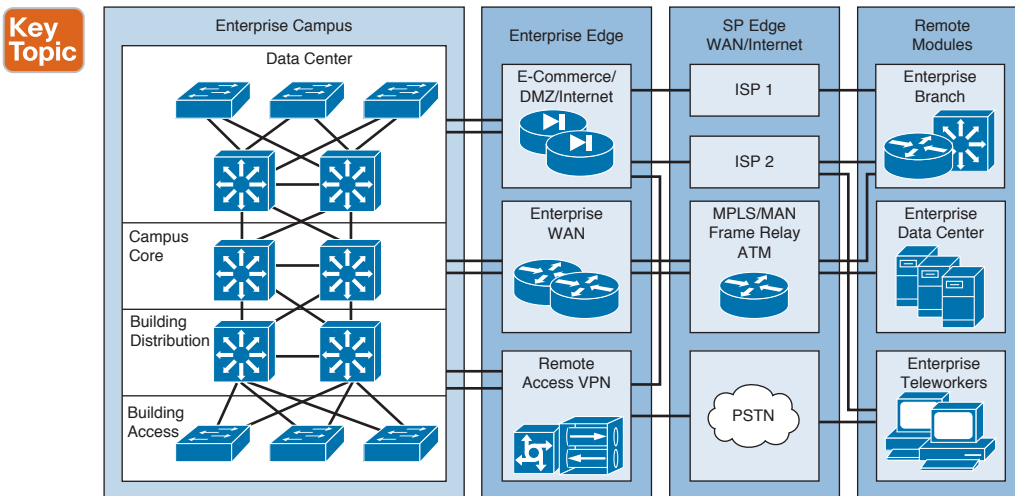


Figure 2-7 Cisco Enterprise Architecture model

The network management servers reside in the campus infrastructure but have tie-ins to all the components in the enterprise network for monitoring and management.

The enterprise edge connects to the edge-distribution module of the enterprise campus. In small and medium sites, the edge distribution can collapse into the campus backbone component. It provides connectivity to outbound services that are further described in later sections.

Enterprise Campus Module

The enterprise campus consists of the following submodules:

- Campus core
- Building distribution and aggregation switches
- Building access
- Server farm/data center

Figure 2-8 shows the Enterprise Campus model. The campus infrastructure consists of the campus core, building distribution, and building access layers. The campus core provides a high-speed switched backbone between buildings, to the server farm, and towards the enterprise edge. This segment consists of redundant and fast-convergence connectivity. The building distribution layer aggregates all the closet access switches and performs access control, QoS, route redundancy, and load balancing. The building access switches provide VLAN access, PoE for IP phones and wireless access points, broadcast suppression, and spanning tree.

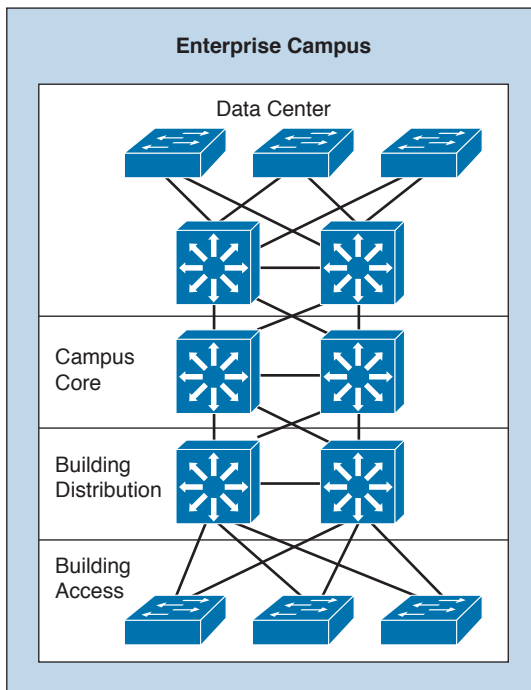


Figure 2-8 *Enterprise Campus model*

The server farm or data center provides high-speed access and high availability (redundancy) to the servers. Enterprise servers such as file and print servers, application servers, email servers, Dynamic Host Configuration Protocol (DHCP) servers, and Domain Name System (DNS) servers are placed in the server farm. Cisco Unified CallManager servers are placed in the server farm for IP telephony networks. Network management servers are located in the server farm, but these servers link to each module in the campus to provide network monitoring, logging, trending, and configuration management.

An enterprise campus infrastructure can apply to small, medium, and large locations. In most instances, large campus locations have a three-tier design with a wiring-closet component (building access layer), a building distribution layer, and a campus core layer. Small campus locations likely have a two-tier design with a wiring-closet component (Ethernet access layer) and a backbone core (collapsed core and distribution layers). It is also possible to configure distribution functions in a multilayer building access device to maintain the focus of the campus backbone on fast transport. Medium-sized campus network designs sometimes use a three-tier implementation or a two-tier implementation, depending on the number of ports, service requirements, manageability, performance, and availability required.

Enterprise Edge Area

As shown in Figure 2-9, the enterprise edge consists of the following submodules:

- Business web applications and databases, e-commerce networks and servers
- Internet connectivity and demilitarized zone (DMZ)
- VPN and remote access
- Enterprise WAN connectivity

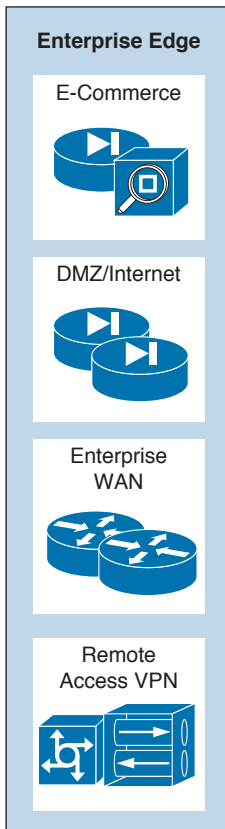


Figure 2-9 *Enterprise Edge module*

E-Commerce Module

The e-commerce submodule of the enterprise edge provides highly available networks for business services. It uses the high availability designs of the server farm module with the Internet connectivity of the Internet module. Design techniques are the same as those described for these modules. Devices located in the e-commerce submodule include the following:

- **Web and application servers:** Primary user interface for e-commerce navigation
- **Database servers:** Contain the application and transaction information

- **Firewall and firewall routers:** Govern the communication between users of the system
- **Network intrusion prevention systems (IPS):** Provide monitoring of key network segments in the module to detect and respond to attacks against the network
- **Multilayer switch with IPS modules:** Provide traffic transport and integrated security monitoring

Internet Connectivity Module

The Internet submodule of the enterprise edge provides services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISPs) is also provided. Components of this submodule include the following:

- **Firewall and firewall routers:** Provide protection of resources, stateful filtering of traffic, and VPN termination for remote sites and users
- **Internet edge routers:** Provide basic filtering and multilayer connectivity
- **FTP and HTTP servers:** Provide for web applications that interface the enterprise with the world via the public Internet
- **SMTP relay servers:** Act as relays between the Internet and the intranet mail servers
- **DNS servers:** Serve as authoritative external DNS servers for the enterprise and relay internal requests to the Internet

Several models connect the enterprise to the Internet. The simplest form is to have a single circuit between the enterprise and the SP, as shown in Figure 2-10. The drawback is that you have no redundancy or failover if the circuit fails.

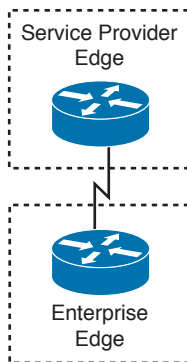


Figure 2-10 *Simple Internet connection*

You can use multihoming solutions to provide redundancy or failover for Internet service. Figure 2-11 shows four Internet multihoming options:

- **Option 1:** Single router, dual links to one ISP
- **Option 2:** Single router, dual links to two ISPs
- **Option 3:** Dual routers, dual links to one ISP
- **Option 4:** Dual routers, dual links to two ISPs

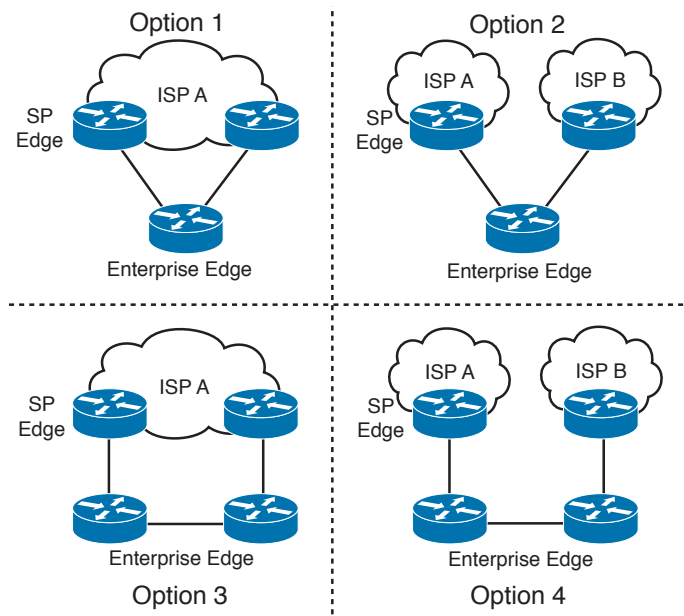


Figure 2-11 Internet multihoming options

Option 1 provides link redundancy but does not provide ISP and local router redundancy. Option 2 provides link and ISP redundancy but does not provide redundancy for a local router failure. Option 3 provides link and local router redundancy but does not provide for an ISP failure. Option 4 provides for full redundancy of the local router, links, and ISPs.

VPN/Remote Access

The VPN/remote access module of the enterprise edge provides remote-access termination services, including authentication for remote users and sites. Components of this submodule include the following:

- **Firewalls:** Provide stateful filtering of traffic, authenticate trusted remote sites, and provide connectivity using IPsec tunnels
- **Dial-in access concentrators:** Terminate legacy dial-in connections and authenticate individual users
- **Cisco Adaptive Security Appliances (ASAs):** Terminate IPsec tunnels, authenticate individual remote users, and provide firewall and intrusion prevention services
- Network intrusion prevention system (IPS) appliances

If you use a remote-access terminal server, this module connects to the PSTN. Today's networks often prefer VPNs over remote-access terminal servers and dedicated WAN links. VPNs reduce communication expenses by leveraging the infrastructure of SPs. For critical applications, the cost savings might be offset by a reduction in enterprise control and the loss of deterministic service. Remote offices, mobile users, and home offices access the Internet using the local SP with secured IPsec tunnels to the VPN/remote access submodule via the Internet submodule.

Figure 2-12 shows a VPN design. Branch offices obtain local Internet access from an ISP. Teleworkers also obtain local Internet access. VPN software creates secured VPN tunnels to the VPN server that is located in the VPN submodule of the enterprise edge.

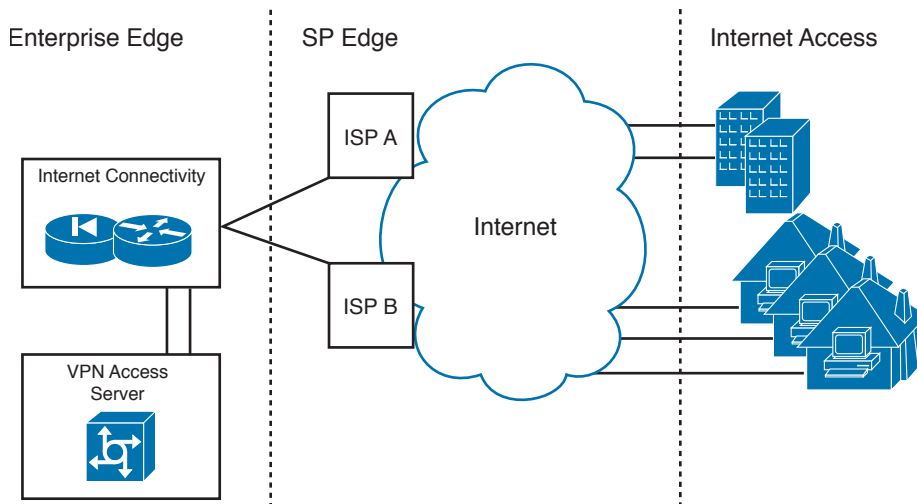


Figure 2-12 VPN architecture

Enterprise WAN

The enterprise edge of the enterprise WAN includes access to WANs. WAN technologies include the following:

- Multiprotocol Label Switching (MPLS)
- Metro Ethernet
- Leased lines
- Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)
- PPP
- Frame Relay
- ATM
- Cable
- Digital subscriber line (DSL)
- Wireless

Chapter 6, “WAN Technologies and the Enterprise Edge,” and Chapter 7, “WAN Design,” cover these WAN technologies. Routers in the enterprise WAN provide WAN access, QoS, routing, redundancy, and access control to the WAN. Of these WAN technologies, MPLS is the most popular WAN technology used today. For MPLS networks, the WAN routers prioritize IP packets based on configured differentiated services code point (DSCP) values to use one of several MPLS QoS levels. Figure 2-13 shows the WAN module connecting to the Frame Relay SP edge. The enterprise edge routers in the WAN module connect to the SP’s Frame Relay switches.

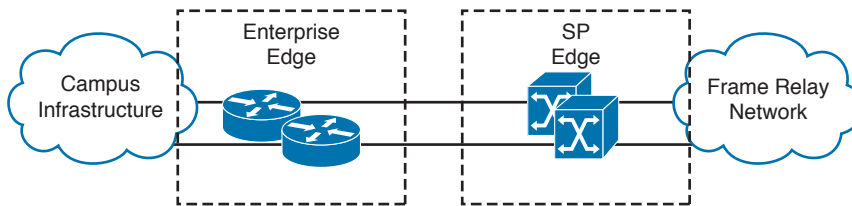


Figure 2-13 *WAN module*

Use the following guidelines when designing the enterprise edge:

- Determine the connection needed to connect the corporate network to the Internet. These connections are assigned to the Internet connectivity module.
- Create the e-commerce module for customers and partners that require Internet access to business and database applications.
- Design the remote access/VPN module for VPN access to the internal network from the Internet. Implement the security policy and configure authentication and authorization parameters.
- Assign the edge sections that have permanent connections to remote branch offices. Assign these to the WAN, metro area network (MAN), and VPN module.

Service Provider Edge Module

The SP edge module, shown in Figure 2-14, consists of SP edge services such as the following:

- Internet services
- PSTN services
- WAN services

Enterprises use SPs to acquire network services. ISPs offer enterprises access to the Internet. ISPs can route the enterprise's networks to their network and to upstream and peer Internet providers. ISPs can provide Internet services via Ethernet, DSL, or T1/DS3 access. It is common now for the SP to have their ISP router at the customer site and provide Ethernet access to the customer. Connectivity with multiple ISPs was described in the section "Internet Connectivity Module."

For voice services, PSTN providers offer access to the global public voice network. For the enterprise network, the PSTN lets dialup users access the enterprise via analog or cellular wireless technologies. It is also used for WAN backup using ISDN services.

WAN SPs offer MPLS, Frame Relay, ATM, and other WAN services for enterprise site-to-site connectivity with permanent connections. These and other WAN technologies are described in Chapter 6.

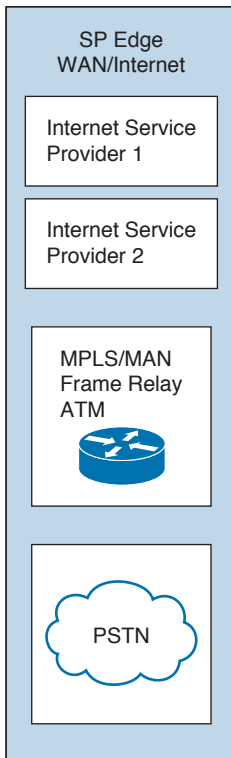


Figure 2-14 *WAN/Internet SP edge module*

Remote Modules

The remote modules of the Cisco Enterprise Architecture model are the enterprise branch, enterprise data center, and enterprise teleworker modules.

Enterprise Branch Module

The enterprise branch normally consists of remote offices or sales offices. These branch offices rely on the WAN to use the services and applications provided in the main campus. Infrastructure at the remote site usually consists of a WAN router and a small LAN switch, as shown in Figure 2-15. As an alternative to MPLS, it is common to use site-to-site IPsec VPN technologies to connect to the main campus.

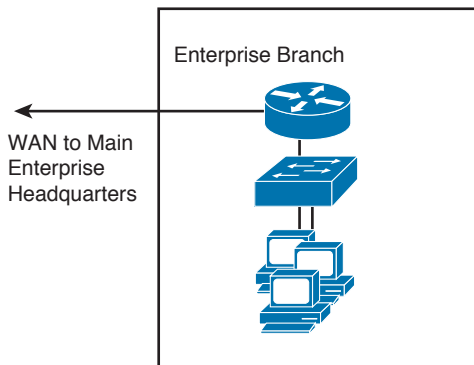


Figure 2-15 *Enterprise branch module*

Enterprise Data Center Module

The enterprise data center uses the network to enhance the server, storage, and application servers. The offsite data center provides disaster recovery and business continuance services for the enterprise. Highly available WAN services are used to connect the enterprise campus to the remote enterprise data center. The data center components include the following:

- **Network infrastructure:** Gigabit and 10 Gigabit Ethernet, InfiniBand, optical transport, and storage switching
- **Interactive services:** Computer infrastructure services, storage services, security, and application optimization
- **DC management:** Cisco Fabric Manager and Cisco VFrame for server and service management

The enterprise data center is covered in detail in Chapter 4, “Data Center Design.”

Enterprise Teleworker Module

The enterprise teleworker module consists of a small office or a mobile user who needs to access services of the enterprise campus. As shown in Figure 2-16, mobile users connect from their homes, hotels, or other locations using dialup or Internet access lines. VPN clients are used to allow mobile users to securely access enterprise applications. The Cisco Virtual Office solution provides a solution for teleworkers that is centrally managed using small integrated service routers (ISRs) in the VPN solution. IP phone capabilities are also provided in the Cisco Virtual Office solution, providing corporate voice services for mobile users.

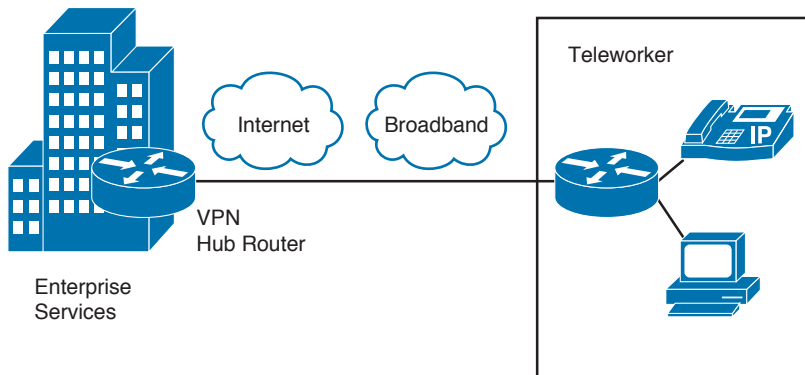


Figure 2-16 Enterprise teleworker solution

Table 2-3 summarizes the Cisco Enterprise Architecture.

Table 2-3 Cisco Enterprise Architecture Model

Enterprise Area or Module	Description
Enterprise campus area	The enterprise campus module includes the building access and building distribution components and the shared campus backbone component or campus core. Edge distribution provides connectivity to the enterprise edge. High availability is implemented in the server farm, and network management monitors the enterprise campus and enterprise edge.
Enterprise edge area	Consists of e-commerce, Internet, VPN/remote access, and WAN modules.
Enterprise WAN module	This module provides MPLS or other WAN technologies.
Enterprise remote branch module	The enterprise branch normally consists of remote offices, small offices, or sales offices. These branch offices rely on the WAN to use the services and applications provided in the main campus.
Enterprise data center module	The enterprise data center consists of using the network to enhance the server, storage, and application servers. The offsite data center provides disaster recovery and business continuance services for the enterprise.
Enterprise teleworker	The enterprise teleworker module supports a small office, mobile users, or home users providing access to corporate systems via VPN tunnels.

High Availability Network Services

This section covers designs for high availability network services in the access layer.

Key Topic

When designing a network topology for a customer who has critical systems, services, or network paths, you should determine the likelihood that these components will fail and then design redundancy where necessary. Consider incorporating one of the following types of redundancy into your design:

- Workstation-to-router redundancy in the building access layer
- Server redundancy in the server farm module
- Route redundancy within and between network components
- Link media redundancy in the access layer

The following sections discuss each type of redundancy.

Workstation-to-Router Redundancy and LAN High Availability Protocols

When a workstation has traffic to send to a station that is not local, the workstation has many possible ways to discover the address of a router on its network segment, including the following:

- ARP
- Explicit configuration
- ICMP Router Discovery Protocol (RDP)
- RIP
- HSRP
- VRRP
- GLBP
- VSS

The following sections cover each of these methods. VSS is covered earlier in the chapter.

ARP

Some IP workstations send an ARP frame to find a remote station. A router running proxy ARP can respond with its data link layer address. Cisco routers run proxy ARP by default.

Explicit Configuration

Most IP workstations must be configured with the IP address of a default router, which is sometimes called the default gateway.

In an IP environment, the most common method for a workstation to find a server is via explicit configuration (a default router). If the workstation's default router becomes unavailable, you must reconfigure the workstation with the address of a different router. Some IP stacks enable you to configure multiple default routers, but many other IP implementations support only one default router.

RDP

RFC 1256 specifies an extension to the Internet Control Message Protocol (ICMP) that allows an IP workstation and router to run RDP to let the workstation learn a router's address.

RIP

An IP workstation can run RIP to learn about routers, although this is not a common practice anymore and is not recommended. You should use RIP in passive mode rather than active mode. (Active mode means that the station sends RIP frames every 30 seconds.) Usually in these implementations, the workstation is a UNIX system running the routed or gated UNIX process.

HSRP

The Cisco HSRP provides a way for IP workstations that support only one default router to keep communicating on the internetwork even if their default router becomes unavailable. HSRP works by creating a virtual router that has its own IP and MAC addresses. The workstations use this virtual IP address as their default router.

HSRP routers on a LAN communicate among themselves to designate two routers as active and standby. The active router sends periodic hello messages. The other HSRP routers listen for the hello messages. If the active router fails and the other HSRP routers stop receiving hello messages, the standby router takes over and becomes the active router. Because the new active router assumes both the phantom's IP and MAC addresses, end nodes see no change. They continue to send packets to the phantom router's MAC address, and the new active router delivers those packets.

HSRP also works for proxy ARP. When an active HSRP router receives an ARP request for a node that is not on the local LAN, the router replies with the phantom router's MAC address instead of its own. If the router that originally sent the ARP reply later loses its connection, the new active router can still deliver the traffic.

Figure 2-17 shows a sample implementation of HSRP.

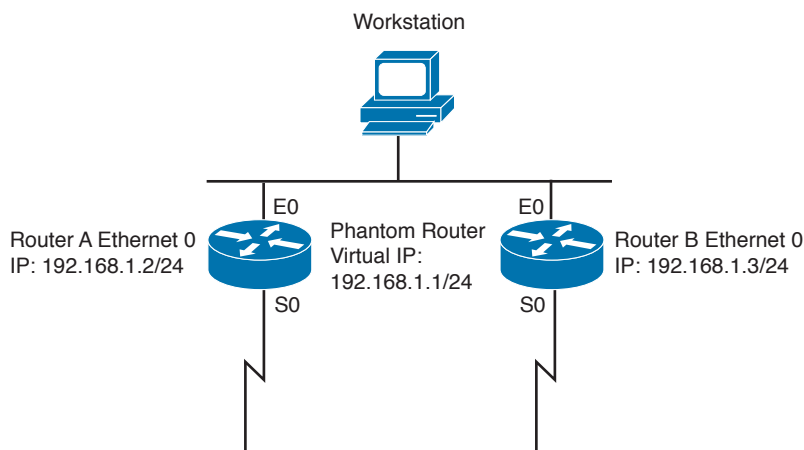


Figure 2-17 HSRP: The phantom router represents the real routers

In Figure 2-17, the following sequence occurs:

1. The workstation is configured to use the phantom router (192.168.1.1) as its default router.

2. Upon booting, the routers elect Router A as the HSRP active router. The active router does the work for the HSRP phantom. Router B is the HSRP standby router.
3. When the workstation sends an ARP frame to find its default router, Router A responds with the phantom router's MAC address.
4. If Router A goes offline, Router B takes over as the active router, continuing the delivery of the workstation's packets. The change is transparent to the workstation.

VRRP

VRRP is a router redundancy protocol defined in RFC 3768. RFC 5768 defined VRRPv3 for both IPv4 and IPv6 networks. VRRP is based on Cisco's HSRP, but is not compatible. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end hosts. The virtual router backup assumes the forwarding responsibility for the virtual router should the master fail.

GLBP

GLBP protects data traffic from a failed router or circuit, such as HSRP, while allowing packet load sharing between a group of redundant routers. Methods for load balancing with HSRP and VRRP work with small networks, but GLBP allows for first-hop load balancing on larger networks.

The difference in GLBP from HSRP is that it provides for load balancing between multiple redundant routers—up to four gateways in a GLBP group. It load-balances by using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. By default, all routers within a group forward traffic and load-balance automatically. GLBP members communicate between each other through hello messages sent every three seconds to the multicast address 224.0.0.102, User Datagram Protocol (UDP) port 3222. GLBP benefits include the following:

- **Load sharing:** GLBP can be configured in a way that traffic from LAN clients can be shared by multiple routers.
- **Multiple virtual routers:** GLBP supports up to 1024 virtual routers (GLBP groups) on each physical interface of a router.
- **Preemption:** GLBP enables you to preempt an active virtual gateway with a higher-priority backup.
- **Authentication:** Simple text password authentication is supported.

Server Redundancy

Some environments need fully redundant (mirrored) file and application servers. For example, in a brokerage firm where traders must access data to buy and sell stocks, two or more redundant servers can replicate the data. Also, you can deploy Cisco Unified Communications Manager (CUCM) servers in clusters for redundancy. The servers should

be on different networks and use redundant power supplies. To provide high availability in the server farm module, you have the following options:

- **Single attachment:** This is not recommended because it requires alternate mechanisms (HSRP, GLBP) to dynamically find an alternate router.
- **Dual attachment:** This solution increases availability by using redundant network interface cards (NIC).
- **Fast EtherChannel (FEC) and Gigabit EtherChannel (GEC) port bundles:** This solution bundles 2 or 4 Fast or Gigabit Ethernet links to increase bandwidth.

Route Redundancy

Designing redundant routes has two purposes: balancing loads and increasing availability.

Load Balancing

Most IP routing protocols can balance loads across parallel links that have equal cost. Use the maximum-paths command to change the number of links that the router will balance over for IP; the default is four, and the maximum is six. To support load balancing, keep the bandwidth consistent within a layer of the hierarchical model so that all paths have the same cost. (Cisco Enhanced Interior Gateway Routing Protocol [EIGRP] is an exception because it can load-balance traffic across multiple routes that have different metrics by using a feature called variance.)

A hop-based routing protocol does load balancing over unequal-bandwidth paths as long as the hop count is equal. After the slower link becomes saturated, packet loss at the saturated link prevents full utilization of the higher-capacity links; this scenario is called pinhole congestion. You can avoid pinhole congestion by designing and provisioning equal-bandwidth links within one layer of the hierarchy or by using a routing protocol that takes bandwidth into account.

IP load balancing in a Cisco router depends on which switching mode the router uses. Process switching load balances on a packet-by-packet basis. Fast, autonomous, silicon, optimum, distributed, and NetFlow switching load balances on a destination-by-destination basis because the processor caches information used to encapsulate the packets based on the destination for these types of switching modes.

Increasing Availability

In addition to facilitating load balancing, redundant routes increase network availability.

You should keep bandwidth consistent within a given design component to facilitate load balancing. Another reason to keep bandwidth consistent within a layer of a hierarchy is that routing protocols converge much faster on multiple equal-cost paths to a destination network.

By using redundant, meshed network designs, you can minimize the effect of link failures. Depending on the convergence time of the routing protocols, a single link failure cannot have a catastrophic effect.

You can design redundant network links to provide a full mesh or a well-connected partial mesh. In a full-mesh network, every router has a link to every other router, as shown in

Figure 2-18. A full-mesh network provides complete redundancy and also provides good performance because there is just a single-hop delay between any two sites. The number of links in a full mesh is $n(n-1)/2$, where n is the number of routers. Each router is connected to every other router. A well-connected partial-mesh network provides every router with links to at least two other routing devices in the network.

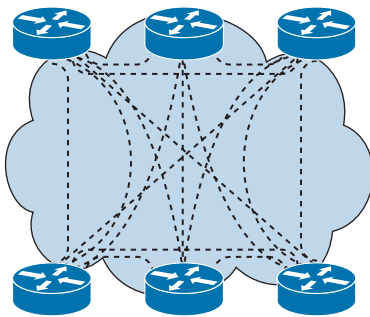


Figure 2-18 *Full-mesh network: Every router has a link to every other router in the network.*

A full-mesh network can be expensive to implement in WANs because of the required number of links. In addition, groups of routers that broadcast routing updates or service advertisements have practical limits to scaling. As the number of routing peers increases, the amount of bandwidth and CPU resources devoted to processing broadcasts increases.

A suggested guideline is to keep broadcast traffic at less than 20 percent of the bandwidth of each link; this amount limits the number of peer routers that can exchange routing tables or service advertisements. When designing for link bandwidth, reserve 80 percent of it for data, voice, and video traffic so that the rest can be used for routing and other link traffic. When planning redundancy, follow guidelines for simple, hierarchical design. Figure 2-19 illustrates a classic hierarchical and redundant enterprise design that uses a partial-mesh rather than a full-mesh topology. For LAN designs, links between the access and distribution layers can be Fast Ethernet, with links to the core at Gigabit Ethernet speeds.

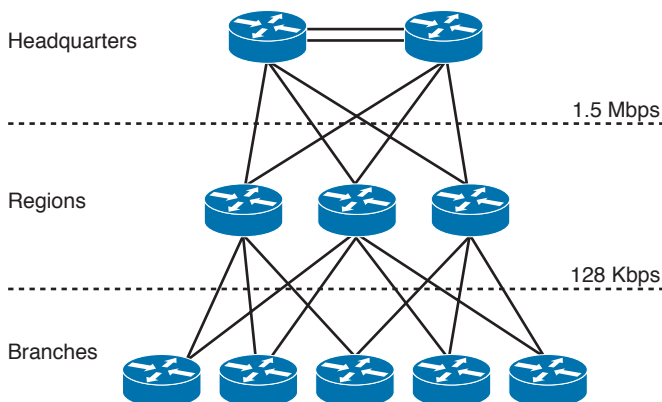


Figure 2-19 *Partial-mesh design with redundancy*

Link Media Redundancy

In mission-critical applications, it is often necessary to provide redundant media.

In switched networks, switches can have redundant links to each other. This redundancy is good because it minimizes downtime, but it can result in broadcasts continuously circling the network, which is called a broadcast storm. Because Cisco switches implement the IEEE 802.1d spanning-tree algorithm, you can avoid this looping in Spanning Tree Protocol (STP). The spanning-tree algorithm guarantees that only one path is active between two network stations. The algorithm permits redundant paths that are automatically activated when the active path experiences problems.

STP has a design limitation of only allowing one of the redundant paths to be active. VSS can be used with Catalyst 6500 switches to overcome this limitation.

You can use EtherChannel to bundle links for load balancing. Links are bundled in powers of 2 (2, 4, 8) groups. It aggregates the bandwidth of the links. Hence, two 10GE ports become 20 Gbps of bandwidth when they are bundled. For more granular load balancing, use a combination of source and destination per-port load balancing if available on the switch. In current networks, EtherChannel uses LACP, which is a standard-based negotiation protocol that is defined in IEEE 802.3ad (an older solution included the Cisco proprietary PAgP protocol). LACP helps protect against Layer 2 loops that are caused by misconfiguration. One downside is that it introduces overhead and delay when setting up the bundle.

Because WAN links are often critical pieces of the internetwork, WAN environments often deploy redundant media. As shown in Figure 2-20, you can provision backup links so that they become active when a primary link goes down or becomes congested.

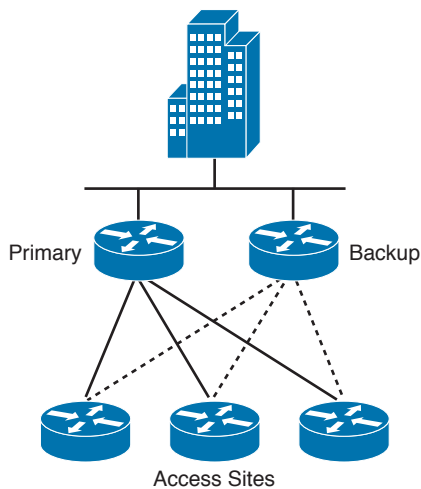


Figure 2-20 Backup links can provide redundancy.

Often, backup links use a different technology. For example, it is common to use Internet VPNs to back up primary MPLS links in today's networks. By using floating static routes, you can specify that the backup route must have a higher administrative distance (used by Cisco routers to select routing information) so that it is not normally used unless the primary route goes down.

Note When provisioning backup links, learn as much as possible about the physical circuit routing. Different carriers sometimes use the same facilities, meaning that your backup path might be susceptible to the same failures as your primary path. Do some investigative work to ensure that your backup really is acting as a backup.

Cisco supports Multilink Point-to-Point Protocol (MPPP), which is an Internet Engineering Task Force (IETF) standard for ISDN B-channel (or asynchronous serial interface) aggregation. It bonds multiple WAN links into a single logical channel. MPPP is defined in RFC 1990. MPPP does not specify how a router should accomplish the decision-making process to bring up extra channels. Instead, it seeks to ensure that packets arrive in sequence at the receiving router. Then, the data is encapsulated within PPP and the datagram is given a sequence number. At the receiving router, PPP uses this sequence number to re-create the original data stream. Multiple channels appear as one logical link to upper-layer protocols. For Frame Relay networks, FRF.16.1 Multilink Frame Relay is used to perform a similar function.

Table 2-4 summarizes the four main redundancy models.

Table 2-4 Redundancy Models

Redundancy Type	Description
Workstation-to-router redundancy	Use of HSRP, VRRP, GLBP, and VSS
Server redundancy	Uses dual-attached NICs, FEC, or GEC port bundles
Route redundancy	Provides load balancing and high availability
Link redundancy	Uses multiple WAN links that provide primary and secondary failover for higher availability. On LANs, use EtherChannel.

References and Recommended Reading

Cisco Enterprise Teleworker Solution, <http://www.cisco.com/c/en/us/solutions/enterprise-networks/teleworker/index.html>.

Enterprise Architectures, <http://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html>.

Cisco Enterprise Solutions Portal, <http://www.cisco.com/c/en/us/solutions/enterprise/index.html>.

Cisco TrustSec, <http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html>.

Medianet at a Glance, www.cisco.com/web/solutions/medianet/docs/C45-511997-00medianet_aag120308.pdf.

Application Performance white paper, www.cisco.com/en/US/solutions/ns1015/lippis_white_paper_application_velocity.pdf.

RFC 3758: Virtual Router Redundancy Protocol (VRRP).

RFC 1990: The PPP Multilink Protocol (MP).

Virtual Switching System, www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topics icon in the outer margin of the page. Table 2-5 lists a reference of these key topics and the page numbers on which each is found.



Table 2-5 Key Topic

Key Topic Element	Description	Page
Summary	Hierarchical Network models	41
List	Hierarchical Network Design	42
Figure 2-7	Cisco Enterprise Architecture model	50
Summary	High availability network services	59

Complete Tables and Lists from Memory

Print a copy of Appendix D, “Memory Tables” (found on the book website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, “Memory Tables Answer Key,” also on the website, includes completed tables and lists to check your work.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

core layer, distribution layer, access layer, VLAN, PoE, ARP, VSS, enterprise campus module, enterprise edge, enterprise WAN module, enterprise remote branch module, enterprise data center module, enterprise teleworker module, HSRP, VRRP, GLBP

Q&A

The answers to these questions appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Questions.” For more practice with exam format questions, use the exam engine from the website.

1. True or false: The core layer of the hierarchical model does security filtering and media translation.
2. True or false: The access layer provides high availability and port security.
3. You add Communications Manager to the network as part of a Voice over IP (VoIP) solution. In which submodule of the Enterprise Architecture model should you place Communications Manager?
4. True or false: HSRP provides router redundancy.

5. Which enterprise edge submodule connects to an ISP?
6. List the six modules of the Cisco Enterprise Architecture model for network design.
7. True or false: In the Cisco Enterprise Architecture model, the network management submodule does not manage the SP edge.
8. True or false: You can implement a full-mesh network to increase redundancy and reduce a WAN's costs.
9. How many links are required for a full mesh of six sites?
10. List and describe four options for multihoming to the SP between the enterprise edge and the SP edge. Which option provides the most redundancy?
11. To what enterprise edge submodule does the SP edge Internet submodule connect?
12. What are four benefits of hierarchical network design?
13. In an IP telephony network, in which submodule or layer are the IP phones and CUCM servers located?
14. Match the redundant model with its description:
 - i. Workstation-router redundancy
 - ii. Server redundancy
 - iii. Route redundancy
 - iv. Media redundancy
 - a. Cheap when implemented in the LAN and critical for the WAN.
 - b. Provides load balancing.
 - c. Host has multiple gateways.
 - d. Data is replicated.
15. True or false: Small-to-medium campus networks must always implement three layers of hierarchical design.
16. How many full-mesh links do you need for a network with ten routers?
17. Which layer provides routing between VLANs and security filtering?
 - a. Access layer
 - b. Distribution layer
 - c. Enterprise edge
 - d. WAN module
18. List the four modules of the enterprise edge area.
19. List the three submodules of the SP edge.
20. List the components of the Internet edge.

- 21.** Which submodule contains firewalls, VPN concentrators, and ASAs?
- a.** WAN
 - b.** VPN/remote access
 - c.** Internet
 - d.** Server farm
- 22.** Which of the following describe the access layer? (Select two.)
- a.** High-speed data transport
 - b.** Applies network policies
 - c.** Performs network aggregation
 - d.** Concentrates user access
 - e.** Provides PoE
 - f.** Avoids data manipulation
- 23.** Which of the following describe the distribution layer? (Select two.)
- a.** High-speed data transport
 - b.** Applies network policies
 - c.** Performs network aggregation
 - d.** Concentrates user access
 - e.** Provides PoE
 - f.** Avoids data manipulation
- 24.** Which of the following describe the core layer? (Select two.)
- a.** High-speed data transport
 - b.** Applies network policies
 - c.** Performs network aggregation
 - d.** Concentrates user access
 - e.** Provides PoE
 - f.** Avoids data manipulation
- 25.** Which campus submodule connects to the enterprise edge module?
- a.** SP edge
 - b.** WAN submodule
 - c.** Building distribution
 - d.** Campus core
 - e.** Enterprise branch
 - f.** Enterprise data center
- 26.** Which remote module connects to the enterprise via the Internet or WAN submodules and contains a small LAN switch for users?
- a.** SP edge

- b.** WAN submodule
 - c.** Building distribution
 - d.** Campus core
 - e.** Enterprise branch
 - f.** Enterprise data center
- 27.** Which three types of servers are placed in the e-commerce submodule?
- a.** Web
 - b.** Application
 - c.** Database
 - d.** Intranet
 - e.** Internet
 - f.** Public share

Use Figure 2-21 to answer questions 28–33.

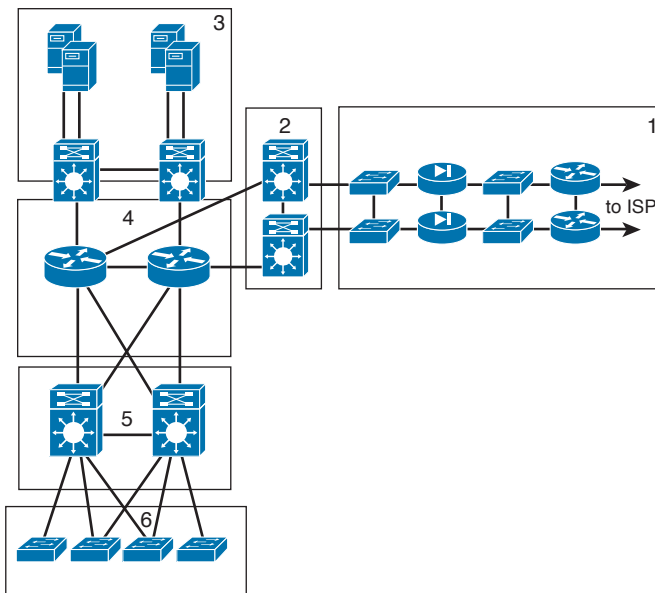


Figure 2-21 Scenario for questions 28–33

- 28.** Which is the campus core layer?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6

- 29.** Which is the enterprise edge?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6
- 30.** Which is the campus access layer?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6
- 31.** Which is the enterprise edge distribution?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6
- 32.** Which is the campus distribution layer?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6
- 33.** Which is the campus data center?
- a.** Block 1
 - b.** Block 2
 - c.** Block 3
 - d.** Block 4
 - e.** Block 5
 - f.** Block 6

- 34.** Which solution supports the enterprise teleworker?
- a.** IP telephony
 - b.** Enterprise campus
 - c.** Cisco Virtual Office
 - d.** SP edge
 - e.** Hierarchical design
 - f.** Data Center 3.0
- 35.** Which are two benefits of using a modular approach?
- a.** Simplifies the network design
 - b.** Reduces the amount of network traffic on the network
 - c.** Often reduces the cost and complexity of the network
 - d.** Makes the network simple by using full mesh topologies
- 36.** Which three modules provide infrastructure for remote users? (Select three.)
- a.** Teleworker module
 - b.** WAN module
 - c.** Enterprise branch module
 - d.** Campus module
 - e.** Enterprise data center
 - f.** Core, distribution, access layers
- 37.** Which are borderless networks infrastructure services? (Select three.)
- a.** IP telephony
 - b.** Security
 - c.** QoS
 - d.** SP edge
 - e.** High availability
 - f.** Routing
- 38.** Which module contains devices that supports AAA and stores passwords?
- a.** WAN module
 - b.** VPN module
 - c.** Server farm module
 - d.** Internet connectivity module
 - e.** SP edge
 - f.** TACACS

- 39.** Which topology is best used for connectivity in the building distribution layer?
- a.** Full mesh
 - b.** Partial mesh
 - c.** Hub and spoke
 - d.** Dual ring
 - e.** EtherChannel
- 40.** What are two ways that wireless access points are used? (Choose two.)
- a.** Function as a hub for wireless end devices
 - b.** Connect to the enterprise network
 - c.** Function as a Layer 3 switch for wireless end devices
 - d.** Provide physical connectivity for wireless end devices
 - e.** Filter out interference from microwave devices
- 41.** In which ways does application network services help resolve application issues? (Choose two.)
- a.** It can compress, cache, and optimize content.
 - b.** Optimizes web streams, which can reduce latency and offload the web server.
 - c.** Having multiple data centers increases productivity.
 - d.** Improves application response times by using faster servers.
- 42.** Which are key features of the distribution layer? (Select three.)
- a.** Aggregates access layer switches
 - b.** Provides a routing boundary between access and core layers
 - c.** Provides connectivity to end devices
 - d.** Provides fast switching
 - e.** Provides transport to the enterprise edge
 - f.** Provides VPN termination
- 43.** Which Cisco solution allows a pair of switches to act as a single logical switch?
- a.** HSRP
 - b.** VSS
 - c.** STP
 - d.** GLB
- 44.** Which module or layer connects the server layer to the enterprise edge?
- a.** Campus distribution layer
 - b.** Campus data center access layer
 - c.** Campus core layer

- d.** Campus MAN module
 - e.** WAN module
 - f.** Internet connectivity module
- 45.** Which server type is used in the Internet connectivity module?
 - a.** Corporate
 - b.** Private
 - c.** Public
 - d.** Internal
 - e.** Database
 - f.** Application
- 46.** Which server types are used in the e-commerce module for users running applications and storing data? (Select three.)
 - a.** Corporate
 - b.** Private
 - c.** Public
 - d.** Internet
 - e.** Database
 - f.** Application
 - g.** Web
- 47.** Which are submodules of the enterprise campus module? (Select two.)
 - a.** WAN
 - b.** LAN
 - c.** Server farm/data center
 - d.** Enterprise branch
 - e.** VPN
 - f.** Building distribution
- 48.** Which are the three layers of the hierarchical model? (Select three.)
 - a.** WAN layer
 - b.** LAN layer
 - c.** Core layer
 - d.** Aggregation layer
 - e.** Access layer
 - f.** Distribution layer
 - g.** Edge layer

- 49.** You need to design for a packet load-sharing between a group of redundant routers. Which protocol allows you to do this?
- a.** HSRP
 - b.** GLBP
 - c.** VRRP
 - d.** AARP
- 50.** Which is a benefit of using network modules for network design?
- a.** Network availability increases.
 - b.** Network becomes more secure.
 - c.** Network becomes more scalable.
 - d.** Network redundancy is higher.
- 51.** The Cisco Enterprise Architecture takes which approach to network design?
- a.** It takes a functional modular approach.
 - b.** It takes a sectional modular approach.
 - c.** It takes a hierarchical modular approach.
 - d.** It takes a regional modular approach.
- 52.** Which is the recommended design geometry for routed networks?
- a.** Design linear point-to-point networks
 - b.** Design in rectangular networks
 - c.** Design in triangular networks
 - d.** Design in circular networks
- 53.** Which layer performs rate limiting, network access control, and broadcast suppression?
- a.** Core layer
 - b.** Distribution layer
 - c.** Access layer
 - d.** Data link layer
- 54.** Which layer performs routing between VLANs, filtering, and load balancing?
- a.** Core layer
 - b.** Distribution layer
 - c.** Access layer
 - d.** Application layer

- 55.** Which topology allows for maximum growth?
- a.** Triangles
 - b.** Collapsed core-distribution
 - c.** Full mesh
 - d.** Core-distribution-access
- 56.** Which layer performs port security and DHCP snooping?
- a.** Core layer
 - b.** Distribution layer
 - c.** Access layer
 - d.** Application layer
- 57.** Which layer performs Active Directory and messaging?
- a.** Core layer
 - b.** Distribution layer
 - c.** Access layer
 - d.** Application layer
- 58.** Which layers perform redundancy? (Select two.)
- a.** Core layer
 - b.** Distribution layer
 - c.** Access layer
 - d.** Data Link Layer
- 59.** Which statement is true regarding hierarchical network design?
- a.** Makes the network harder since there are many submodules to use
 - b.** Provides better performance and network scalability
 - c.** Prepares the network for IPv6 migration from IPv4
 - d.** Secures the network with access filters in all layers

- 60.** Based on Figure 2-22, and assuming that devices may be in more than one layer, list which devices are in each layer.

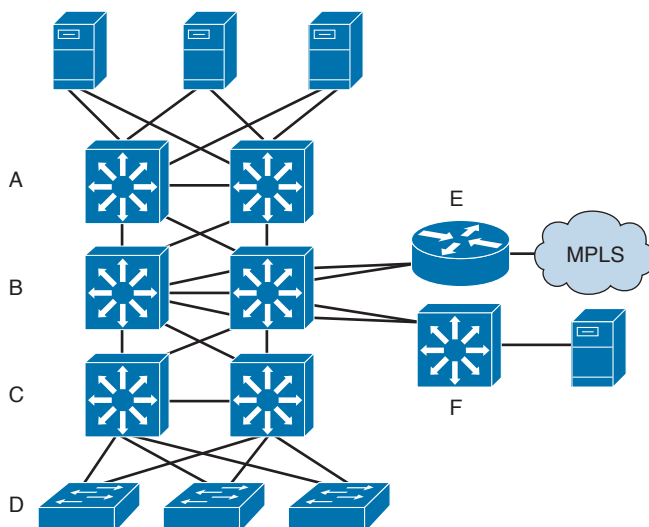


Figure 2-22 Question 60

Access layer:

Distribution layer:

Core:

Use Figure 2-23 to answer questions 61–63.

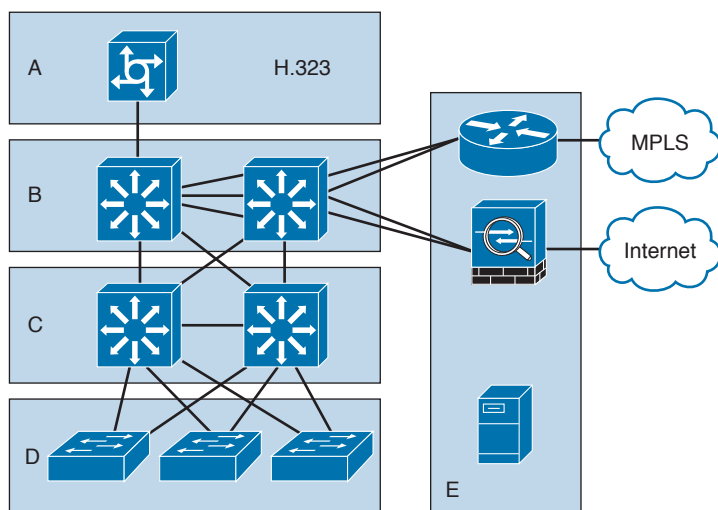


Figure 2-23 Scenario for questions 61–63

- 61.** Which section(s) belong(s) to the core layer?
- 62.** Which section(s) belong(s) to the distribution layer?
- 63.** Which section(s) belong(s) to the access layer?



Index

Numbers

4-way handshakes, WLAN, 172
4G LTE (Long Term Evolution), 224
10 Gigabit Ethernet, LAN design, 87
40 Gigabit Ethernet, LAN design, 87-88
100 Gigabit Ethernet, LAN design, 87-88
100BASE-FX Fast Ethernet, LAN design, 85
100BASE-T4 Fast Ethernet, LAN design, 84
100BASE-TX Fast Ethernet, LAN design, 84
802.1X, 527
1000BASE-CX Gigabit Ethernet over Coaxial Cable, LAN design, 86
1000BASE-LX long-wavelength Gigabit Ethernet, LAN design, 86
1000BASE-SX short-wavelength Gigabit Ethernet, LAN design, 86
1000BASE-T Gigabit Ethernet over UTP, LAN design, 86

A

AAA (Authentication, Authorization, Accounting), 542
ABR (Area Border Routers)
 OSPFv2, 434-436
 OSPFv3, 440
access
 controlling access, network virtualization, 156-157
 unauthorized access (security threats), 490-494

access layer
 campus LAN, 94-97, 101
 DC, 147-148
 hierarchical network models, 44-46
access services, video networks, 579
accounting (security), 506
accounting management (networks), 619
ACD (Automatic Call Distribution), PSTN, 569
ACI (Application Centric Infrastructure), 135
Acknowledgment packets, EIGRP, 403
ACL (Access Control Lists), 495, 530
AD (Administrative Distance), BGP, 449
administrative distance, routing protocols, 386-387
ADSL (Asymmetric Digital Subscriber Lines), 222
adware, 490
AES (Advanced Encryption Standard), WLAN, 172
AFI field (RIPv2 message format), 395
aggregation layer (DC), 147-149
AIM (Advanced Integration Module), 543
AirMagnet Analyzer Pro, network audits, 20
ALG (Application Layer Gateways), 359
AMP (Advanced Malware Protection), 538
analog signaling, voice networks, 562-567
analog-to-digital signal conversion (codecs), 580
antivirus software, 529
Anycast-based load balancing, 160
anycast IPv6 addresses, 344-346

AP (Access Points)

- autonomous AP, Cisco UWN, 176
- Bridge mode, 181
- CAPWAP, 178-182
- Controller Equipment scaling and WLC, 185-186
- H-REAP mode, 180
- LAP discovery of WLC via CAPWAP, 181-182
- Local mode, 180
- LWAPP, 177-178
- MAP, 196
- Monitor mode, 181
- RAP, 196
- Rogue Detector mode, 181
- self-healing, 193
- Sniffer mode, 181
- WLAN, campus design, 196

AP Manager interface (WLC), 185**API (Application Programming Interfaces), 135, 359****APIC (Application Centric Infrastructure Controller), 135****Application layer (SDN), 134****application level getaways, 528****applications**

- filtering, 529
- growth of applications and network design, 6
- load balancing, DC, 159
- security, 533

architectures (networks)

- benefits of, 9
- borderless network architectures, 7
- collaboration and video architectures, 8
- data center and virtualization architectures, 8-9

areas

- defining, 432
- OSPFv2 areas, 432-433
- OSPFv3 areas, 440

ARP (Address Resolution Protocol), 60

- DAI, 495
- IPv4 addressing, 321-322

ASA (Access Control Servers), 540, 548**ASA (Adaptive Security Appliances), 525, 543****ASA Services Modules, 544****ASBR (Autonomous System Boundary Routers)**

- OSPFv2, 434-436
- OSPFv3, 440

Assessment process (Plan phase), 10**ATM (Asynchronous Transfer Mode), VoATM, 572****atomic aggregate attribute, BGP, 452****audits (networks), 19**

- AirMagnet Analyzer Pro, 20
- CDP, 20
- Cisco Prime Infrastructure and Solarwinds, 20
- Ekahau Site Survey, 20
- LanGuard network security scanner, 20
- LLDP, 20
- manual assessments, 20-22
- NBAR, 20
- NetFlow, 20-23
- show commands, 20-22
- SNMP, 20
- Syslog, 20
- Wireshark, 20

authentication, 506

- EAP-FAST, 183
- EAP-TLS, 183
- EAP-TTLS, 183
- IS-IS, 411
- LEAP, 183
- PEAP, 183
- RIPng, 397
- RIPv2, 394
- router authentication, OSPFv2, 439
- user authentication, 532
- WLAN, 173, 182-183

- authNoPriv security (SNMPv3), 623
- authorization (security), 506
- authPriv security (SNMPv3), 623
- Auto QoS (Quality of Service), 599
- Auto-RP, 469
- autonomous system path attribute, BGP, 451
- availability
 - route redundancy, 63-64
 - security risks, 494-495
- AVC (Application Visibility and Control), 538

B

- backbone routers
 - OSPFv2, 434
 - OSPFv3, 440
- BackboneFast, 104-105
- backups
 - enterprise branch architectures, 271
 - WAN, 263-264
- bandwidth. *See also* QoS; throughput
 - routing protocols, 389, 401-402, 409
 - video networks, 595-599
 - VoIP, 595-599
 - WAN
 - backups*, 263
 - enterprise edge design*, 231-236
- BGP (Border Gateway Protocol), 382-383, 388, 443, 462
 - AD, 449
 - atomic aggregate attribute, 452
 - autonomous system path attribute, 451
 - characteristics of, 454-455
 - community attribute, 452
 - confederations, 448
 - decision process, 453-454
 - eBGP, 445
 - iBGP, 445-446
 - local preference attributes, 450
 - MED attribute, 451
 - MP-BGP, 446
 - neighbor discovery, 444-445
 - next-hop attributes, 450
 - origin attributes, 450
 - path attributes, 449
 - QPPB, 446
 - route filtering, 461
 - route reflectors, 446-447
 - weight, 453
- BGP4+, 353
- BHT (Busy Hour Traffic), voice networks, 570
- Big Oil and Gas comprehensive scenario, 642-643, 650-651
- blade servers, enterprise DC, 136
- blocking probability (voice networks), 571
- blocking state (STP switch ports), 102
- BOM (Bills of Materials) and LLD documents, 16
- BOOTP (Bootstrap Protocol), IPv4 address assignments, 317
- borderless network architectures, 7
- borders (removal of), network design, 6
- bottom-up network design versus top-down design, 25
- BPDU Filter, 104-105
- BPDU Guard, 97, 104-105
- Bridge mode (AP), 181
- bridges
 - flooding, 90
 - LAN, 89
 - root bridges, 90, 102
 - STP, 90
 - wireless bridges, 223
- bridging services, video networks, 579
- broadcast IPv4 addresses, 299
- BSR (Bootstrap Routers), 470
- Build phase (network design), 9-12
- business forces and network design, 6
- busy hour (voice networks), 570

C

cable

- CMTS, 222
- coaxial cable, 1000BASE-CX Gigabit Ethernet over Coaxial Cable, 86
- dark fiber, 227
- DC cabling, 141-143
- DOCSIS protocol, 223
- modems, 223
- WAN strategies, 222

call processing, converged multiservice networks, 571

campus LAN

- access layer best practices, 94-97, 101
- application types, 93
- core layer best practices, 99-101
- distribution layer best practices, 97-101
- network requirements, 93
- STP, 101-103
- STP Toolkit, 103-105
- transmission media comparisons, 88
- VLAN trunking, 105

campus networks, security, 545

CAPWAP (Control and Provisioning for Wireless Access Point), 178-182

CAR (Committed Access Rate), 233

CAS (Channel Associated Signaling) circuits, 562, 565

case studies

- Big Oil and Gas, 642-643, 650-651
- Diamond Communications, 645-646, 652-653
- Friendswood Hospital, 641-642, 646-650
- Video Games Spot, 643-645, 651-652

Catalyst 6500 security service modules, 544

CBWFQ (Class-Based Weighted Fair Queuing), 234

CCS (Centum Call Seconds), video networks, 570

CCS (Common Channel Signaling) circuits, 562-566

CDP (Cisco Discovery Protocol), 20, 629-631

CDR (Call Detail Records), voice networks, 571

cell-switched WAN, 252

centralized Internet, WAN and enterprise edge connectivity, 240

Centrex services (PSTN), 569

certificates (security), 506

CGMP (Cisco Group Management Protocol), 113, 466-467

channelized T1/E1 circuits, 562, 565

characterizing networks, 24

- information gathering process, 19
- network audits, 19-23
- performance checklists, 23

CIR (Committed Information Rates), 228

circuit-switched WAN, 252

Cisco APIC (Application Centric Infrastructure Controller), 135

Cisco Catalyst switches, 526

Cisco Enterprise Architecture Model, 49

- Enterprise Campus module, 50, 59
- Enterprise Edge module, 52, 59
- E-Commerce module, 52*
- Enterprise WAN, 55-56, 59*
- Internet Connectivity module, 53-54*
- SP edge module, 56*
- VPN/Remote Access module, 54-55*

remote modules

- Enterprise Branch module, 57-59*
- Enterprise Data Center module, 58-59*
- Enterprise Teleworker module, 58-59*

SP edge module, 56

Cisco ESA (Email Security Appliances), 538

Cisco ISE (Identity Services Engines), 527, 544

Cisco Learning Network, 657

- Cisco Prime Infrastructure and Solarwinds, network audits, 20
- Cisco SAFE (Security Architecture for the Enterprise)
 - ASA, 525
 - benefits of, 525
 - Cisco Catalyst switches, 526
 - Cisco SCF, 526
 - Compliance, 524
 - ISR G2, 525
 - Management, 525
 - Secure Services, 524
 - Security Intelligence, 525
 - Segmentation, 525
 - Threat Defense, 524
- Cisco SCF (Security Control Framework), 526
- Cisco TDS (Threat Defense System)
 - infrastructure protection, 512
 - physical security, 510-511
- Cisco unified networks, 571
- Cisco UWN (Unified Wireless Networks)
 - architecture of, 175-176
 - autonomous AP, 176
 - benefits of, 175
 - CAPWAP, 178-182
 - centralized WLAN architecture, 177
 - local MAC, 179, 200
 - LWAPP, 177-178
 - split-MAC architectures, 179
 - WLAN
 - authentication*, 182-183
 - intracontroller roaming*, 187
 - Layer 2 intercontroller roaming*, 187
 - Layer 3 intercontroller roaming*, 188
 - mobility groups*, 189-190
 - WLC*, 183-186
- Cisco Virtual Office Solution, enterprise teleworker design, 279-280
- Cisco WSA (Web Security Appliances), 538-539
- Class A IPv4 addresses, 297
- Class B IPv4 addresses, 298
- Class C IPv4 addresses, 298
- Class D IPv4 addresses, 298
- Class E IPv4 addresses, 298
- classful routing protocols versus classless protocols, 385
- classification (QoS), 233
- classless routing protocols versus classful routing protocols, 385
- cloud services DMZ, 237
- CME (CallManager Express), unified CME deployments, 578
- CMTS (Cable Modem Termination System), 222
- CO-to-PBX trunks, 561
- coaxial cable, 1000BASE-CX Gigabit Ethernet over Coaxial Cable, 86
- codecs
 - analog-to-digital signal conversion, 580
 - converged multiservice networks, 580-581
 - MOS, 581
 - standards, 580-581
- collaboration and video architectures, 8
- collaboration services, 8
- collapsed core design
 - enterprise branch architectures, 275
 - hierarchical network design, 49
- Command field
 - RIPng message format, 397
 - RIPv2 message format, 395
- communication and collaboration applications (collaboration and video architectures), 8
- community attribute, BGP, 452
- competition, network design, 6
- Compliance (Cisco SAFE), 524
- composite metric, routing protocols, 403, 409
- comprehensive scenarios
 - Big Oil and Gas, 642-643, 650-651

- Diamond Communications, 645-646, 652-653
 - Friendswood Hospital, 641-642, 646-650
 - Video Games Spot, 643-645, 651-652
 - confederations (BGP), 448
 - confidentiality (data), security risks, 494-497
 - configuration management (networks), 619
 - configuration/software archive hosts and security management, 540
 - congestion management (QoS), 234
 - connected mode (H-REAP), 200
 - connection management, borderless network architectures, 7
 - content security defense, 533
 - continuous security, 501-502
 - Control layer (SDN), 134
 - controllers (SDN), 134-135
 - converged multiservice networks
 - call packetized voice systems, 571
 - call processing, 571
 - codecs, 580-581
 - design recommendations, 600
 - dial plans, 571
 - IPT
 - components of, 574*
 - CUCM, 574-577*
 - design goals, 575*
 - functional areas, 574*
 - multisite WAN with centralized call processing deployments, 576*
 - multisite WAN with distributed call processing deployments, 577*
 - PoE, 575*
 - single-site deployments, 576*
 - unified CME deployments, 578*
 - service class recommendations, 600-602
 - video deployment considerations, 578-579
 - VoATM, 572
 - VoFR, 572
 - VoIP, 572-573
 - bandwidth, 590-592, 595-599*
 - control protocols, 581-589*
 - delays, 592-593*
 - design goals, 575*
 - echo cancellation, 595*
 - packet loss, 594*
 - QoS, 595-599*
 - transport protocols, 581-589*
 - VAD, 590-591*
 - cooling, DC cooling requirements/solutions, 140-141
 - core layer
 - campus LAN, 99-101
 - DC, 149-150
 - hierarchical network models, 42-45
 - counting to infinity, routing loops, 393
 - country codes (numbering plans), PSTN switches, 567-568
 - CQ (Custom Queuing), 234
 - cRTP (Compressed Real-time Transport Protocol), 583, 596, 599
 - CSM (Cisco Security Manager), 540
 - CUCM (Cisco Unified Communications Manager), 574
 - multisite WAN
 - with centralized call processing, 576*
 - with distributed call processing, 577*
 - single-site deployments, 576
 - customer requirements and network design, 17-18
- ## D
-
- DAI (Dynamic ARP Inspection), 495
 - dark fiber, 227
 - data center
 - security, 546-547
 - virtualization architectures, 8-9
 - data confidentiality (security risks), 494
 - data integrity (security), 494-497, 509-510
 - data leaks (security threats), 490-491
 - data modification/disclosure attacks (security threats), 490-491

data packets

- Acknowledgment packets, EIGRP, 403
- Hello packets, EIGRP, 403
- packet loss, VoIP, 594
- Query packets, EIGRP, 403
- Reply packets, EIGRP, 403
- Update packets, EIGRP, 403

database services (PSTN), 569**DC (Data Centers)**

- access layer, 147-148
- aggregation layer, 147-149
- cabling, 141-143
- challenges of, 136
- cooling requirements/solutions, 140-141
- core layer, 149-150

DCI

- L2 considerations, 159*
- transport options, 158*
- use cases, 157-158*

enterprise DC, 111

- architecture of, 130-131*
- foundation layer, 130*
- network programmability, 133-135*
- SDN, 134*
- SDN controllers, 134*
- services layer, 130*
- topology of, 133*
- UCS, 132*
- unified fabric, 132*
- user services layer, 131*
- virtualization, 132*

facility consideration, 136-138**FEX, 151****load balancing**

- application load balancing, 159*
- network load balancing, 160*

physical space constraints, 138-139**power requirements, 139-140****reference architecture, 146-147****security, 150****servers, 136****storage, 144-146****virtualization, 151**

- access control, 156-157*
- device contexts, 155*
- device virtualization, 153*
- network virtualization, 152*
- path isolation, 156-157*
- risks of, 152*
- servers, 155*
- services edge, 157*
- virtual switches, 156*
- vPC, 154*
- VRF, 154*
- VSS, 153*

DCI (Data Center Interconnect)

- L2 considerations, 159
- transport options, 158
- use cases, 157-158

DDoS (Distributed DoS) attacks, 495**decryption, 529****dedicated L4-7 load balancers, 160****delay metric, routing protocols, 391, 402****delays**

- jitter, 594
- processing delay, 593-594
- propagation delay, 593-594
- queuing delay, 593-594
- serialization delay, 593-594
- VoIP, 592-593

deliverables (projects)

- HLD documents, 16
- LLD documents, 16
- NIP documents, 16
- NRFU documents, 16

deploying IPv6, 357

- dual-stack model, 360, 363
- hybrid model, 361-363
- service block model, 362-363

Deployment process (Build phase), 11**design documents, 25-26**

Design phase (network design), PPDIOO, 14-15

Design process (Plan phase), 10

Design Strategy (STP Toolkit), 97

designing IP addressing schemes

IPv4 addresses

goal of, 310

NAT guidelines, 313

planning for future growth, 310

planning for hierarchical IP address networks, 311-312

private/public IP addresses, 313

route summarization, 311

standards for addressing, 313-314

subnet allocation case study, 314-316

IPv6 addresses

/64 subnets, 354-355

address allocations, 355-356

address blocks, 354-355

planning, 354

private addresses, 355

route summarization, 354

designing networks

borderless network architectures, 7

Build phase, 9-12

business forces effects on, 6

campus LAN

access layer best practices, 94-97, 101

application types, 93

core layer best practices, 99-101

distribution layer best practices, 97-101

enterprise campus LAN, 107-109

enterprise DC, 111

large-building LAN, 106

medium-size LAN, 109

multicast traffic, 113-114

network requirements, 93

QoS, 111-112

remote site LAN, 110

server farm modules, 110

small LAN, 110

STP, 101-103

STP Toolkit, 103-105

VLAN trunking, 105

characterizing networks, 19-24

collaboration and video architectures, 8

competition, 6

customer requirements, 17-18

data center and virtualization architectures, 8-9

design documents, 25-26

Design phase (PPDIOO), 14-15

EIGRP, 404-407

enterprise DC

access layer, 147-148

aggregation layer, 147-149

architecture of, 130-131

cabling, 141-143

challenges of, 136

cooling requirements, 140

cooling solutions, 141

core layer, 149-150

DCI, 157-159

facility considerations, 136-138

FEX, 151

foundation layer, 130

load balancing, 159-160

network programmability, 133-135

physical space constraints, 138-139

power requirements, 139-140

reference architecture, 146-147

SDN, 134

SDN controllers, 134

security, 150

servers, 136

services layer, 130

storage, 144-146

topology of, 133

UCS, 132

unified fabric, 132

user services layer, 131

virtualization, 132, 151-157

- growth of applications, 6
- Implement phase (PPDIOO), 15
- IPv6, 407
- IS-IS, 409-411
- IT optimization, 6
- Manage phase, 10-12
- methodology of, 16
- Operate phase (PPDIOO), 15
- Optimize phase (PPDIOO), 15
- pilot sites, 25
- Plan phase, 9
- Plan phase (PBM), 10-12
- Plan phase (PPDIOO), 14-15
- PPDIOO, 12-15
- Prepare phase (PPDIOO), 14-15
- project deliverables, 16
- prototype networks, 25
- regulation, 6
- removal of borders, 6
- return on investment, 6
- RIPng, 398
- RIPv2, 396
- security integration with network design, 502
- technological forces effects on, 6
- top-down design approach, 24-25
- virtualization, 6
- VPN, 240-241
- WAN
 - design requirements*, 218
 - DMZ connectivity*, 236-238
 - enterprise edge design methodologies*, 229-236
 - Internet connectivity*, 238-240
 - VPN*, 240-241
- Destination Address field**
 - IPv4 headers, 291
 - IPv6 headers, 338
- device virtualization, 153-155**
- DHCP (Dynamic Host Configuration Protocol)**
 - DHCPv6, 352
 - DHCPv6 Lite, 352
 - IPv4
 - address assignments*, 317-319
 - name resolution*, 321
 - snooping, 495
 - VoIP, 582, 589
- dial plans, converged multiservice networks, 571**
- Diamond Communications comprehensive scenario, 645-646, 652-653**
- digital signaling**
 - DTMF, 567
 - voice networks, 562-567
- digital signatures (security), 510**
- direct Internet, WAN and enterprise edge connectivity, 240**
- Directive 95/46/EC security legislation, 489**
- disabled state (STP switch ports), 102**
- disclosure/data modification attacks (security threats), 490-491**
- discovery, network audits, 20**
- disruption of service (security threats), 490-491**
- distance-vector routing protocols, 383-384**
- distribution layer**
 - campus LAN, 97-101
 - hierarchical network models, 43-45
- DLCI (Data Link Connection Identifiers), 225**
- DMVPN (Dynamic Multipoint VPN), 257-258**
- DMZ (Demilitarized Zones), 220**
 - cloud services DMZ, 237
 - Internet DMZ, 236
 - per-service DMZ, 238
 - remote access VPN DMZ, 236
 - security services DMZ, 237
 - segmenting, 237
 - shared DMZ, 238

- site-to-site VPN DMZ, 236
- unified communications DMZ, 237
- WAN and enterprise edge connectivity, 236-238
- DNS (Domain Name Systems)**
 - DHCP and DNS servers, 321
 - IPv4 name resolution, 319-321
 - load balancing, 160
 - RR, 320
- DOCSIS (Data Over Cable Service Interface Specifications) protocol, 223**
- documents**
 - design documents, 25-26
 - project deliverables, 16
- DoS (Denial of Service) attacks, 490, 495**
- DR (Disaster Recovery), 157**
 - IS-IS, 410
 - OSPFv2, 435
- DS (Differentiated Services) field (IPv4 headers), 293**
- DSCP (Differentiated Services Codepoints)**
 - AF packet-drop precedence values, 294
 - IP precedence values, 293-295
- DSL (Digital Subscriber Lines), 222**
- DSTM (Dual-Stack Transition Mechanism), 359**
- DTMF (Dual-Tone Multifrequency) dialing, digital signaling, 567**
- DTP (Dynamic Trunking Protocol), 105**
- DUAL (Diffusing Update Algorithm), EIGRP, 400-401, 407**
- dual-stack IPv6 deployment model, 360, 363**
- DVMRP (Distance Vector Multicast Routing Protocol), 470**
- DWDM (Dense Wavelength-Division Multiplexing), 228**
- Dynamic interface (WLC), 185**
- dynamic NAT, 300-301**
- dynamic routing versus static routing assignment, 380-381**
- dynamic WEP keys, WLAN, 174**

E

- E-Commerce module (Enterprise Edge module), 52**
- E&M (Ear and Mouth)**
 - ports, 561
 - signaling, 562-565
- E1 circuits (channelized), 562, 565**
- EAP-FAST (EAP-Flexible Authentication via Secure Tunneling), 183**
- EAP-TLS (EAP-Transport Layer Security), 183**
- EAP-TTLS (EAP-Tunneled Transport Layer Security), 183**
- eBGP (External Border Gateway Protocol), 445**
- echo cancellation, VoIP, 595**
- edge distribution, campus LAN, 109**
- EGP (Exterior Gateway Protocols) versus IGP, 382**
- EIGRP (Enhanced Interior Gateway Routing Protocol), 383-388, 398, 462**
 - Acknowledgment packets, 403
 - bandwidth metric, 401-402
 - characteristics of, 399
 - composite metric, 403
 - delay metric, 402
 - DUAL, 400-401, 407
 - Hello packets, 403
 - IPv4, 406
 - IPv6, 353, 406
 - characteristics of, 407-408*
 - network design, 407*
 - neighbor discovery/recovery, 399
 - network design, 404-405
 - protocol-dependent modules, 399
 - Query packets, 403
 - reliability metric, 402
 - Reply packets, 403
 - route redistribution, 460
 - RTRP, 400

- stub routers, 404
 - timers, 399-401
 - Update packets, 403
 - variance command, 405
- Ekahau Site Survey, network audits, 20**
- email**
 - Cisco ESA, 538
 - Cisco WSA, 538-539
- encryption**
 - AES, 172
 - decryption, 529
 - encryption keys, 507-508
 - fundamentals of, 507
 - Secure Services, 507-508
- endpoint security, 533, 545**
- enterprise branch architectures**
 - backups, 271
 - collapsed core design, 275
 - components of, 270
 - design questions, 270
 - dual WAN carriers, 272
 - Flat Layer 2 design, 274
 - Hybrid WAN, 271-275
 - Internet traffic flows, 274
 - Internet WAN, 271
 - large branch design, 275, 278-279
 - medium branch design, 275-277
 - MPLS WAN, 271
 - dual MPLS carriers, 272-273*
 - single MPLS carriers, 272*
 - single WAN carriers, 271
 - small branch design, 275-276
- Enterprise Branch module (Cisco Enterprise Architecture model), 57-59**
- enterprise campus LAN (Local Area Networks), 107-109**
- Enterprise Campus module (Cisco Enterprise Architecture Model), 50, 59**
- enterprise campus security, 545**
- Enterprise Data Center module (Cisco Enterprise Architecture model), 58-59**
- enterprise data centers, 546-547**
- enterprise edge**
 - defining, 218
 - design methodologies, 229
 - application requirements, 230*
 - bandwidth, 231-236*
 - key design principles, 230*
 - links, 232*
 - QoS and bandwidth optimization, 233-236*
 - reliability, 231*
 - response time, 230-231*
 - throughput, 231*
- DMZ, 220**
 - cloud DMZ, 237*
 - connectivity, 236-238*
 - Internet DMZ, 236*
 - per-service DMZ, 238*
 - remote access VPN DMZ, 236*
 - security services DMZ, 237*
 - segmenting, 237*
 - shared DMZ, 238*
 - site-to-site VPN DMZ, 236*
 - unified communications DMZ, 237*
- Internet connectivity, 238-240
- security, 548-550
- SP edge, 220
- VPN, 240-241
- Enterprise Edge module (Cisco Enterprise Architecture Model)**
- E-Commerce module, 52
- Enterprise WAN, 55-56, 59
- Internet Connectivity module, 53-54
- SP edge module, 56
- VPN/Remote Access module, 54-55
- enterprise MAN/WAN architectures, 265-267**
- enterprise teleworker design, WAN, 279-280**
- Enterprise Teleworker module (Cisco Enterprise Architecture model), 58-59**

Enterprise VPN

DMVPN, 257-258

GETVPN, 258

GRE, 257

IPsec, 255

*direct encapsulation, 256-257**DMVPN, 257-258**GETVPN, 258**GRE, 257**IPsec tunneling across the Internet,
263-264**VTI, 258*

Service Provider VPN versus, 255-263

VTI, 258

enterprise WAN architectures

components of, 268-270

Enterprise Edge module, 55-56, 59

growth, support for, 265

HA, 264

implementation costs, 265

network segmentation support, 265

operational complexity, 265

operational expenses, 265

video support, 265

voice support, 265

EoIP tunnels, WLAN, 194**Erlangs, 569-570****Ethernet**

EtherChannel, 110

*LAN design, 88**MEC, 95, 99, 153*

Fast Ethernet

*100BASE-FX Fast Ethernet, 85**100BASE-T4 Fast Ethernet, 84**100BASE-TX Fast Ethernet, 84**LAN design, 84*

Gigabit Ethernet

*10 Gigabit Ethernet, 87**40 Gigabit Ethernet, 87-88**100Gigabit Ethernet, 87-88**1000BASE-CX Gigabit Ethernet over
Coaxial Cable, 86**1000BASE-LX long-wavelength
Gigabit Ethernet, 86**1000BASE-SX short-wavelength
Gigabit Ethernet, 86**1000BASE-T Gigabit Ethernet over
UTP, 86**LAN design, 85-88*

handoffs, 260

LAN design, 83

*EtherChannel, 88**Fast Ethernet, 84**Gigabit Ethernet, 85-88*

Metro Ethernet, 225, 259-260

PoE, 197, 575

exam preparation

Cisco Learning Network, 657

memory tables, 657

Pearson Cert Practice Test engine, 655,
659-660

Pearson IT Certification website, 655-657

practice tests, 655-660

Premium Editions, 657

review tools

*chapter-ending review tools, 658**Pearson IT Certification website, 655**review/study plan, 658*

subnetting practice, 658-659

exams

updates, 699

web resources, 699

Explicit Configuration protocol, 60**Extranet VPN, 241****F****Fast Ethernet**

100BASE-FX Fast Ethernet, 85

100BASE-T4 Fast Ethernet, 84

100BASE-TX Fast Ethernet, 84

LAN design, 84

- fault management (networks), 619
- FEX (Fabric Extenders), DC, 151
- filtering (routing), 461
- final review/study plan (exam preparation), 658
- FirePOWER IPS, 538
- firewalls, 527
 - ACL, 530
 - antivirus software, 529
 - applications
 - application level gateways*, 528
 - filtering*, 529
 - decryption, 529
 - guidelines, 530
 - host-based firewalls, 528
 - hybrid firewalls, 529
 - IOS firewalls, 542
 - IPS, 529
 - NAT, 529
 - NGFW, 529
 - packet-filtering firewalls, 528
 - stateful firewalls, 528
 - transparent mode firewalls, 529
 - URL filtering, 529
 - user identification, 529
- first-hop redundancy protocols, 98
- Flags field (IPv4 headers), 290-291
- Flat Layer 2 design, enterprise branch architectures, 274
- flat routing protocols versus hierarchical protocols, 385
- Flexible NetFlow, 627-628
- FLGS (Flags) field (multicast IPv6 addresses), 345
- flooding and bridges, 90
- Flow Label field (IPv6 headers), 337
- forwarding state (STP switch ports), 102
- foundation layer (enterprise DC), 130
- Fragment Offset field (IPv4 headers), 290-291
- fragmentation, IPv4, 295

- Frame Relay, 224, 228
 - PVC, 225
 - SVC, 225
 - VoFR, 572
- fraud/identity theft (security threats), 490-491
- Friendswood Hospital comprehensive scenario, 641-642, 646-650
- full-mesh topologies, WAN, 253
- FXO (Foreign Exchange Offices), 561
- FXS (Foreign Exchange Stations), 561

G

- Get request messages
 - SNMPv1, 622
 - SNMPv2, 623
- Get response messages
 - SNMPv1, 622
 - SNMPv2, 623
- GetBulk messages (SNMPv2), 623
- GetNext request messages
 - SNMPv1, 622
 - SNMPv2, 623
- GETVPN (Group Encrypted Transport VPN), 258
- Gigabit Ethernet
 - 10 Gigabit Ethernet, 87
 - 40 Gigabit Ethernet, 87-88
 - 100 Gigabit Ethernet, 87-88
 - 1000BASE-CX Gigabit Ethernet over Coaxial Cable, 86
 - 1000BASE-LX long-wavelength Gigabit Ethernet, 86
 - 1000BASE-SX short-wavelength Gigabit Ethernet, 86
 - 1000BASE-T Gigabit Ethernet over UTP, 86
 - LAN design, 85-88
- GLBA (Gramm-Leach-Bliley Act) security legislation, 489

GLBP (Gateway Load Balancing Protocol), 62, 98
 global aggregatable IPv6 addresses, 343
 global unicast IPv6 addresses, 342
 globally unique IPv6 addresses, SLAAC, 350-351
 GoS (Grade of Service), voice networks, 569
 GPRS (General Packet Radio Service), 224
 GRE (Generic Routing Encapsulation), 257
 ground-start signaling, 562-563
 group key handshakes, WLAN, 172
 GSM (Global System for Mobile Communications), 224

H

H.264, VoIP, 587-588
 H.323, VoIP, 582-587, 590
 HA (High Availability)
 enterprise WAN architectures, 264
 WAN and enterprise edge Internet connectivity, 240
 handshakes (security), WLAN, 172
 Header Checksum field (IPv4 headers), 291
 health checklist (network), 23
 Hello packets, EIGRP, 403
 hello timers, OSPFv2, 431
 hierarchical network models
 access layer, 44-46
 benefits of, 41
 collapsed core design, 49
 core layer, 42-45
 distribution layer, 43-45
 examples of, 46-47
 hub-and-spoke design, 48
 route summarization, 42
 hierarchical routing protocols versus flat routing protocols, 385
 High Availability Network Services, 59
 ARP, 60
 Explicit Configuration protocol, 60

GLBP, 62
 HSRP, 61
 RDP, 60
 redundancy
 link media, 65-66
 routes, 63-66
 servers, 62, 66
 RIP, 61
 VRRP, 62
 VSS, 47
 HIPAA (Health Insurance Portability and Accountability Act) security legislation, 489
 HLD (High-Level Design) documents, 16
 hop counts, routing protocols, 388-389
 Hop Limit field (IPv6 headers), 338
 host-based firewalls, 528
 H-REAP (Hybrid Remote Edge AP) mode (AP), 180, 200
 HSRP (Hot Standby Router Protocol), 61, 98
 hub-and-spoke (star) topologies
 hierarchical network design, 48
 WAN, 252
 hubs, LAN, 89
 hybrid firewalls, 529
 hybrid IPv6 deployment model, 361-363
 Hybrid WAN, enterprise branch architectures, 271-275

I

iBGP (Internal Border Gateway Protocol), 445-446
 ICMPv6, 347-348
 Identification field (IPv4 headers), 290-291
 identity management/trust (security)
 802.1X, 527
 access control deployments, 532
 ACL, 527
 certificates, 506
 Cisco ISE, 527, 544

- domains of trust, 503-504
- firewalls, 527-530
- identity-based network services, 531
- IOS, 542
- network access control, 506
- passwords, 505
- port security, 527
- tokens, 505
- identity theft/fraud (security threats), 490-491
- IDS (Intrusion Detection Systems), 534-536
- IEEE 802.1P, VoIP, 596
- IGMP (Internet Group Management Protocol), 113
 - IGMP snooping, 114, 467
 - IGMPv1, 465
 - IGMPv2, 465
 - IGMPv3, 466
- IGP (Interior Gateway Protocols)
 - EGP versus, 382
 - OSPFv2, 430, 462
 - ABR, 434-436*
 - adjacencies, 431*
 - advancements to OSPFv3, 440*
 - areas, 432-433*
 - ASBR, 434-436*
 - backbone routers, 434*
 - changes from OSPFv2, 440*
 - characteristics of, 439*
 - cost metric, 430-431*
 - DR, 435*
 - hello timers, 431*
 - internal routers, 434*
 - LSA, 436*
 - neighbor discovery, 431*
 - NSSA, 438*
 - router authentication, 439*
 - route redistribution, 460*
 - stub areas, 437*
 - totally stubby areas, 438*
 - virtual links, 438*
 - OSPFv3, 462
 - ABR, 440*
 - areas, 440*
 - ASBR, 440*
 - backbone routers, 440*
 - characteristics of, 443*
 - LSA, 441-443*
 - route redistribution, 460*
- IHL (Internet Header Length) field (IPv4 headers), 289-291
- Implement phase (network design), PPDIOO, 15
- infection containment (security), 533
- infinity, counting to (routing loops), 393
- Inform request messages (SNMPv2), 623
- information gathering process (characterizing networks), 19
- Infrastructure layer (SDN), 134
- infrastructure protection (security), 512
- infrastructures (collaboration and video architectures), 8
- inside/outside global addresses, 301
- inside/outside local addresses, 301
- integrity of data (security), 494-497, 509-510
- intercontroller roaming, WLAN, 187-188
- internal routers
 - OSPFv2, 434
 - OSPFv3, 440
- Internet
 - DMZ, 236
 - enterprise branch architectures, traffic flow, 274
 - WAN
 - enterprise branch architectures, 271*
 - enterprise edge connectivity, 238-240*
- Internet Connectivity module (Enterprise Edge module), 53-54
- interoffice trunks, 560
- intertoll trunks, 561
- intracontroller roaming, WLAN, 187

investment (return on), network design, 6

IOS security, 542

IP Address field (RIPv2 message format), 395

IP (Internet Protocol). *See also* IPv4; IPv6

IP multicast

Auto-RP, 469

BSR, 470

CGMP, 466-467

dense multicast, 467-468

DVMRP, 470

IGMP snooping, 467

IGMPv1, 465

IGMPv2, 465

IGMPv3, 466

IPv6 multicast addresses, 470-471

Layer 3 to Layer 2 mapping, 464-465

multicast addresses, 463-464

PIM DR, 469

PIM-SM, 469

shared trees, 468

source trees, 468

sparse multicast, 467-468

IPsec, 255

direct encapsulation, 256-257

DMVPN, 257-258

GETVPN, 258

GRE, 257

IOS, 542

IPsec tunneling across the Internet, 263-264

IPsec VPN SPA, 544

VTI, 258

spoofing, 109

VoIP, 572-573

bandwidth, 590-592, 595-599

control protocols, 581-589

delays, 592-593

design goals, 575

echo cancellation, 595

packet loss, 594

QoS, 595-599

transport protocols, 581-589

VAD, 590-591

IP Options field (IPv4 headers), 291

IP telephony networks, VLSM and IPv4 addressing, 308

IPS (Intrusion Prevention Systems), 529

FirePOWER IPS, 538

guidelines, 535-536

inline IPS and anomaly detection, 534

IOS, 542

IPS NME, 543

pros/cons, 535

security, anomaly detection, 534

signatures, 495

IPT (Internet Protocol Telephony)

codecs, 580-581

components of, 574

CUCM, 574

multisite WAN with centralized call processing, 576

multisite WAN with distributed call processing, 577

single-site deployments, 576

design goals, 575

design recommendations, 600

functional areas, 574

multisite WAN

centralized call processing model, 576

distributed call processing model, 577

PoE, 575

service class recommendations, 600-602

single-site deployments, 576

unified CME deployments, 578

IPv4 (Internet Protocol version 4)

addressing, 296

ARP, 321-322

assigning addresses, 317-319

broadcast addresses, 299

Class A addresses, 297

- Class B addresses*, 298
- Class C addresses*, 298
- Class D addresses*, 298
- Class E addresses*, 298
- goal of*, 310
- IPv4-compatible IPv6 addresses*, 339-340, 344
- multicast addresses*, 299
- NAT*, 300-302, 313
- PAT*, 313
- planning for future growth*, 310
- planning for hierarchical IP address networks*, 311-312
- private addresses*, 299
- private/public IP addresses*, 313
- route summarization*, 311
- standards for addressing*, 313-314
- subnet allocation case study*, 314-316
- unicast addresses*, 299
- EIGRP, 406
- fragmentation, 295
- headers
 - Destination Address field*, 291
 - DSCP*, 293-295
 - DS field*, 293
 - Flags field*, 290-291
 - fragmentation*, 295
 - Fragment Offset field*, 290-291
 - Header Checksum field*, 291
 - Identification field*, 290-291
 - IHL field*, 289-291
 - IP Options field*, 291
 - Padding field*, 291
 - Protocol field*, 290-291
 - Source Address field*, 291
 - Time to Live field*, 290-291
 - ToS field*, 290-293
 - Total Length field*, 290-291
 - Version field*, 289-291
- IPv6
 - dual-stack mechanism*, 357
 - IPv4-compatible IPv6 addresses*, 339-340, 344
 - IPv6 enhancements over IPv4*, 336-337
 - IPv6/IPv4 comparison table*, 363-364
 - partly linked IPv4 addresses in IPv6*, 355
 - protocol translation mechanisms*, 359-360
 - routing protocols versus IPv4 protocols*, 386
 - transition mechanisms*, 357-360
 - tunneling mechanisms*, 357-359
 - whole IPv4 addresses linked in IPv6*, 356
- name resolution
 - DHCP*, 321
 - DNS*, 319-321
- subnetting
 - AND logical operation*, 304
 - design example*, 303-304
 - determining network portion of IP addresses*, 304-305
 - planning for future growth*, 310
 - subnet allocation case study*, 314-316
 - subnet masks*, 302-305
 - VLSM*, 305-310
- IPv6 (Internet Protocol version 6)**
 - addressing
 - /64 subnets*, 354-355
 - address allocations*, 341-342, 355-356
 - address blocks*, 354-355
 - address representation*, 339-340, 344
 - anycast addresses*, 344-346
 - DHCPv6*, 352
 - DHCPv6 Lite*, 352
 - IPv4-compatible IPv6 addresses*, 339-340, 344
 - loopback addresses*, 342

- manual address configuration*, 350
- multicast addresses*, 344-346
- name resolution*, 348-349
- planning*, 354
- prefix allocations*, 341-342
- prefix representation*, 340, 346
- private addresses*, 355
- route summarization*, 354
- SLAAC of globally-unique addresses*, 350-351
- SLAAC of link-local addresses*, 350
- unicast addresses*, 342-346
- deployment models, 357
 - dual-stack model*, 360, 363
 - hybrid model*, 361-363
 - service block model*, 362-363
- EIGRP, 406
 - IPv6 characteristics*, 407-408
 - network design*, 407
- headers, 337-339
- ICMPv6, 347-348
- IPv4
 - dual-stack mechanism*, 357
 - IPv4-compatible IPv6 addresses*, 339-340, 344
 - IPv4/IPv6 comparison table*, 363-364
 - IPv6 enhancements over IPv4*, 336-337
 - partly linked IPv4 addresses in IPv6*, 355
 - protocol translation mechanisms*, 359-360
 - routing protocols versus IPv6 protocols*, 386
 - transition mechanisms*, 357-360
 - tunneling mechanisms*, 357-359
 - whole IPv4 addresses linked in IPv6*, 356
- multicast addresses, 470-471
- ND protocol, 348
- path MTU discovery, 349-350
- routing protocols, 353

- security, 352
- subnetting, 354-355
- IPv6 prefix field (RIPng message format)**, 397
- IS-IS**, 388, 408
 - authentication, 411
 - bandwidth metric, 409
 - characteristics of, 411-412
 - composite metric, 409
 - DR, 410
 - IPv6 and, 353
 - NET addressing, 409
 - network design, 409-411
 - routers (areas), 410
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)**, 359
- ISDN (Integrated Services Digital Network)**, 221
- ISDN PRI/BRI circuits**, 565-566
- ISE (Identity Services Engines)**, 527, 540, 544
- ISM frequencies, WLAN**, 170
- ISP service**, 267
- ISR (Integrated Services Routers)**
 - ISR G2, 525, 542-543
 - teleworkers, 280
- IT optimization**, 6
- IVR systems (PSTN)**, 569

J-K-L

- jitter, VoIP, 594

- Kismet, 491

- L4-7 load balancers (dedicated)**, 160
- LAG (Link Aggregation)**, WLC LAG, 184-186
- LAN (Local Area Networks)**
 - bridges, 89
 - campus LAN

- access layer best practices*, 94-97, 101
- application types*, 93
- core layer best practices*, 99-101
- distribution layer best practices*, 97-101
- enterprise campus LAN*, 107-109
- enterprise DC*, 111
- large-building LAN*, 106
- medium-size LAN*, 109
- multicast traffic*, 113-114
- network requirements*, 93
- QoS*, 111-112
- remote site LAN*, 110
- server farm modules*, 110
- small LAN*, 110
- STP*, 101-103
- STP Toolkit*, 103-105
- transmission media comparisons*, 88
- VLAN trunking*, 105
- enterprise campus LAN*, 107-109
- enterprise DC*, 111
 - access layer*, 147-148
 - aggregation layer*, 147-149
 - architecture of*, 130-131
 - cabling*, 141-143
 - challenges of*, 136
 - cooling requirements/solutions*, 140-141
 - core layer*, 149-150
 - DCI*, 157-159
 - facility considerations*, 136-138
 - FEX*, 151
 - foundation layer*, 130
 - load balancing*, 159-160
 - network programmability*, 133-135
 - physical space constraints*, 138-139
 - power requirements*, 139-140
 - reference architecture*, 146-147
 - SDN*, 134
 - security*, 150
 - servers*, 136
 - services layer*, 130
 - storage*, 144-146
 - topology of*, 133
 - UCS*, 132
 - unified fabric*, 132
 - user services layer*, 131
 - virtualization*, 132, 151-157
- Ethernet, 83
 - EtherChannel*, 88
 - Fast Ethernet*, 84
 - Gigabit Ethernet*, 85-88
- High Availability protocols
 - ARP*, 60
 - Explicit Configuration protocol*, 60
 - GLBP*, 62
 - HSRP*, 61
 - RDP*, 60
 - RIP*, 61
 - VRRP*, 62
 - VSS*, 47
- hubs, 89
- large-building LAN, 106
- Layer 3 switches, 92
- medium-size LAN, 109
- remote site LAN, 110
- repeaters, 89
- routers, 91-92
- server farm modules, 110
- small LAN, 110
- switches, 90-91
- VLAN
 - MST*, 103
 - PVST+*, 102
 - Rapid PVST+*, 102
 - RPVST+*, 147
 - trunking*, 105
 - VTP*, 97
- VPLS, 261
- WLAN, 223
- LanGuard network security scanner, network audits, 20
- LAP (Lightweight Access Protocol), WLC discovery via CAPWAP, 181-182

- large-building LAN (Local Area Networks), 106
 - large office design, enterprise branch architectures, 275, 278-279
 - layer 2 access method (WLAN), 172
 - Layer 2 intercontroller roaming, 187
 - Layer 2 VPN service, 260
 - VPLS, 262
 - VPWS, 261
 - Layer 3 intercontroller roaming, 188
 - Layer 3 switches, LAN, 92
 - Layer 3 VPN service, 260
 - Hybrid WAN, 273-275
 - MPLS, 262-263
 - LEAP (Lightweight Extensible Authentication Protocol), 174, 183
 - learning state (STP switch ports), 102
 - leased line WAN, 252, 255
 - leased links, 232
 - legislation (security), 489
 - LFI (Link Fragmentation and Interleaving), 236, 597-599
 - link-local IPv6 addresses, 343, 350
 - link-state routing protocols, 384
 - links
 - efficiency (QoS), 235-236
 - leased links, 232
 - media redundancy, 65-66
 - private links, 232
 - shared links, 232
 - UDLD protocol, 106
 - virtual links, OSPFv2, 438
 - WAN and enterprise edge design, 232
 - listening state (STP switch ports), 102
 - LLD (Low-Level Design) documents, 16
 - LLDP (Link Layer Discovery Protocol), 20, 630
 - LLQ (Low Latency Queuing), 235, 597-599
 - load balancing
 - application load balancing, DC, 159
 - network load balancing, 160
 - route redundancy, 63
 - WAN backups, 263
 - load metric, routing protocols, 390
 - load sharing, WAN backups, 263
 - local loops, voice networks, 560-561
 - local MAC, 179, 200
 - Local mode (AP), 180
 - local preference attributes, BGP, 450
 - Loop Guard, 97, 104-106
 - loop-start signaling, 562-563
 - loopback addresses
 - IPv6, 342
 - VLSM and IPv4 addressing, 307
 - loops
 - local loops, voice networks, 560-561
 - routing loops
 - counting to infinity versus*, 393
 - poison reverse versus*, 392
 - split horizon versus*, 392
 - triggered updates versus*, 393
 - STP loops, 106, 147
 - LSA (Link-State Agreements)
 - OSPFv2, 436
 - OSPFv3, 441-443
 - LTE (Long Term Evolution), 224
 - LWAPP (Lightweight Access Point Protocol), 177-178
- ## M
-
- malware, 490, 538
 - Manage phase (network design), 10-12
 - Management interface (WLC), 184-185
 - managing
 - Management (Cisco SAFE), 525
 - networks
 - accounting management*, 619
 - CDP*, 629-631
 - configuration management*, 619
 - fault management*, 619

- LLDP*, 630
- NetFlow*, 626-628, 631
- performance management*, 619
- RMON*, 619, 624-628, 631
- security management*, 619
- SNMP*, 619-624, 628
- Syslog*, 630-631
- security, 512-513, 539-541, 619
- MAP (Mesh AP), 196
- MBSA (Microsoft Baseline Security Analyzer), 492
- MD5 authentication, RIPv2, 394
- MEC (Multichassis EtherChannel), 95, 99, 153
- MED attribute, BGP, 451
- medium office design, enterprise branch architectures, 275-277
- medium-size LAN (Local Area Networks), 109
- memory tables (exam preparation), 657
- methodology of network design, 16
- Metric field
 - RIPng message format, 397
 - RIPv2 message format, 395
- metrics, routing protocols
 - bandwidth, 389, 401-402, 409
 - composite, 403, 409
 - cost, 389
 - delay, 391, 402
 - EIGRP, 401-403
 - hop count, 388
 - IS-IS, 409
 - load, 390
 - MTU, 391
 - reliability, 391, 402
- Metro Ethernet, 225, 259-260
- MGCP (Media Gateway Control Protocol), VoIP, 582-584
- MIB (Management Information Bases), SNMP, 620-621
- Migration process (Build phase), 11
- MLP (Multilink PPP), 236
- mobile wireless WAN strategies, 223-224
- mobility groups, WLAN, 189-190
- modems
 - cable modems, 223
 - CMTS, 222
- Monitor mode (AP), 181
- MOS (Mean Opinion Scores), codecs, 581
- MP-BGP (Multiprotocol BGP), 353, 446
- MPLS (Multiprotocol Label Switching), 226-228, 360
 - enterprise branch architectures
 - dual MPLS carriers*, 272-273
 - MPLS WAN*, 271
 - single MPLS carriers*, 272
 - Layer 3 VPN service, 262-263
 - Private MPLS, 267
 - VPLS, 261
- MST (Multiple Spanning Tree), 103
- MTU (Maximum Transmission Units), routing protocols, 391
- multicast (IP)
 - Auto-RP, 469
 - BSR, 470
 - campus LAN, 113-114
 - CGMP, 466-467
 - dense multicast, 467-468
 - DVMRP, 470
 - IGMP
 - IGMP snooping*, 467
 - IGMPv1*, 465
 - IGMPv2*, 465
 - IGMPv3*, 466
 - IPv4 multicast addresses, 299
 - IPv6 multicast addresses, 344-346, 470-471
 - Layer 3 to Layer 2 mapping, 464-465
 - multicast addresses, 463-464
 - PIM DR, 469
 - PIM-SM, 469
 - shared trees, 468

source trees, 468

sparse multicast, 467-468

multiservice networks (converged)

call processing, 571

codecs, 580-581

design recommendations, 600

dial plans, 571

IPT

components of, 574

CUCM, 574-577

design goals, 575

functional areas, 574

multisite WAN with centralized call processing deployments, 576

multisite WAN with distributed call processing deployments, 577

PoE, 575

single-site deployments, 576

unified CME deployments, 578

packetized voice systems, 571

service class recommendations, 600-602

video deployment considerations, 578-579

VoATM, 572

VoFR, 572

VoIP, 572-573

bandwidth, 590-592, 595-599

control protocols, 581-589

delays, 592-593

design goals, 575

echo cancellation, 595

packet loss, 594

QoS, 595-599

transport protocols, 581-589

VAD, 590-591

multisite WAN (Wide Area Networks)

centralized call processing model, 576

distributed call processing model, 577

N

N+1 WLC redundancy, 190-192

N+N WLC redundancy, 191-192

N+N+1 WLC redundancy, 191-192

name resolution, IPv6 addresses, 348-349

NAT (Network Address Translation)

dynamic NAT, 300-301

firewalls, 529

inside/outside global addresses, 301

inside/outside local addresses, 301

IPv4 addresses, 300-302

IPv4 addressing, 313

PAT, 301

public networks, 301

static NAT, 300-301

stub domains, 301

NAT-PT, 359-360

NBAR (Network-Based Application Recognition), 20, 233

ND (Neighbor Discovery) protocol, IPv6, 348

Nessus, 492

NET addressing, IS-IS, 409

NetFlow, 536, 631

benefits of, 627

components of, 626

data analysis, 627

data records, 627

Flexible NetFlow, 627-628

network audits, 20-23

RMON versus, 628

NetscanTools, 491

NetStumbler, 491

Network Analysis Module 3, 544

network services, borderless network architectures, 7

networks

abuse (security threats), 490-491

access control, 506

architectures

benefits of, 9

borderless network architectures, 7

collaboration and video architectures, 8

data center and virtualization architectures, 8-9

- audits, 19
 - AirMagnet Analyzer Pro*, 20
 - CDP, 20
 - Cisco Prime Infrastructure and Solarwinds*, 20
 - Ekabau Site Survey*, 20
 - LanGuard network security scanner*, 20
 - LLDP, 20
 - manual assessments*, 20-22
 - NBAR, 20
 - NetFlow*, 20-23
 - show commands*, 20-22
 - SNMP, 20
 - Syslog, 20
 - Wireshark*, 20
- campus network security, 545
- characterizing, 24
 - information gathering process*, 19
 - network audits*, 19-23
 - performance checklists*, 23
- Cisco Enterprise Architecture Model, 49
 - Enterprise Campus module*, 50, 59
 - Enterprise Edge module*, 52-56, 59
 - remote modules*, 57-59
 - SP edge module*, 56
- designing
 - borderless network architectures*, 7
 - Build phase*, 9-12
 - business forces effects on*, 6
 - campus LAN*, 93-114
 - characterizing networks*, 19-24
 - collaboration and video architectures*, 8
 - competition*, 6
 - customer requirements*, 17-18
 - data center and virtualization architectures*, 8-9
 - design documents*, 25-26
 - Design phase (PPDIOO)*, 14-15
 - EIGRP, 404-407
 - enterprise campus LAN*, 107-109
 - enterprise DC*, 111, 130-160
 - growth of applications*, 6
 - Implement phase (PPDIOO)*, 15
 - IPv6, 407
 - IS-IS, 409-411
 - IT optimization, 6
 - large-building LAN*, 106
 - Manage phase*, 10-12
 - medium-size LAN*, 109
 - methodology of*, 16
 - Operate phase (PPDIOO)*, 15
 - Optimize phase (PPDIOO)*, 15
 - pilot sites*, 25
 - Plan phase*, 9
 - Plan phase (PBM)*, 10-12
 - Plan phase (PPDIOO)*, 14-15
 - PPDIOO, 12-15
 - Prepare phase (PPDIOO)*, 14-15
 - project deliverables*, 16
 - prototype networks*, 25
 - regulation*, 6
 - remote site LAN*, 110
 - removal of borders*, 6
 - return on investment*, 6
 - RIPng, 398
 - RIPv2, 396
 - security integration with network design*, 502
 - server farm modules*, 110
 - small LAN*, 110
 - technological forces effects on*, 6
 - top-down design approach*, 24-25
 - virtualization*, 6
 - VPN, 240-241
 - WAN, 218, 229-241
- hierarchical network models
 - access layer*, 44-46
 - benefits of*, 41
 - collapsed core design*, 49
 - core layer*, 42-45
 - distribution layer*, 43-45
 - examples of*, 46-47
 - hub-and-spoke design*, 48
 - route summarization*, 42

High Availability Network Services, 59
 ARP, 60
 Explicit Configuration protocol, 60
 GLBP, 62
 HSRP, 61
 link media redundancy, 65-66
 RDP, 60
 RIP, 61
 route redundancy, 63-66
 server redundancy, 62, 66
 VRRP, 62
 VSS, 47

IP telephony networks, VLSM and IPv4
 addressing, 308

LAN

 bridges, 89
 campus LAN, 88, 93-114
 enterprise campus LAN, 107-109
 enterprise DC, 111, 130-160
 EtherChannel, 88
 Ethernet design rules, 83-88
 Fast Ethernet, 84
 Gigabit Ethernet, 85-88
 hubs, 89
 large-building LAN, 106
 Layer 3 switches, 92
 medium-size LAN, 109
 remote site LAN, 110
 repeaters, 89
 routers, 91-92
 server farm modules, 110
 small LAN, 110
 switches, 90-91
 VLAN, 97

load balancing, 160

managing

 accounting management, 619
 CDP, 629-631
 configuration management, 619
 fault management, 619
 LLDP, 630
 NetFlow, 626-628, 631

 performance management, 619
 RMON, 619, 624-628, 631
 security management, 619
 SNMP, 619-624, 628
 Syslog, 630-631

performance checklist, 23

pilot sites, 25

programmability, enterprise DC, 133-135

prototype networks, 25

public networks, 301

reconnaissance, 109

segmentation, enterprise WAN architectures, 265

virtualization

 access control, 156-157
 DC, 152
 path isolation, 156-157
 services edge, 157

Next Header field (IPv6 headers), 338

Next Hop field (RIPv2 message format),
 395, 398

next-hop attributes, BGP, 450

Nexus 9000 series switches, 135

NGFW (Next-Generation Firewalls), 529

NGIPS (Next-Generation Intrusion
 Prevention System), 538

NIC (Network Interface Cards), 111

NIP (Network Implementation Plan)
 documents, 16

NMAP (Network Mapper), 491

NMP (Network Migration Plans) and LLD
 documents, 16

NMS manager

 SNMPv1, 622

 SNMPv2, 623

noAuthNoPriv security (SNMPv3), 623

NRFU (Network Ready For Use)
 documents, 16

NSSA (Not So Stubby Areas), OSPFv2, 438

NTP (Network Time Protocol), 540

numbering plans, PSTN switches, 567-568

O

OC (Optical Carrier) rates, SONET/SDH, 226

online resources, 699

OpenDaylight, 135

Operate phase (network design), PPDIOO, 15

Operation Management process (Manage phase), 11

optimization
IT, 6
Optimization process (Manage phase), 11

Optimize phase (network design), PPDIOO, 15

origin attributes, BGP, 450

OSPF (Open Shortest Path First), 383, 388-389

OSPFv2, 384, 462
ABR, 434-436, 440
adjacencies, 431
advancements to OSPFv3, 440
areas, 432-433
ASBR, 434-436
backbone routers, 434
characteristics of, 439
cost metric, 430-431
DR, 435
hello timers, 431
internal routers, 434
LSA, 436
neighbor discovery, 431
NSSA, 438
router authentication, 439
route redistribution, 460
stub areas, 437
totally stubby areas, 438
virtual links, 438

OSPFv3, 384, 462
areas, 440
ASBR, 440
backbone routers, 440

changes from OSPFv2, 440
characteristics of, 443
internal routers, 440
IPv6 and, 353
LSA, 441-443
route redistribution, 460

outdoor wireless, WLAN, 195-196

outside/inside global addresses, 301

outside/inside local addresses, 301

overlapping dynamic NAT, 300

overloading dynamic NAT, 300

P

packets
filtering firewalls, 528
inspection, NBAR, 233
loss, VoIP, 594
packet-switched WAN, 252
packetized voice systems, converged multiservice networks, 571
sniffers, 109

Padding field (IPv4 headers), 291

partial-mesh topologies, WAN, 253

passwords (security), 505

PAT (Port Address Translation), 301, 313

path attributes, BGP, 449

path isolation, network virtualization, 156-157

path MTU, IPv6, 349-350

Payload Length field (IPv6 headers), 338

PBM (Plan, Build, Manage) phase
Build phase, 11-12
design methodology, 16
Manage phase, 11-12
Plan phase, 10-12

PBR (Policy-Based Routing), 455

PBX switches, voice networks, 559

PBX-to-CO trunks, 561

PCI DSS (Payment Card Industry Data Security Standard) security legislation, 489

PEAP (Protected Extensible Authentication Protocol), 183

Pearson Cert Practice Test engine, 655, 659-660

Pearson IT Certification website, 655-657

performance, networks

checklists, 23

managing, 619

per-service DMZ, 238

physical security, 510-511

pilot sites, 25

PIM DR, 469

PIM-SM, 469

PKI (Public Key Infrastructure), 542

Plan phase (network design), 9

PBM, 10-12

PPDIOO, 14-15

PoE (Power over Ethernet), 197, 575

point-to-point topologies, WAN, 254

poison reverse, routing loops, 392

policing (QoS), 233-235

policy and control (borderless network architectures), 7

PortFast, 97, 103-105

ports

authentication, WLAN security, 173

CAS circuits, 562

CCS circuits, 562-563

channelized T1/E1 circuits, 562

E&M, 561

FXO, 561

FXS, 561

scanning attacks, 491

security, 527

STP switch ports, 102

voice networks, 561-562

power requirements, DC, 139-140

PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) phase

benefits of, 12-13

Design phase, 14-15

Implement phase, 15

Operate phase, 15

Optimize phase, 15

Plan phase, 14-15

Prepare phase, 14-15

PQ (Priority Queuing), 234

practice tests (exam preparation), 655-660

Prefix Length field (RIPng message format), 397

Premium Editions (exam preparation), 657

Prepare phase (PPDIOO), 14-15

preparing for the exam

Cisco Learning Network, 657

memory tables, 657

Pearson Cert Practice Test engine, 655, 659-660

Pearson IT Certification website, 655-657

practice tests, 655-660

Premium Editions, 657

review tools

chapter-ending review tools, 658

Pearson IT Certification website, 655

review/study plan, 658

subnetting practice, 658-659

private IP addresses, 313

private IPv4 addresses, 299

private IPv6 addresses, 355

private links, 232

Private MPLS (Multiprotocol Label Switching), 267

Private WAN (Wide Area Networks), 266

processing delays, VoIP, 593-594

Product Support process (Manage phase), 11

programmability (network), enterprise DC, 133

ACI, 135

API, 135

SDN, 134

SDN controllers, 134

project deliverables

HLD documents, 16

LLD documents, 16

NRFU documents, 16

propagation delay, VoIP, 593-594**Protocol field (IPv4 headers), 290-291****protocol translation mechanisms,**

IPv4-toIPv6 transitions, 359-360

prototype networks, 25**proxy firewalls. *See* application level
gateways****pseudowires. *See* VPWS****PSTN (Public Switched Telephone
Networks)**

SP edge module, 56

switches

*ACD, 569**Centrex services, 569**country codes, 567-568**database services, 569**IVR systems, 569**numbering plans, 567-568**voice mail, 569**voice networks, 559-560, 567-569***public IP addresses, 313****public networks, 301****pulse (rotary) dialing, digital signaling, 567****Pure OpenFlow, 135****PVC (Permanent Virtual Circuits), 225****PVST+ (Per VLAN Spanning Tree Plus),
102****Q**

Q.SIG, 563, 566**QoS (Quality of Service). *See also*
bandwidth**

Auto QoS, 599

campus LAN, 111-112

classification, 233

congestion management, 234

link efficiency, 235-236

policing, 233-235

QoS policing, 495

QPPB, 446

queuing, 233-235

traffic shaping, 233-235

video networks, 595-599

VoIP, 595-599

WAN and enterprise edge design, 233-236

window size, 236

WLAN campus design, 197-199

**QPPB (QoS Policy Propagation on BGP),
446****Query packets, EIGRP, 403****queuing**

delays, VoIP, 593-594

QoS, 233-235

R

rack-mounted servers, enterprise DC, 136**Rapid PVST+ (Per VLAN Spanning Tree
Plus), 102****RAP (Rooftop AP), 196****RDP (Remote Desktop Protocol), 60****REAP (Remote-Edge AP), WLAN branch
design, 200****reconnaissance**

networks, 109

security threats, 490-491

records (CDR), voice networks, 571**redistribution (routing), 458-460****redundancy**

enterprise brand architectures, 271

link media, 65-66

routes, 66

*availability, 63-64**load balancing, 63*

servers, 62, 66

VSS, 46-47

WAN

*backup links, 263**bandwidth, 263*

- IPsec tunneling across the Internet*, 263-264
- load sharing/balancing*, 263
- secondary WAN links*, 263
- WLAN
 - controller redundancy design*, 190-192
 - N+1 WLC redundancy*, 190-192
 - N+N+1 WLC redundancy*, 191-192
 - N+N WLC redundancy*, 191-192
- WLC
 - controller redundancy design*, 190-192
 - N+1 WLC redundancy*, 190-192
 - N+N WLC redundancy*, 191-192
 - N+N+1 WLC redundancy*, 191-192
- workstation-to-router redundancy protocols, 66
 - ARP, 60
 - Explicit Configuration protocol*, 60
 - GLBP, 62
 - HSRP, 61
 - RDP, 60
 - RIP, 61
 - VRRP, 62
 - VSS, 47
- regulation, network design, 6
- reliability
 - reliability metric, routing protocols, 391, 402
 - WAN and enterprise edge design, 231
- remote access VPN, 236, 241
- remote modules (Cisco Enterprise Architecture model)
 - Enterprise Branch module, 57-59
 - Enterprise Data Center module, 58-59
 - Enterprise Teleworker module, 58-59
- remote site connectivity, WAN, 254-255
- remote site LAN (Local Area Networks), 110
- removal of borders, network design, 6
- repeaters, LAN, 89
- Reply packets, EIGRP, 403
- requirements (customer) and network design, 17-18
- resources (web), 699
- response time, WAN and enterprise edge design, 230-231
- return on investment, network design, 6
- review tools (exam preparation)
 - chapter-ending review tools, 658
 - Pearson IT Certification website, 655
- review/study plan (exam preparation), 658
- RF groups, WLAN, 193-194
- RF site surveys, WLAN, 194
- RIP (Routing Information Protocol), 61
 - RIPv1, 382-383, 393-395
 - RIPv2, 382-383, 388, 393
 - authentication*, 394
 - characteristics of*, 396
 - message format*, 394-395, 398
 - network design*, 396
 - routing database*, 394
 - timers*, 396
- RIPng, 383, 386, 393
 - authentication, 397
 - characteristics of, 398
 - IPv6 and, 353
 - message format, 397
 - network design, 398
 - timers, 397
- risk assessments (security), 500-501
- risk indexes (security), 501
- RMON (Remote Monitoring), 619, 631
 - NetFlow versus, 628
 - RMON1, 624-625
 - RMON2, 625-626
- roaming
 - intercontroller roaming, 187-188
 - intracontroller roaming, WLAN, 187
- Rogue Detector mode (AP), 181
- root bridges, 90, 102
- Root Guard, 97, 104-105

rotary (pulse) dialing, digital signaling, 567

route redundancy, 66

availability, 63-64

load balancing, 63

route reflectors, BGP, 446-447

route summarization

hierarchical network models, 42

IPv4 addresses, 311

IPv6 addresses, 354

Route tag field

RIPng message format, 397

RIPv2 message format, 395

routers

ABR

OSPFv2, 434-436

OSPFv3, 440

ASBR

OSPFv2, 434-436

OSPFv3, 440

authentication, OSPFv2, 439

backbone routers

OSPFv2, 434

OSPFv3, 440

BSR, 470

internal routers

OSPFv2, 434

OSPFv3, 440

IS-IS, 410

ISR G2, 525

LAN, 91-92

security, 548

stub routers, EIGRP, 404

workstation-to-router redundancy protocols, 66

ARP, 60

Explicit Configuration protocol, 60

GLBP, 62

HSRP, 61

RDP, 60

RIP, 61

VRRP, 62

VSS, 47

routing

loops, 392-393

PBR, 455

route filtering, 461

route redistribution, 458-460

route summarization, 455-458

weight, BGP, 453

routing protocols

administrative distance, 386-387

bandwidth metric, 389, 401-402, 409

BGP, 382-383, 388

characteristics of, 380

classful routing protocols, 385

classless routing protocols, 385

composite metric, 403, 409

cost metric, 389

counting to infinity, 393

delay metric, 391, 402

distance-vector routing protocols, 383-384

dynamic routing assignments, 380-381

EGP versus IGP, 382

EIGRP, 383-388, 398

Acknowledgment packets, 403

bandwidth metric, 401-402

characteristics of, 399

composite metric, 403

delay metric, 402

DUAL, 400-401, 407

Hello packets, 403

IPv4, 406

IPv6, 406-408

neighbor discovery/recovery, 399

network design, 404-405

protocol-dependent modules, 399

Query packets, 403

reliability metric, 402

Reply packets, 403

RTP, 400

stub routers, 404

- timers*, 399-401
- Update packets*, 403
- variance command*, 405
- flat routing protocols, 385
- hierarchical routing protocols, 385
- hop count, 388-389
- IGP versus EGP, 382
- IPv4 protocols, 386
- IPv6 protocols, 386
- IS-IS, 388, 408
 - authentication*, 411
 - bandwidth metric*, 409
 - characteristics of*, 411-412
 - composite metric*, 409
 - DR*, 410
 - NET addressing*, 409
 - network design*, 409-411
 - routers (areas)*, 410
- link-state routing protocols, 384
- load metric, 390
- MTU metric, 391
- OSPF, 383, 388-389
 - OSPFv2*, 384
 - OSPFv3*, 384
- poison reverse, 392
- reliability metric, 391, 402
- RIPng, 383, 386, 393
 - authentication*, 397
 - characteristics of*, 398
 - message format*, 397
 - network design*, 398
 - timers*, 397
- RIPv1, 382-383, 393-395
- RIPv2, 382-383, 388, 393
 - authentication*, 394
 - characteristics of*, 396
 - message format*, 394-395, 398
 - network design*, 396
 - routing database*, 394
 - timers*, 396

- routing loops, 392-393
- split horizon, 392
- static routing assignments, 380-381
- summarization, 393
- triggered updates, 393

RP (Rendezvous Points), Auto-RP, 469

RPVST+ (Rapid Per-VLAN Spanning Tree Plus), 97, 147

RRM (Radio Resource Management)

- WLAN, 192-193

- WLC, 193

RR (Resource Records), 320

RSN (Robust Security Networks), WLAN, 172

RSVP (Resource Reservation Protocol), VoIP, 597

RTCP (Real-time Transport Control Protocol), VoIP, 582-583, 590

RTP (Real-time Transport Protocol), 236

- cRTP, 583, 596, 599

- EIGRP packets, 400

- VoIP, 582-583, 589

S

SAINT (Security Administrator's Integrated Network Tool), 492

scaling servers, 155

SCCP (Skinny Client Control Protocol), VoIP, 582, 589

scenarios (comprehensive)

- Big Oil and Gas, 642-643, 650-651

- Diamond Communications, 645-646, 652-653

- Friendswood Hospital, 641-642, 646-650

- Video Games Spot, 643-645, 651-652

SCF (Security Control Framework), 526

SCOP (Scope) field (multicast IPv6 addresses), 345

SCP (Signaling Control Points), SS7, 567

SDN (Software-Defined Networking)

- Application layer, 134

- Control layer, 134
- controllers, 134-135
- enterprise DC, 134
- Infrastructure layer, 134

security

- 4-way handshakes, 172
- AAA, 542
- accounting, 506
- ACL, 495
- adware, 490
- AES, 172
- AIM, 543
- AMP, 538
- application security, 533
- ASA, 525, 540, 543, 548
- ASA Services Modules, 544
- authentication, 173, 182-183, 506, 532
- authorization, 506
- AVC, 538
- campus networks, 545
- Catalyst 6500 security service modules, 544
- certificates, 506
- Cisco Catalyst switches, 526
- Cisco ESA, 538
- Cisco ISE, 527
- Cisco SAFE
 - ASA, 525
 - benefits of*, 525
 - Cisco Catalyst switches*, 526
 - Cisco SCF*, 526
 - Compliance*, 524
 - ISR G2*, 525
 - Management*, 525
 - Secure Services*, 524
 - Security Intelligence*, 525
 - Segmentation*, 525
 - Threat Defense*, 524
- Cisco TDS
 - infrastructure protection*, 512
 - physical security*, 510-511

- Cisco WSA, 538-539
- confidentiality breaches, 496-497
- configuration/software archive hosts, 540
- content security defense, 533
- continuous security, 501-502
- CSM, 540
- DAI, 495
- data centers, 546-547
- data integrity, 509-510
- data leaks, 490-491
- DC, 150
- DDoS attacks, 495
- design goals, 488
- DHCP snooping, 495
- digital security, 510
- disclosure/data modification attacks, 490-491
- DoS attacks, 490, 495
- email, ESA, 538
- encryption
 - AES, 172
 - decryption*, 529
 - encryption keys*, 507-508
 - fundamentals of*, 507
- endpoints, 533, 545
- enterprise edge, 548-550
- firewalls, 527
 - ACL, 530
 - antivirus software*, 529
 - application level gateways*, 528
 - application-filtering*, 529
 - decryption*, 529
 - guidelines*, 530
 - host-based firewalls*, 528
 - hybrid firewalls*, 529
 - IOS, 542
 - IPS, 529
 - NAT, 529
 - NGFW, 529
 - packet-filtering firewalls*, 528
 - stateful firewalls*, 528

- transparent mode firewalls*, 529
 - URL filtering*, 529
 - user identification*, 529
- group key handshakes, 172
- identity theft/fraud, 490-491
- IDS, 534
 - guidelines*, 535-536
 - pro/cons*, 535
- infection containment, 533
- infrastructure protection, 512
- integrating security into network devices
 - ASA, 543
 - ASA VPN, 543
 - Catalyst 6500 security service modules*, 544
 - Cisco ISE*, 544
 - endpoint security*, 545
 - IOS security*, 542
 - ISR G2 security*, 542-543
- integrity violations, 496-497
- IOS security, 542
- IPS
 - FirePOWER IPS*, 538
 - guidelines*, 535-536
 - inline IPS and anomaly detection*, 534
 - IOS*, 542
 - pros/cons*, 535
 - signatures*, 495
- IPS NME, 543
- IPsec
 - IOS*, 542
 - IPsec VPN SPA*, 544
- IPv6, 352
- ISE, 540, 544
- ISR G2, 525, 542-543
- LanGuard network security scanner, network audits, 20
- legislation, 489
- lifecycle of, 497-498
- malware, 490, 538
- management solutions, 512-513
- managing, 539
 - ASA, 540
 - configuration/software archive hosts*, 540
 - CSM, 540
 - ISE, 540
 - networks*, 619
 - NTP, 540
 - security management network*, 540-541
 - system administration jump hosts*, 540
- MBSA, 492
- NetFlow, 536
- Network Analysis Module 3, 544
- networks
 - abuse*, 490-491
 - access control*, 506
 - design*, 502
 - managing*, 619
- NGIPS, 538
- NTP, 540
- passwords, 505
- physical security, 510-511
- PKI, 542
- policies, 497
 - basic approach of*, 498
 - components of*, 499-500
 - continuous security*, 501-502
 - creating*, 498
 - defined*, 498
 - purpose of*, 499
 - risk assessments*, 500-501
 - risk indexes*, 501
- port scanning, 491
- port security, 527
- process of, 497-498
- QoS policing, 495
- reconnaissance attacks, 490-491
- risks
 - assessments*, 500-501
 - data confidentiality*, 494

- data integrity*, 494
- indexes*, 501
- system availability*, 494-495
- targets*, 494
- routers, 548
- RSN, 172
- Secure Services, 506
 - data integrity*, 509-510
 - DMZ*, 237
 - encryption*, 507-508
 - transmission confidentiality*, 509
 - VPN protocols*, 508-509
- service disruption, 490-491
- SNMP, 536
 - SNMPv1*, 624
 - SNMPv2*, 624
 - SNMPv3*, 623-624
- spyware, 490
- SSH, 542
- SSL, 542
- Syslog, 536
- system administration jump hosts, 540
- targets, 494
- threat categories
 - adware*, 490
 - data leaks*, 490-491
 - DDoS attacks*, 495
 - disclosure/data modification*, 490-491
 - DoS attacks*, 490, 495
 - identity theft/fraud*, 490-491
 - malware*, 490
 - network abuse*, 490-491
 - reconnaissance*, 490-491
 - service disruption*, 490-491
 - spyware*, 490
 - unauthorized access*, 490-494
- threat detection/mitigation, 533, 536-537
- tokens, 505
- transmission confidentiality, 509
- trust/identity management
 - 802.1X*, 527
 - access control deployments*, 532
 - ACL*, 527
 - certificates*, 506
 - Cisco ISE*, 527, 544
 - domains of trust*, 503-504
 - firewalls*, 527-530
 - identity-based network services*, 531
 - network access control*, 506
 - passwords*, 505
 - port security*, 527
 - tokens*, 505
- unauthorized access attacks, 490-494
- uRFP, 495
- URL filtering, 538
- USB, 543
- voice networks, Secure Voice, 543
- VPN
 - ASA VPN*, 543
 - built-in acceleration*, 543
 - IPsec VPN SPA*, 544
 - WebVPN Services Module*, 544
- vulnerability scanners, 492-493
- WebVPN Services Module, 544
- WLAN, 172
 - controlling server access*, 174
 - design approach*, 173
 - dynamic WEP keys*, 174
 - LEAP*, 174
 - port-based authentication*, 173
 - unauthorized access*, 173
- segmentation
 - Cisco SAFE, 525
 - networks, enterprise WAN architectures, 265
- serialization delay, VoIP, 593-594
- server distribution switches, 110
- server farm modules, 110
- servers
 - access, controlling, WLAN, 174
 - blade servers, enterprise DC, 136
 - connectivity options, 111

- enterprise DC, 136
- rack-mounted servers, enterprise DC, 136
- redundancy, 62, 66
- scaling, 155
- virtualization, 155
- service block IPv6 deployment model, 362-363**
- service disruption (security threats), 490-491**
- Service-Port interface (WLC), 184-185**
- Service Provider VPN**
 - Enterprise VPN versus, 255-263
 - Layer 2 VPN service, 260
 - VPLS*, 262
 - VPWS*, 261
 - Layer 3 VPN service, 260
 - Hybrid WAN*, 273-275
 - MPLS*, 262-263
 - Metro Ethernet, 259-260
 - MPLS
 - Layer 3 VPN service*, 262-263
 - Private MPLS*, 267
 - VPLS*, 261
 - VPLS, 261-262
 - VPWS, 260-261
- services edge, network virtualization, 157**
- services layer (enterprise DC), 130**
- session control services, video networks, 579**
- Set request messages**
 - SNMPv1, 622
 - SNMPv2, 623
- shared DMZ, 238**
- shared links, 232**
- show commands, network audits, 20-22**
- signaling**
 - CAS T1/E1 circuits, 562, 565
 - CCS ISDN PRI circuits, 563-565
 - E&M, 562-565
 - ground-start signaling, 562-563
 - IEEE 802.1P, VoIP, 596
 - ISDN PRI/BRI circuits, 565-566
 - loop-start signaling, 562-563
 - Q.SIG, 563, 566
 - SS7 interswitch PSTN signaling, 563, 566-567
 - voice networks
 - analog signaling*, 562-567
 - digital signaling*, 562-567
- signatures (digital), 510**
- single NIC (Network Interface Cards), 111**
- SIP (Session Initiation Protocol), VoIP, 582, 588-590**
- site-to-site VPN, 236, 241**
- SLA (Service Level Agreements), WAN, 218**
- SLAAC (Stateless Address Autoconfiguration)**
 - DHCPv6 and, 352
 - globally unique IPv6 addresses, 350-351
 - link-local IPv6 addresses, 350
- small LAN (Local Area Networks), 110**
- small office design, enterprise branch architectures, 275-276**
- Sniffer mode (AP), 181**
- SNMP (Simple Network Management Protocol), 536, 619**
 - components of, 620
 - MIB, 620-621
 - NetFlow versus SNMP, 628
 - network audits, 20
 - SNMPv1, 622-624
 - SNMPv2, 622-624
 - SNMPv3, 623-624
- Solarwinds, Cisco Prime Infrastructure and, 20**
- Solution Support process (Manage phase), 11**
- SONET/SDH, 225-226**
- Source Address field**
 - IPv4 headers, 291
 - IPv6 headers, 338

SOX (Sarbane-Oxley) security legislation, 489

spanning-tree portfast default global commands, 97

SP (Service Provider) edge, 220

SP edge module

 Cisco Enterprise Architecture Model, 56

 Enterprise Edge model, 56

SP MPLS/IP VPN, 267

split horizon, routing loops, 392

spyware, 490

SS7 interswitch PSTN signaling, 563, 566-567

SSH (Secure Shell), 542

SSID (Service Set Identifiers), WLAN, 171

SSL (Secure Sockets Layer), 542

SSP (Signaling Switching Point), SS7, 567

standalone mode (H-REAP), 200

star (hub-and-spoke) topologies, WAN, 252

stateful firewalls, 528

stateless firewalls. *See* packets, filtering firewalls

static NAT, 300-301

static routing, 380-381, 462

storage

 DC storage, 144-146

 storage services, video networks, 579

STP (Spanning Tree Protocol)

 bridges and, 90

 campus LAN, 101-103

 loops, 106, 147

 MST, 103

 PVST+, 102

 Rapid PVST+, 102

 root bridges, 102

 RPVST+, 97, 147

 switch ports, 102

 UDLD protocol, 106

STP Toolkit

 BackboneFast, 104-105

 BPDU Filter, 104-105

BPDU Guard, 97, 104-105

Design Strategy, 97

Loop Guard, 97, 104-106

PortFast, 97, 103-105

Root Guard, 97, 104-105

UplinkFast, 104-105

Strategy and Analysis process (Plan phase), 10

stub areas, OSPFv2, 437

stub domains, 301

stub routers, EIGRP, 404

study/review plan (exam preparation), 658

Subnet Mask field (RIPv2 message format), 395

subnetting

 IPv4 addresses

AND logical operation, 304

design example, 303-304

determining network portion of IP addresses, 304-305

planning for future growth, 310

subnet allocation case study, 314-316

subnet masks, 302-305

VLSM, 305-310

 IPv6 addresses, 354-355

 practicing (exam preparation), 658-659

summarization (routing), 393, 455-458

SVC (Switched Virtual Circuits), 225

switches

 Catalyst 6500 security service modules, 544

 Cisco Catalyst switches, 526

 LAN, 90-91

 MST, 103

 Nexus 9000 series switches, 135

 PBX switches, voice networks, 559

 PSTN switches

ACD, 569

Centrex services, 569

country codes, 567-568

- database services*, 569
- IVR systems*, 569
- numbering plans*, 567-568
- voice mail*, 569
- voice networks*, 559-560, 567-569
- PVST+, 102
- Rapid PVST+, 102
- server distribution switches, 110
- server farm switches, 110
- STP switch ports, 102
- virtual switches, 156
- switchport host commands, 97
- Syslog, 20, 36, 630-631
- system administration jump hosts and security management, 540
- system availability (security risks), 494-495

T

- T1 circuits (channelized), 562, 565
- tandem trunks, 560
- tariffs, 218, 229
- TDM (Time-Division Multiplexing), 225
- TDS (Threat Defense System)
 - infrastructure protection, 512
 - physical security, 510-511
- technological forces and network design, 6
- teleworkers
 - enterprise teleworker design, WAN, 279-280
 - ISR, 280
- tests (practice), 655-660
- TFTP (Trivial File Transfer Protocol), VoIP, 582, 589
- Threat Defense (Cisco SAFE), 524
- threat detection/mitigation (security), 533, 536-537
- throughput, WAN and enterprise edge design, 231. *See also* bandwidth
- tie trunks, 561
- Time to Live field (IPv4 headers), 290-291
- timers
 - EIGRP, 399-401
 - RIPng, 397
 - RIPv2, 396
- tokens (security), 505
- toll-connecting trunks, 561
- top-down network design, 24-25
- topologies, WAN
 - full-mesh, 253
 - hub-and-spoke (star), 252
 - partial-mesh, 253
 - point-to-point, 254
 - star (hub-and-spoke), 252
- ToS (Type of Service) field (IPv4 headers), 290-293
- Total Length field (IPv4 headers), 290-291
- totally stubby areas, OSPFv2, 438
- traffic
 - BHT, 570
 - busy hour (voice networks), 570
 - shaping (QoS), 233-235
- Traffic Class field (IPv6 headers), 337
- transmission confidentiality (security), 509
- transparent mode firewalls, 529
- transport services, video networks, 579
- Trap messages
 - SNMPv1, 622
 - SNMPv2, 623
- triggered updates, routing loops, 393
- trunking
 - CO-to-PBX trunks, 561
 - DTP, 105
 - interoffice trunks, 560
 - intertoll trunks, 561
 - PBX-to-CO trunks, 561
 - tandem trunks, 560
 - tie trunks, 561
 - toll-connecting trunks, 561
 - VLA, 105

voice networks, 560-561

VTP, 97

trust/identity management (security)

802.1X, 527

access control deployments, 532

ACL, 527

certificates, 506

Cisco ISE, 527, 544

domains of trust, 503-504

firewalls, 527-530

identity-based network services, 531

IOS, 542

network access control, 506

passwords, 505

port security, 527

tokens, 505

tunneling

EAP-FAST, 183

EAP-TTLS, 183

EoIP tunnels, WLAN, 194

IPsec tunneling across the Internet,
263-264

IPv6 over IPv4 tunnels, 357-359

ISATAP, 359

VTI, 258

U

UCS (Unified Computing System),
enterprise DC, 132

UDLD (Unidirectional Link Detection)
protocol, 106

UMTS (Universal Mobile Telecommunica-
tions Service), 224

unauthorized access (security threats), 109,
490-494

unicast IPv4 addresses, 299

unicast IPv6 addresses, 342, 346

global aggregatable addresses, 343

global unicast addresses, 342

IPv4-compatible IPv6 addresses, 344

link-local addresses, 343

unique local addresses, 343

unified communications DMZ, 237

unified computing, data center and
virtualization architectures, 9

unified fabric

data center and virtualization architectures,
8

enterprise DC, 132

unified management, data center and
virtualization architectures, 8

unified networks, 571

UNII frequencies, WLAN, 170

unique local IPv6 addresses, 343

Update packets, EIGRP, 403

updates

exam updates, 699

triggered updates, routing loops, 393

UplinkFast, 104-105

uRFP (Unicast Reverse Path Forwarding),
495

URL filtering, 529, 538

USB (Universal Serial Buses), security, 543

user authentication, 532

user identification, 529

user services, borderless network architec-
tures, 7

user services layer (enterprise DC), 131

UTP (Unshielded Twisted Pair),
1000BASE-T Gigabit Ethernet over
UTP, 86

V

VAD (Voice Activity Detection), VoIP,
590-591

Validation process (Build phase), 11

variance command (EIGRP), 405

Version field

IPv4 headers, 289-291

IPv6 headers, 337

RIPng message format, 397

RIPv2 message format, 395

video

collaboration and video architectures, 8

enterprise WAN architectures, 265

video networks

access services, 579

bandwidth, 595-599

bridging services, 579

CCS, 570

deployment considerations, 578-579

Erlangs, 569-570

QoS, 595-599

session control services, 579

storage services, 579

transport services, 579

Video Games Spot comprehensive scenario, 643-645, 651-652

virtual circuits

PVC, 225

SVC, 225

Virtual interface (WLC), 185

virtual links, OSPFv2, 438

virtual offices

enterprise teleworker design, WAN,
279-280

ISR, 280

virtual switches, 156

virtualization

data center and virtualization architectures,
8-9

DC, 151

access control, 156-157

device contexts, 155

device virtualization, 153

network virtualization, 152

path isolation, 156-157

risks of, 152

servers, 155

services edge, 157

virtual switches, 156

vPC, 154

VRF, 154

VSS, 153

device contexts, 155

device virtualization, DC, 153

enterprise DC, 132

networks

access control, 156-157

DC, 152

design, 6

path isolation, 156-157

services edge, 157

servers, 155

virtual switches, 156

vPC, 154

VRF, 154

VSS, 153

viruses, antivirus software, 529

VLAN (Virtual Local Area Networks)

MST, 103

PVST+, 102

RPVST+, 97, 102, 147

trunking, 105

VTP, 97

VLSM (Variable-Length Subnet Masks), IPv4 addressing

address assignment

example 1, 305-307

example 2, 308-310

IP telephony networks, 308

loopback addresses, 307

VMware NSX Controller, 135

VoATM (Voice over Asynchronous Transfer Mode), 572

VoFR (Voice over Frame Relay), 572

voice mail (PSTN), 569

voice networks

BHT, 570

blocking probability, 571

busy hour, 570

CDR, 571

converged multiservice networks

call processing, 571

codecs, 580-581

- design recommendations*, 600
- dial plans*, 571
- IPT*, 574-578
- packetized voice systems*, 571
- service class recommendationx*, 600-602
- VoATM*, 572
- VoFR*, 572
- VoIP*, 572-575, 581-599
- enterprise WAN architectures, 265
- GoS, 569
- IPT
 - codecs*, 580-581
 - components of*, 574
 - CUCM*, 574-577
 - design goals*, 575
 - design recommendations*, 600
 - functional areas*, 574
 - multisite WAN with centralized all processing deployments*, 576
 - multisite WAN with distributed all processing deployments*, 577
 - PoE*, 575
 - service class recommendations*, 600-602
 - single-site deployments*, 576
 - unified CME deployments*, 578
- local loops, 560-561
- PBX switches, 559
- ports, 561-562
- PSTN switches, 559-560, 567-569
- security, Secure Voice, 543
- signaling
 - analog signaling*, 562-567
 - digital signaling*, 562-567
- trunks, 560-561
- VoIP
 - bandwidth*, 590-592, 595-599
 - control protocols*, 581-589
 - delays*, 592-593
 - echo cancellation*, 595
 - packet loss*, 594
 - QoS*, 595-599
 - transport controls*, 581-589
 - VAD*, 590-591
- VoIP (Voice over Internet Protocol)**, 572-573
 - bandwidth*, 590-592, 595-599
 - control protocols*, 581-589
 - delays*, 592-593
 - design goals*, 575
 - echo cancellation*, 595
 - packet loss*, 594
 - QoS*, 595-599
 - transport protocols*, 581-589
 - VAD*, 590-591
- vPC (Virtual Port Channel)**, 154
- VPLS (Virtual Private LAN Services)**, 261-262
- VPN/Remote Access module (Enterprise Edge module)**, 54-55
- VPN (Virtual Private Networks)**, 240
 - acceleration (built-in)*, 543
 - ASA VPN*, 543
 - benefits of*, 263
 - Enterprise VPN*
 - DMVPN*, 257-258
 - GETVPN*, 258
 - GRE*, 257
 - IPsec*, 255-257
 - Service Provider VPN versus*, 255-263
 - VTI*, 258
 - Extranet VPN*, 241
 - IPsec VPN SPA*, 544
 - Layer 2 VPN service*, 260
 - VPLS*, 262
 - VPWS*, 261
 - Layer 3 VPN service*, 260
 - Hybrid WAN*, 273-275
 - MPLS*, 262-263
 - protocols, Secure Services*, 508-509

- remote access
 - requirements, 241*
 - VPN, 241*
- Service Provider VPN
 - Enterprise VPN versus, 255-263*
 - Layer 2 VPN service, 260-262*
 - Layer 3 VPN service, 260-263, 273-275*
 - Metro Ethernet, 259-260*
 - MPLS, 261-263*
 - VPLS, 261-262*
 - VPWS, 260-261*
- site-to-site VPN, 241
- WebVPN Services Module, 544
- VPWS (Virtual Private Wire Services), 260-261
- VRF (Virtual Routing and Forwarding), 154
- VRRP (Virtual Router Redundancy Protocol), 62
- VSS (Virtual Switching Systems), 46-47, 98, 153
- VTI (Virtual Tunnel Interface), 258
- VTP (VLAN Trunking Protocol), 97
- vulnerability scanners, 492-493

W – X – Y – Z

WAN (Wide Area Networks)

- backups
 - backup links, 263*
 - bandwidth, 263*
 - IPsec tunneling across the Internet, 263-264*
 - secondary WAN links, 263*
- benefits of, 263
- cell-switched WAN, 252
- circuit-switched WAN, 252
- connectivity, 219
- costs, 218
- defining, 218
- design requirements, 218
- DMZ connectivity, 236-238

- enterprise branch architectures
 - backups, 271*
 - collapsed core design, 275*
 - components of, 270*
 - design questions, 270*
 - dual MPLS carriers, 272-273*
 - dual WAN carriers, 272*
 - Flat Layer 2 design, 274*
 - Hybrid WAN, 271-275*
 - Internet traffic flows, 274*
 - Internet WAN, 271*
 - large branch design, 275, 278-279*
 - medium branch design, 275-277*
 - MPLS WAN, 271*
 - single MPLS carriers, 272*
 - single WAN carriers, 271*
 - small branch design, 275-276*
- enterprise edge design methodologies, 229
 - application requirements, 230*
 - bandwidth, 231-236*
 - key design principle, 230*
 - links, 232*
 - QoS and bandwidth optimization, 233-236*
 - reliability, 231*
 - response time, 230-231*
 - throughput, 231*
- enterprise MAN/WAN architectures, 265
 - ISP service, 267*
 - Private MPLS, 267*
 - Private WAN, 266*
 - SP MPLS/IP VPN, 267*
- enterprise teleworker design, 279-280
- Enterprise VPN
 - DMVPN, 257-258*
 - GETVPN, 258*
 - GRE, 257*
 - IPsec, 255-257*
 - Service Provider VPN versus, 255-263*
 - VTI, 258*

- enterprise WAN architectures, 55-56, 59
 - components of*, 268-270
 - growth, support for*, 265
 - HA*, 264
 - implementation costs*, 265
 - network segmentation support*, 265
 - operational complexity*, 265
 - operational expenses*, 265
 - video support*, 265
 - voice support*, 265
- Hybrid WAN, enterprise branch architectures, 271-275
- Internet connectivity, 238-240
- Internet WAN, enterprise branch architectures, 271
- leased line WAN, 252, 255
- load sharing/balancing, 263
- MPLS, enterprise branch architectures, 271-273
- multisite WAN
 - centralized call processing model*, 576
 - distributed call processing model*, 577
- packet-switched WAN, 252
- remote site connectivity, 254-255
- Service Provider VPN
 - Enterprise VPN versus*, 255-263
 - Layer 2 VPN service*, 260-262
 - Layer 3 VPN service*, 260-263, 273-275
 - Metro Ethernet*, 259-260
 - MPLS*, 261-263
 - VPLS*, 261-262
 - VPWS*, 260-261
- SLA, 218
- tariffs, 218, 229
- topologies
 - full-mesh topology*, 253
 - hub-and-spoke (star) topology*, 252
 - partial-mesh topology*, 253
 - point-to-point topology*, 254
- transport technologies
 - cable*, 222
 - CIR*, 228
 - comparison table*, 220-221
 - dark fiber*, 227
 - DSL*, 222
 - DWDM*, 228
 - Frame Relay*, 224-225, 228
 - ISDN*, 221
 - Metro Ethernet*, 225
 - MPLS*, 226-228
 - ordering/contracting*, 228-229
 - SONET/SDH*, 225-226
 - TDM*, 225
 - wireless strategies*, 223-224
- usage, 218
- virtual offices, 279-280
- VPN, 240-241
- WCS (Wireless Control System), 196
- web resources, 699
- WebVPN Services Module, 544
- weight (routing), BGP, 453
- WEP (Wired Equivalent Privacy), dynamic
 - WEP keys and WLAN, 174
- WFQ (Weighted Fair Queuing), 234
- window size (QoS), 236
- wireless bridges, 223
- wireless mesh
 - MAP, 196
 - RAP, 196
 - WCS, 196
 - WLAN, 195-196
 - WLC, 196
- Wireshark, network audits, 20
- WLAN (Wireless Local Area Networks), 223
 - AP, campus design, 196
 - authentication, 182-183
 - branch design, 200-201

campus design, 196

PoE, 197

QoS, 197-199

Cisco UWN

architecture of, 175-176

autonomous AP, 176

benefits of, 175

CAPWAP, 178-182

centralized WLAN architecture, 177

intracontroller roaming, 187

Layer 2 intercontroller roaming, 187

Layer 3 intercontroller roaming, 188

local MAC, 179, 200

LWAPP, 177-178

mobility groups, 189-190

split-MAC architectures, 179

WLAN authentication, 182-183

WLC, 183-186

controller redundancy design

N+1 WLC redundancy, 190-192

N+N WLC redundancy, 191-192

N+N+1 WLC redundancy, 191-192

EoIP tunnels, 194

layer 2 access method, 172

mobile wireless, 223

mobility groups, 189-190

outdoor wireless, 195-196

RF groups, 193-194

RF site surveys, 194

roaming

intracontroller roaming, 187

Layer 2 intercontroller roaming, 187

Layer 3 intercontroller roaming, 188

RRM, 192-193

security, 172

controlling server access, 174

design approach, 173

dynamic WEP keys, 174

LEAP, 174

port-based authentication, 173

unauthorized access, 173

SSID, 171

standards, 169

ISM frequencies, 170

summary of, 171

UNII frequencies, 170

wireless bridges, 223

wireless mesh, 195-196

WLC (WLAN Controllers), 183, 196

AP controller equipment scaling, 185-186

AP Manager interface, 185

controller redundancy design

N+1 redundancy, 190-192

N+N+1 redundancy, 191-192

N+N redundancy, 191-192

Dynamic interface, 185

LAP discovery of WLC via CAPWAP,
181-182

Management interface, 184-185

mobility groups, 189

RRM, 193

Service-Port interface, 184-185

Virtual interface, 185

WLAN, campus design, 197

WLC LAG, 184-186

**workstation-to-router redundancy
protocols**, 66

ARP, 60

Explicit Configuration protocol, 60

GLBP, 62

HSRP, 61

RDP, 60

RIP, 61

VRRP, 62

VSS, 47