



# Official Cert Guide

Learn, prepare, and practice for exam success



## CCDA 640-864

- Master **CCDA 640-864** exam topics
- Assess your knowledge with **chapter-opening quizzes**
- Review key concepts with **exam preparation tasks**
- Practice with **realistic exam questions** on the CD-ROM

[ciscopress.com](http://ciscopress.com)

**ANTHONY BRUNO, CCIE NO. 2738**  
**STEVE JORDAN, CCIE NO. 11293**

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

# CCDA 640-864

## Official Cert Guide

---

Anthony Bruno, CCIE No. 2738

Steve Jordan, CCIE No. 11293

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

## **CCDA 640-864 Official Cert Guide**

Anthony Bruno, CCIE No. 2738

Steve Jordan, CCIE No. 11293

Copyright © 2011 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.

Third Printing: September 2012

Library of Congress Cataloging-in-Publication data is on file.

ISBN-10: 1-58714-257-0

ISBN-13: 978-1-58714-257-4

### **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](mailto: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](mailto:corpsales@pearsontechgroup.com)

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

**International Sales** 1-317-581-3793 [international@pearsontechgroup.com](mailto:international@pearsontechgroup.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.

**Publisher:** Paul Boger

**Manager, Global Certification:** Erik Ullanderson

**Associate Publisher:** David Dusthimer

**Business Operation Manager, Cisco Press:** Anand Sundaram

**Executive Editor:** Brett Bartow

**Technical Editors:** David Morgan and Farai Tafa

**Managing Editor:** Sandra Schroeder

**Copy Editor:** Keith Cline

**Development Editor:** Andrew Cupp

**Book Designer:** Gary Adair

**Senior Project Editor:** Tonya Simpson

**Publishing Coordinator:** Vanessa Evans

**Cover Designer:** Sandra Schroeder

**Composition:** Mark Shirar

**Indexer:** Cheryl Lenser



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

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

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

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

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

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

## About the Authors

**Anthony Bruno**, CCIE No. 2738, is a senior principal consultant 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 network certifications include CCDP, CCVP, CCSP, Cisco Data Center Network Infrastructure Specialist, Cisco Security Solutions & Design Specialist, JNCIS-ER, Project+, ITILv3 Foundation, and CWNA. He has consulted for many enterprise and service provider customers in the design, implementation, and optimization of large-scale data and IP telephony 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.

**Steve Jordan**, CCIE No. 11293, is a senior consultant with Extropy with more than 15 years of experience in the internetworking field. Previously, he worked for General Datatech in Houston, Texas. His other certifications include VMware VCP4 and Cisco DC specializations in Network Infrastructure, Storage, and Unified Computing Design. He specializes in data center architecture involving network, storage, compute, and virtualization technologies. He has extensive experience with large-scale data center environments and has designed and implemented network solutions in the financial, energy, retail, manufacturing, and telecommunications industries.

Steve was also the coauthor for the previous edition of the *CCDA Exam Certification Guide, Third Edition*.

## About the Technical Reviewers

**David Morgan** is a senior technical consultant, technical trainer, and UC Practice Lead for General Datatech, a Cisco Gold Partner in Dallas, Texas. He has designed, deployed, and supported hundreds of communications systems, with enterprise implementations supporting as many as 120,000+ phones and 2000+ remote sites. He has more than 12 years of general networking experience. He also has experience supporting LAN, WAN, security, and voice technologies and Microsoft server technology, and IBM AS/400 systems. David lives in Arlington, Texas with his wife, Trisha, and two sons.

**Farai Tafa**, CCIE No. 14811, is a senior consultant with British Telecom with ten years of experience in the internetworking field. He holds CCIE certifications in the Routing and Switching and Service Provider tracks. His other certifications include the CCVP, JNCIA, JNCIS, and ITILv3 Foundation certifications. Prior to British Telecom, Farai had the privilege of working for industry powerhouses such as Google, Inc. and Cisco Systems, Inc. Farai has ten years of experience in the design, implementation, and support of enterprise and service provider routing and switching solutions, and Enterprise Cisco IP Telephony and Unified Wireless solutions.

## Dedications

This book is dedicated to my wife, Yvonne Bruno, Ph.D., and to our daughters, Joanne and Dianne. Thanks for all of your support during the development of this book. Joanne, hopefully this book will help me pay for your computer engineering classes at Texas A&M!

—Anthony Bruno

This book is dedicated to my wife of 17 years, Dorin, and my three sons, Blake, Lance, and Miles, for their support during the development of this book. For Blake, Lance, and Miles, we can now play many more games! I also want to dedicate this book to both of my grandmothers, Frances Cross and Anna C. Smith, who recently passed. I miss you both very much!

—Steve Jordan

## Acknowledgments

This book would not have been possible without the efforts of many dedicated people. Thanks to Andrew Cupp, development editor, for his guidance and special attention to detail. Thanks to Tonya Simpson, senior project editor, for her accuracy. 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, David Morgan and Farai Tafa. 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 Brett Bartow, executive editor, for his guidance and support during the book development. Thanks again to Andrew Cupp, development editor, for supporting my schedule delays and keeping me on track.

Special thanks goes to the technical reviewers of this book, David Morgan and Farai Tafa, 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 xxxi

### **Part I General Network Design 3**

Chapter 1 Network Design Methodology 5

Chapter 2 Network Structure Models 37

### **Part II LAN and WAN Design 77**

Chapter 3 Enterprise LAN Design 79

Chapter 4 Data Center Design 121

Chapter 5 Wireless LAN Design 153

Chapter 6 WAN Technologies 199

Chapter 7 WAN Design 227

### **Part III The Internet Protocol and Routing Protocols 263**

Chapter 8 Internet Protocol Version 4 265

Chapter 9 Internet Protocol Version 6 305

Chapter 10 Routing Protocol Characteristics, RIP, and EIGRP 345

Chapter 11 OSPF, BGP, Route Manipulation, and IP Multicast 387

### **Part IV Security, Convergence, Network Management 443**

Chapter 12 Managing Security 445

Chapter 13 Security Solutions 481

Chapter 14 Voice and Video Design 515

Chapter 15 Network Management Protocols 575

### **Part V Comprehensive Scenarios and Final Prep 597**

Chapter 16 Comprehensive Scenarios 599

Chapter 17 Final Preparation 613



## **Part VI    Appendixes    621**

Appendix A    Answers to the “Do I Know This Already?” Quizzes  
and Q&A Questions    623

Appendix B    CCDA Exam Updates: Version 1.0    657

Appendix C    OSI Model, TCP/IP Architecture, and Numeric Conversion    661

Glossary    677

Index    690

## **Elements Available on the CD**

Appendix D    Memory Tables

Appendix E    Memory Tables Answer Key

# Contents

Introduction xxxi

## **Part I      General Network Design    3**

### **Chapter 1    Network Design Methodology    5**

“Do I Know This Already?” Quiz	5
Foundation Topics	8
Cisco Architectures for the Enterprise	8
Borderless Networks Architecture	9
Collaboration Architecture	9
Data Center/Virtualization Architecture	10
Prepare, Plan, Design, Implement, Operate, and Optimize Phases	11
Prepare Phase	13
Plan Phase	14
Design Phase	14
Implement Phase	14
Operate Phase	14
Optimize Phase	14
Summary of PPDIOO Phases	14
Design Methodology Under PPDIOO	15
Identifying Customer Design Requirements	15
Characterizing the Existing Network	17
Steps in Gathering Information	17
Network Audit Tools	18
Network Analysis Tools	22
Network Checklist	22
Designing the Network Topology and Solutions	23
Top-Down Approach	23
Pilot and Prototype Tests	24
Design Document	25
References and Recommended Reading	26
Exam Preparation Tasks	27
Review All Key Topics	27
Complete Tables and Lists from Memory	27
Define Key Terms	27
Q&A	28

## **Chapter 2 Network Structure Models 37**

“Do I Know This Already?” Quiz	37
Foundation Topics	40
Hierarchical Network Models	40
Benefits of the Hierarchical Model	40
Hierarchical Network Design	41
<i>Core Layer</i>	41
<i>Distribution Layer</i>	42
<i>Access Layer</i>	43
Hierarchical Model Examples	45
Cisco Enterprise Architecture Model	47
Enterprise Campus Module	48
Enterprise Edge Area	50
<i>E-Commerce Module</i>	50
<i>Internet Connectivity Module</i>	51
<i>VPN/Remote Access</i>	52
<i>Enterprise WAN</i>	53
Service Provider Edge Module	54
Remote Modules	55
<i>Enterprise Branch Module</i>	56
<i>Enterprise Data Center Module</i>	56
<i>Enterprise Teleworker Module</i>	56
Borderless Network Services	58
High Availability Network Services	58
Workstation-to-Router Redundancy and LAN	
High Availability Protocols	59
<i>ARP</i>	59
<i>Explicit Configuration</i>	59
<i>RDP</i>	59
<i>RIP</i>	59
<i>HSRP</i>	60
<i>VRRP</i>	61
<i>GLBP</i>	61
Server Redundancy	61
Route Redundancy	62
<i>Load Balancing</i>	62
<i>Increasing Availability</i>	62
Link Media Redundancy	64

References and Recommended Reading 65

Exam Preparation Tasks 66

Review All Key Topics 66

Complete Tables and Lists from Memory 66

Define Key Terms 66

Q&A 66

## **Part II LAN and WAN Design 77**

### **Chapter 3 Enterprise LAN Design 79**

“Do I Know This Already?” Quiz 79

Foundation Topics 82

LAN Media 82

Ethernet Design Rules 83

*100-Mbps Fast Ethernet Design Rules 84*

Gigabit Ethernet Design Rules 86

*1000BASE-LX Long-Wavelength Gigabit Ethernet 86*

*1000BASE-SX Short-Wavelength Gigabit Ethernet 87*

*1000BASE-CX Gigabit Ethernet over Coaxial Cable 87*

*1000BASE-T Gigabit Ethernet over UTP 87*

10 Gigabit Ethernet Design Rules 88

*10GE Media Types 88*

EtherChannel 89

Comparison of Campus Media 89

LAN Hardware 89

Repeaters 90

Hubs 90

Bridges 91

Switches 91

Routers 92

Layer 3 Switches 93

Campus LAN Design and Best Practices 94

Best Practices for Hierarchical Layers 95

*Access Layer Best Practices 96*

*Distribution Layer Best Practices 96*

*Core Layer Best Practices 98*

Large-Building LANs 101

Enterprise Campus LANs 102

*Edge Distribution 103*

Medium-Size LANs	103
Small and Remote Site LANs	103
Server Farm Module	104
<i>Server Connectivity Options</i>	105
Enterprise Data Center Infrastructure	105
Campus LAN QoS Considerations	106
Multicast Traffic Considerations	108
<i>CGMP</i>	108
<i>IGMP Snooping</i>	109
References and Recommended Readings	109
Exam Preparation Tasks	110
Review All Key Topics	110
Complete Tables and Lists from Memory	110
Define Key Terms	110
Q&A	110

## **Chapter 4 Data Center Design 121**

“Do I Know This Already?” Quiz	121
Foundation Topics	124
Enterprise DC Architectures	124
Data Center 3.0 Components	125
Data Center 3.0 Topology Components	127
Challenges in the DC	127
Data Center Facility Aspects	128
Data Center Space	130
Data Center Power	131
Data Center Cooling	132
Data Center Heat	133
Data Center Cabling	133
Enterprise DC Infrastructure	135
Defining the DC Access Layer	136
Defining the DC Aggregation Layer	138
Defining the DC Core Layer	139
Virtualization Overview	141
Challenges	141
Defining Virtualization and Benefits	141
Types of Virtualization	142

Virtualization Technologies	143
VSS	143
VRF	143
vPC	143
Device Contexts	144
Server Virtualization	144
Network Virtualization Design Considerations	144
Access Control	145
Path Isolation	145
Services Edge	145
References and Recommended Readings	145
Exam Preparation Tasks	147
Review All Key Topics	147
Complete Tables and Lists from Memory	148
Define Key Terms	148
Q&A	148
<b>Chapter 5 Wireless LAN Design</b>	<b>153</b>
“Do I Know This Already?” Quiz	153
Foundation Topics	155
Wireless LAN Technologies	155
WLAN Standards	155
<i>ISM and UNII Frequencies</i>	156
<i>Summary of WLAN Standards</i>	157
Service Set Identifier	157
WLAN Layer 2 Access Method	157
WLAN Security	157
<i>Unauthorized Access</i>	158
<i>WLAN Security Design Approach</i>	158
<i>IEEE 802.1X-2001 Port-Based Authentication</i>	159
<i>Dynamic WEP Keys and LEAP</i>	159
<i>Controlling WLAN Access to Servers</i>	159
Cisco Unified Wireless Network	160
Cisco UWN Architecture	160
LWAPP	162
CAPWAP	163
<i>Cisco Unified Wireless Network Split-MAC Architecture</i>	163

<i>Local MAC</i>	164
<i>AP Modes</i>	164
<i>LWAPP Discovery of WLC</i>	166
WLAN Authentication	167
<i>Authentication Options</i>	168
WLAN Controller Components	169
<i>WLC Interface Types</i>	169
<i>AP Controller Equipment Scaling</i>	171
Roaming and Mobility Groups	173
<i>Intracontroller Roaming</i>	173
<i>Layer 2 Intercontroller Roaming</i>	173
<i>Layer 3 Intercontroller Roaming</i>	174
<i>Mobility Groups</i>	174
WLAN Design	176
Controller Redundancy Design: Deterministic vs. Dynamic	176
<i>N+1 WLC Redundancy</i>	176
<i>N+N WLC Redundancy</i>	177
<i>N+N+1 WLC Redundancy</i>	177
Radio Management and Radio Groups	178
<i>RF Groups</i>	179
RF Site Survey	179
Using EoIP Tunnels for Guest Services	181
Wireless Mesh for Outdoor Wireless	181
<i>Mesh Design Recommendations</i>	182
Campus Design Considerations	183
Branch Design Considerations	184
<i>Local MAC</i>	184
<i>REAP</i>	184
<i>Hybrid REAP</i>	184
<i>Branch Office Controller Options</i>	185
References and Recommended Readings	186
Exam Preparation Tasks	187
Review All Key Topics	187
Complete Tables and Lists from Memory	187
Define Key Terms	187
Q&A	188

## **Chapter 6    WAN Technologies    199**

“Do I Know This Already?” Quiz	199
Foundation Topics	202
WAN Overview	202
WAN Defined	202
WAN Connection Modules	203
WAN Transport Technologies	204
ISDN	205
<i>ISDN BRI Service</i>	205
<i>ISDN PRI Service</i>	205
Digital Subscriber Line	206
Cable	206
Wireless	207
Frame Relay	208
Time-Division Multiplexing	209
Metro Ethernet	209
SONET/SDH	209
Multiprotocol Label Switching	211
Dark Fiber	211
Dense Wavelength-Division Multiplexing	212
Ordering WAN Technology and Contracts	212
WAN Design Methodology	213
Response Time	214
Throughput	214
Reliability	215
Bandwidth Considerations	215
WAN Link Categories	216
Optimizing Bandwidth Using QoS	217
<i>Queuing, Traffic Shaping, and Policing</i>	217
<i>Classification</i>	218
<i>Congestion Management</i>	218
<i>Priority Queuing</i>	218
<i>Custom Queuing</i>	218
<i>Weighted Fair Queuing</i>	218
<i>Class-Based Weighted Fair Queuing</i>	218
<i>Low-Latency Queuing</i>	219
<i>Traffic Shaping and Policing</i>	219



	<i>Link Efficiency</i>	220
	<i>Window Size</i>	220
	References and Recommended Readings	220
	Exam Preparation Tasks	221
	Review All Key Topics	221
	Complete Tables and Lists from Memory	221
	Define Key Terms	221
	Q&A	222
<b>Chapter 7</b>	<b>WAN Design</b>	<b>227</b>
	“Do I Know This Already?” Quiz	227
	Foundation Topics	230
	Traditional WAN Technologies	230
	Hub-and-Spoke Topology	230
	Full-Mesh Topology	231
	Partial-Mesh Topology	231
	Remote-Access Network Design	232
	VPN Network Design	232
	Enterprise VPN vs. Service Provider VPN	233
	Enterprise VPNs	234
	Service Provider Offerings	234
	Enterprise Managed VPN: IPsec	234
	<i>IPsec Direct Encapsulation</i>	234
	<i>Cisco Easy VPN</i>	235
	<i>Generic Routing Encapsulation</i>	236
	<i>IPsec DMVPN</i>	236
	<i>IPsec Virtual Tunnel Interface Design</i>	237
	<i>Layer 2 Tunneling Protocol Version 3</i>	237
	Service Provider Managed Offerings	237
	<i>Metro Ethernet</i>	237
	<i>Virtual Private LAN Services</i>	238
	MPLS	238
	MPLS Layer 3 Design Overview	239
	VPN Benefits	239
	WAN Backup Design	240
	Load-Balancing Guidelines	240
	WAN Backup over the Internet	241

Enterprise WAN Architecture	241
Cisco Enterprise MAN/WAN	243
Enterprise WAN/MAN Architecture Comparison	243
Enterprise WAN Components	245
Comparing Hardware and Software	247
Enterprise Branch Architecture	248
Branch Design	248
Enterprise Branch Profiles	248
<i>ISR G2 New Features</i>	249
<i>Small Branch Design</i>	250
<i>Medium Branch Design</i>	250
<i>Large Branch Design</i>	252
Enterprise Teleworker Design	254
ISRs for Teleworkers	254
References and Recommended Readings	255
Exam Preparation Tasks	256
Review All Key Topics	256
Complete Tables and Lists from Memory	256
Define Key Terms	257
Q&A	257

### **Part III      The Internet Protocol and Routing Protocols    263**

#### **Chapter 8      Internet Protocol Version 4    265**

“Do I Know This Already?” Quiz	265
Foundation Topics	268
IPv4 Header	268
ToS	271
IPv4 Fragmentation	274
IPv4 Addressing	275
IPv4 Address Classes	276
<i>Class A Addresses</i>	277
<i>Class B Addresses</i>	277
<i>Class C Addresses</i>	277
<i>Class D Addresses</i>	277
<i>Class E Addresses</i>	278
IPv4 Address Types	278
IPv4 Private Addresses	279

NAT	279
Private and Public IP Address and NAT Guidelines	280
IPv4 Address Subnets	282
Mask Nomenclature	283
IP Address Subnet Design	283
Determining the Network Portion of an IP Address	285
Variable-Length Subnet Masks	286
<i>VLSM Address Assignment: Example 1</i>	286
<i>Loopback Addresses</i>	288
<i>IP Telephony Networks</i>	288
<i>VLSM Address Assignment: Example 2</i>	289
Address Assignment and Name Resolution	290
Recommended Practices of IP Address Assignment	290
BOOTP	291
DHCP	291
DNS	292
ARP	295
References and Recommended Readings	296
Exam Preparation Tasks	297
Review All Key Topics	297
Complete Tables and Lists from Memory	297
Define Key Terms	297
Q&A	298

## **Chapter 9 Internet Protocol Version 6 305**

“Do I Know This Already?” Quiz	305
Foundation Topics	308
Introduction to IPv6	308
IPv6 Header	309
IPv6 Address Representation	311
IPv4-Compatible IPv6 Addresses	312
IPv6 Prefix Representation	312
IPv6 Address Scope Types and Address Allocations	313
IPv6 Address Allocations	313
IPv6 Unicast Address	314
<i>Global Unicast Addresses</i>	314
<i>Link-Local Addresses</i>	315
<i>Unique Local IPv6 Address</i>	315

<i>Global Aggregatable IPv6 Address</i>	316
<i>IPv4-Compatible IPv6 Address</i>	316
IPv6 Anycast Addresses	316
IPv6 Multicast Addresses	317
IPv6 Mechanisms	320
ICMPv6	320
IPv6 Neighbor Discovery Protocol	320
IPv6 Name Resolution	321
Path MTU Discovery	322
IPv6 Address-Assignment Strategies	322
<i>Link-Local Address (Stateless Autoconfiguration)</i>	322
<i>Autoconfiguration of Globally Unique IP address</i>	323
DHCPv6	324
IPv6 Security	324
IPv6 Routing Protocols	325
RIPng	325
EIGRP for IPv6	325
OSPFv3	325
IS-IS for IPv6	325
BGP4 Multiprotocol Extensions (MP-BGP) for IPv6	326
IPv4 to IPv6 Transition Mechanisms and Deployment Models	326
Dual-Stack Mechanism	326
IPv6 over IPv4 Tunnels	326
Protocol Translation Mechanisms	328
IPv6 Deployment Models	329
<i>Dual-Stack Model</i>	329
<i>Hybrid Model</i>	330
<i>Service Block Model</i>	330
<i>IPv6 Deployment Model Comparison</i>	332
IPv6 Comparison with IPv4	333
References and Recommended Readings	334
Exam Preparation Tasks	336
Review All Key Topics	336
Complete Tables and Lists from Memory	337
Define Key Terms	337
Q&A	337

**Chapter 10 Routing Protocol Characteristics, RIP, and EIGRP 345**

“Do I Know This Already?” Quiz	345
Foundation Topics	348
Routing Protocol Characteristics	348
Static Versus Dynamic Route Assignment	348
Interior Versus Exterior Routing Protocols	350
Distance-Vector Routing Protocols	351
<i>EIGRP</i>	351
Link-State Routing Protocols	352
Distance-Vector Routing Protocols Versus Link-State Protocols	352
Hierarchical Versus Flat Routing Protocols	353
Classless Versus Classful Routing Protocols	353
IPv4 Versus IPv6 Routing Protocols	354
Administrative Distance	355
Routing Protocol Metrics and Loop Prevention	356
Hop Count	356
Bandwidth	357
Cost	358
Load	358
Delay	359
Reliability	359
Maximum Transmission Unit	360
Routing Loop-Prevention Schemes	360
<i>Split Horizon</i>	360
<i>Poison Reverse</i>	361
<i>Counting to Infinity</i>	361
Triggered Updates	361
Summarization	361
RIPv2 and RIPv6	362
Authentication	362
<i>MD5 Authentication</i>	362
RIPv2 Routing Database	362
RIPv2 Message Format	363
RIPv2 Timers	364
RIPv2 Design	364
RIPv2 Summary	364
RIPv6	365

<i>RIPng Timers</i>	365
<i>Authentication</i>	365
<i>RIPng Message Format</i>	365
<i>RIPng Design</i>	366
<i>RIPng Summary</i>	366
EIGRP	367
EIGRP Components	367
<i>Protocol-Dependent Modules</i>	368
<i>Neighbor Discovery and Recovery</i>	368
RTP	368
DUAL	368
EIGRP Timers	369
EIGRP Metrics	370
EIGRP Packet Types	371
EIGRP Design	372
EIGRP for IPv4 Summary	373
EIGRP for IPv6 (EIGRPv6) Networks	373
<i>EIGRP for IPv6 Design</i>	374
<i>EIGRP for IPv6 Summary</i>	374
References and Recommended Readings	375
Exam Preparation Tasks	377
Review All Key Topics	377
Complete Tables and Lists from Memory	377
Define Key Terms	377
Q&A	377
<b>Chapter 11 OSPF, BGP, Route Manipulation, and IP Multicast</b>	<b>387</b>
“Do I Know This Already?” Quiz	387
Foundation Topics	391
OSPFv2	391
OSPFv2 Metric	391
OSPFv2 Adjacencies and Hello Timers	392
OSPFv2 Areas	393
OSPF Router Types	394
OSPF DRs	395
LSA Types	396
<i>Autonomous System External Path Types</i>	397

OSPF Stub Area Types	397
<i>Stub Areas</i>	397
<i>Totally Stubby Areas</i>	398
NSSAs	398
Virtual Links	399
OSPFv2 Router Authentication	399
OSPFv2 Summary	399
OSPFv3	400
OSPFv3 Changes from OSPFv2	400
OSPFv3 Areas and Router Types	401
OSPFv3 LSAs	401
OSPFv3 Summary	404
BGP	404
BGP Neighbors	405
<i>eBGP</i>	406
<i>iBGP</i>	406
Route Reflectors	407
Confederations	409
BGP Administrative Distance	409
BGP Attributes, Weight, and the BGP Decision Process	409
<i>BGP Path Attributes</i>	410
<i>Next-Hop Attribute</i>	411
<i>Local Preference Attribute</i>	411
<i>Origin Attribute</i>	411
<i>Autonomous System Path Attribute</i>	412
<i>MED Attribute</i>	412
<i>Community Attribute</i>	413
<i>Atomic Aggregate and Aggregator Attributes</i>	413
<i>Weight</i>	414
<i>BGP Decision Process</i>	414
BGP Summary	415
Route Manipulation	416
PBR	416
Route Summarization	416
Route Redistribution	419
<i>Default Metric</i>	420
<i>OSPF Redistribution</i>	421

Route Filtering	421
Routing Protocols on the Hierarchical Network Infrastructure	422
IP Multicast Review	423
Multicast Addresses	423
Layer 3-to-Layer 2 Mapping	424
IGMP	425
<i>IGMPv1</i>	425
<i>IGMPv2</i>	425
<i>IGMPv3</i>	426
CGMP	426
<i>IGMP Snooping</i>	427
Sparse Versus Dense Multicast	427
Multicast Source and Shared Trees	428
PIM	428
PIM-SM	429
PIM DR	429
Auto-RP	429
PIMv2 Bootstrap Router	430
DVMRP	430
IPv6 Multicast Addresses	430
References and Recommended Readings	431
Exam Preparation Tasks	433
Review All Key Topics	433
Complete Tables and Lists from Memory	433
Define Key Terms	433
Q&A	434
<b>Part IV</b>	<b>Security, Convergence, Network Management 443</b>
<b>Chapter 12</b>	<b>Managing Security 445</b>
“Do I Know This Already?” Quiz	445
Foundation Topics	448
Network Security Overview	448
Security Legislation	448
Security Threats	450
<i>Reconnaissance and Port Scanning</i>	450
<i>Vulnerability Scanners</i>	451
<i>Unauthorized Access</i>	452



Security Risks	453
<i>Targets</i>	453
<i>Loss of Availability</i>	454
<i>Integrity Violations and Confidentiality Breaches</i>	455
Security Policy and Process	456
Security Policy Defined	457
Basic Approach of a Security Policy	458
Purpose of Security Policies	458
Security Policy Components	459
Risk Assessment	459
Risk Index	460
Continuous Security	461
Integrating Security Mechanisms into Network Design	462
Trust and Identity Management	462
Trust	463
<i>Domains of Trust</i>	463
Identity	464
<i>Passwords</i>	464
<i>Tokens</i>	464
<i>Certificates</i>	465
Access Control	466
Secure Connectivity	466
Encryption Fundamentals	466
Encryption Keys	467
VPN Protocols	467
Transmission Confidentiality	469
Data Integrity	469
Threat Defense	470
Physical Security	470
Infrastructure Protection	471
Security Management Solutions	472
References and Recommended Readings	473
Exam Preparation Tasks	474
Review All Key Topics	474
Complete Tables and Lists from Memory	474
Define Key Terms	475
Q&A	475

## **Chapter 13 Security Solutions 481**

“Do I Know This Already?” Quiz	481
Foundation Topics	484
Cisco SAFE Architecture	484
Network Security Platforms	485
Cisco Security Control Framework	486
Trust and Identity Technologies	486
Firewall ACLs	487
Cisco NAC Appliance	488
Cisco Identity-Based Network Services	489
Identity and Access Control Deployments	489
Detecting and Mitigating Threats	490
Threat Detection and Mitigation Technologies	491
Threat-Detection and Threat-Mitigation Solutions	492
Cisco IronPort ESA	493
Cisco IronPort WSA	494
Security Management Applications	495
Security Platform Solutions	495
Security Management Network	496
Integrating Security into Network Devices	497
IOS Security	498
ISR G2 Security Hardware Options	499
Cisco Security Appliances	499
Intrusion Prevention	500
Catalyst 6500 Service Modules	500
Endpoint Security	502
Securing the Enterprise	502
Implementing Security in the Campus	502
Implementing Security in the Data Center	503
Implementing Security in the Enterprise Edge and WAN	504
References and Recommended Readings	507
Exam Preparation Tasks	508
Review All Key Topics	508
Complete Tables and Lists from Memory	508
Define Key Terms	509
Q&A	509

**Chapter 14 Voice and Video Design 515**

“Do I Know This Already?” Quiz	515
Foundation Topics	518
Traditional Voice Architectures	518
PBX and PSTN Switches	518
Local Loop and Trunks	519
Ports	520
Major Analog and Digital Signaling Types	521
<i>Loop-Start Signaling</i>	522
<i>Ground-Start Signaling</i>	522
<i>E&amp;M Signaling</i>	523
<i>CAS and CCS Signaling</i>	524
PSTN Numbering Plan	526
Other PSTN Services	527
<i>Centrex Services</i>	528
<i>Voice Mail</i>	528
<i>Database Services</i>	528
<i>IVR</i>	528
<i>ACD</i>	528
Voice Engineering Terminology	528
<i>Grade of Service</i>	528
<i>Erlangs</i>	528
<i>Centum Call Second</i>	529
<i>Busy Hour</i>	529
<i>Busy-Hour Traffic</i>	529
<i>Blocking Probability</i>	530
<i>Call Detail Records</i>	530
Converged Multiservice Networks	530
VoIP	531
IPT Components	532
<i>Design Goals of IP Telephony</i>	534
IPT Deployment Models	535
<i>Single-Site Deployment</i>	535
<i>Multisite WAN with Centralized Call Processing Model</i>	536
<i>Multisite WAN with Distributed Call Processing Model</i>	536
<i>Unified CallManager Express Deployments</i>	537
Video Deployment Considerations	537
Codecs	539

<i>Analog-to-Digital Signal Conversion</i>	540
<i>Codec Standards</i>	540
VoIP Control and Transport Protocols	541
<i>DHCP, DNS, and TFTP</i>	542
<i>SCCP</i>	542
<i>RTP and RTCP</i>	543
<i>MGCP</i>	544
<i>H.323</i>	544
<i>H.264</i>	547
<i>SIP</i>	548
IPT Design	549
Bandwidth	550
VAD	550
Calculating Voice Bandwidth	551
Delay Components in VoIP Networks	552
Packet Loss	555
Echo Cancellation	555
QoS and Bandwidth Mechanisms for VoIP and Video Networks	555
<i>cRTP</i>	556
<i>IEEE 802.1P</i>	556
<i>Resource Reservation Protocol</i>	557
<i>LFI</i>	557
<i>LLQ</i>	557
<i>Auto QoS</i>	559
IPT Design Recommendations	560
<i>Service Class Recommendations</i>	561
References and Recommended Readings	562
Exam Preparation Tasks	564
Review All Key Topics	564
Complete Tables and Lists from Memory	564
Define Key Terms	565
Q&A	565
<b>Chapter 15 Network Management Protocols</b>	<b>575</b>
“Do I Know This Already?” Quiz	575
Foundation Topics	578
Simple Network Management Protocol	579
SNMP Components	579
MIB	580

	SNMP Message Versions	581
	<i>SNMPv1</i>	581
	<i>SNMPv2</i>	582
	<i>SNMPv3</i>	582
	Other Network Management Technologies	583
	RMON	583
	<i>RMON2</i>	584
	NetFlow	585
	<i>NetFlow Compared to RMON and SNMP</i>	586
	CDP	587
	Syslog	588
	References and Recommended Reading	589
	Exam Preparation Tasks	591
	Review All Key Topics	591
	Complete Tables and Lists from Memory	591
	Define Key Terms	591
	Q&A	592
<b>Part V</b>	<b>Comprehensive Scenarios and Final Prep</b>	<b>597</b>
<b>Chapter 16</b>	<b>Comprehensive Scenarios</b>	<b>599</b>
	Scenario One: Pearland Hospital	599
	Scenario One Questions	600
	Scenario One Answers	601
	Scenario Two: Big Oil and Gas	604
	Scenario Two Questions	604
	Scenario Two Answers	605
	Scenario Three: Beauty Things Store	606
	Scenario Three Questions	607
	Scenario Three Answers	608
	Scenario Four: Falcon Communications	608
	Scenario Four Questions	609
	Scenario Four Answers	609
<b>Chapter 17</b>	<b>Final Preparation</b>	<b>613</b>
	Tools for Final Preparation	613
	Pearson Cert Practice Test Engine and Questions on the CD	613
	Install the Software from the CD	614
	Activate and Download the Practice Exam	614

	Activating Other Exams	615
	Premium Edition	615
	The Cisco Learning Network	615
	Memory Tables	615
	Chapter-Ending Review Tools	616
	Suggested Plan for Final Review/Study	616
	Subnetting Practice	616
	Using the Exam Engine	617
	Summary	618
<b>Part VI</b>	<b>Appendixes</b>	<b>621</b>
<b>Appendix A</b>	<b>Answers to the “Do I Know This Already?” Quizzes and Q&amp;A Questions</b>	<b>623</b>
<b>Appendix B</b>	<b>CCDA Exam Updates: Version 1.0</b>	<b>657</b>
<b>Appendix C</b>	<b>OSI Model, TCP/IP Architecture, and Numeric Conversion</b>	<b>661</b>
	<b>Glossary</b>	<b>677</b>
	<b>Index</b>	<b>690</b>
 <b>Elements Available on the CD</b>		
<b>Appendix D</b>	<b>Memory Tables</b>	
<b>Appendix E</b>	<b>Memory Tables Answer Key</b>	

## 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.

## 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 and engineers 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, IP telephony, and wireless LANs.

Although it is not required, Cisco suggests taking the DESGN 2.1 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 [www.cisco.com/web/learning/le3/learning\\_career\\_certifications\\_and\\_learning\\_paths\\_home.html](http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html).

Our goal with this book is to help you pass the 640-864 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 640-864 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 such as borderless networks, data centers design, and updates on 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 #640-864. It is a computer-based test that has 65 questions and a 90-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 course and exam updates at [www.cisco.com/web/learning/le3/learning\\_career\\_certifications\\_and\\_learning\\_paths\\_home.html](http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html).

You can take the exam at Pearson VUE testing centers. You can register with VUE at [www.vue.com/cisco/](http://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 642 or Cisco Specialist exam.



## 640-864 CCDA Exam Topics

Table I-1 lists the topics of the 640-864 CCDA exam and indicates the part in the book where they are covered.

**Table I-1** 640-864 CCDA Exam Topics

<b>Exam Topic</b>	<b>Part</b>
<b>Describe the Methodology Used to Design a Network</b>	
Describe developing business trends	I
Identify network requirements to support the organization	I
Describe the tools/process to characterize an existing network	I
Describe the top down approach to network design	I
Describe network management protocols and features	IV
<b>Describe Network Structure and Modularity</b>	
Describe the network hierarchy	I
Describe the modular approach in network design	I
Describe network architecture for the enterprise	II
<b>Design Basic Enterprise Campus Networks</b>	
Describe Campus Design considerations	II
Design the enterprise campus network	II
Design the enterprise data center	II
Describe enterprise network virtualization tools	II
<b>Design Enterprise Edge and Remote Network Modules</b>	
Describe the enterprise edge, branch, and teleworker design characteristics	II
Describe physical and logical WAN connectivity	II
Design the branch office WAN solutions	II
Describe access network solutions for a remote worker	II
Design the WAN to support selected redundancy methodologies	II
Identify design considerations for a remote data center	II
<b>Design IP Addressing and Routing Protocols</b>	
Describe IPv4 addressing	III
Describe IPv6 addressing	III
Identify Routing Protocol Considerations in an Enterprise Network	III
Design a routing protocol deployment	III

<b>Design Network Services</b>	
Describe the security life cycle	IV
Identify Cisco technologies to mitigate security vulnerabilities	IV
Select appropriate Cisco security solutions and deployment placement	IV
Describe high-level voice and video architectures	IV
Identify the design considerations for voice/video services	IV
Describe Cisco Unified Wireless network architectures and features	II
Design wireless network using controllers	II

## About the **CCDA 640-864 Official Cert Guide**

This book maps to the topic areas of the 640-864 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 on 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. So, 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 CD

## 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:** These are the core sections of each chapter. They explain 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.
- **CD-based practice exam:** The companion CD contains the Pearson Cert Practice Test engine that allows you to take practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.

## 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 Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) methodology, and the process of completing a network design.
- **Chapter 2: Network Structure 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, technology trends, data center challenges, and virtualization technologies.

- **Chapter 5: Wireless LAN Design** covers technologies and design options used for wireless LANs.
- **Chapter 6: WAN Technologies** examines technologies, design methodologies, 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** covers the header, addressing, subnet design, and protocols used by IPv4.
- **Chapter 9: Internet Protocol Version 6** covers the header, addressing, design, and protocols used by IPv6.
- **Chapter 10: Routing Protocol Characteristics, RIP, and EIGRP** covers routing protocol characteristics, metrics, RIPv2, and Enhanced Interior Gateway Routing Protocol (EIGRP).
- **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, 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), 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 CD material to study.

### Part VI: Appendixes

- **Appendix A: Answers to "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 CD-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 exams. This appendix is available in PDF format on the CD; it is not in the printed book.
- **Appendix E: Memory Tables Answer Key** (a CD-only appendix) contains the answer key for the memory tables in Appendix D. This appendix is available in PDF format on the CD; it is not in the printed book.

*This page intentionally left blank*

**CCDA exam topics covered in this part:**

- Describe developing business trends
- Identify network requirements to support the organization
- Describe the tools/process to characterize an existing network
- Describe the top-down approach to network design
- Describe the network hierarchy
- Describe the modular approach in network design
- Describe network architecture for the enterprise



---

This chapter covers the following subjects:

- Enterprise DC Architectures
- Challenges in the DC
- Enterprise DC Infrastructure
- Virtualization Overview
- Virtualization Technologies
- Network Virtualization Design Considerations



# Data Center Design

This chapter covers enterprise data center design fundamentals, technology trends, and challenges facing the data center. General data center architecture, components, and design considerations are examined, but detailed data center design is not covered.

This chapter also provides an overview of virtualization, discusses the various virtualization technologies and network virtualization design considerations.

The CCDA candidate can expect plenty of questions related to data center fundamentals, challenges, architecture, and virtualization.

## “Do I Know This Already?” Quiz

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

The ten-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 4-1 outlines the major topics discussed in this chapter and the “Do I Know This Already?” quiz questions that correspond to those topics.

**Table 4-1** *Do I Know This Already?” Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Enterprise DC Overview	1, 2
Challenges in the DC	3, 4
Enterprise DC Infrastructure	5, 6
Virtualization Overview	7
Virtualization Technologies	8, 9
Network Virtualization Design Considerations	10

1. What are two methods for implementing unified fabric in the data center over 10Gigabit Ethernet?
  - a. VSS
  - b. FCoE
  - c. iSCSI
  - d. vPC
2. What best describes the characteristics of Data Center 3.0 architecture?
  - a. Mainframes
  - b. Consolidation/virtualization/automation
  - c. Distributed client/server computing
  - d. Decentralized computing
3. Which of the following data center facility aspects best corresponds with architectural and mechanical specifications?
  - a. Space, load, and power capacity
  - b. PCI, SOX, and HIPPA
  - c. Operating temperature and humidity
  - d. Site access, fire suppression, and security alarms
4. Which of the following uses the highest percentage of power within the overall data center power budget?
  - a. Lighting
  - b. Servers and storage
  - c. Network devices
  - d. Data center cooling
5. Which data center architecture layer provides Layer 2/Layer 3 physical port density for servers in the data center?
  - a. Data center core
  - b. Data center aggregation
  - c. Data center access
  - d. Data center distribution

6. Layer 4 security and application services including server load balancing, Secure Sockets Layer (SSL) offloading, firewalling, and intrusion prevention system (IPS) services are provided by the data center \_\_\_\_\_ layer?
- a. Access
  - b. Routed
  - c. Core
  - d. Aggregation
7. Virtualization technologies allow a \_\_\_\_\_ device to share its resources by acting as multiple versions of itself?
- a. Software
  - b. Virtual
  - c. Logical
  - d. Physical
8. Which of the following are examples of logical isolation techniques in which network segments share the same physical infrastructure? (Select all that apply.)
- a. VRF
  - b. VLAN
  - c. VSAN
  - d. VSS
9. Which of the following are examples of technologies that employ device virtualization or the use of contexts? (Select all that apply.)
- a. VRF
  - b. ASA
  - c. VLAN
  - d. ACE
10. What involves the creation of independent logical network paths over a shared network infrastructure?
- a. Access control
  - b. Services edge
  - c. Path isolation
  - d. Device context

---

## Foundation Topics

---

This chapter covers general enterprise data center considerations that you need to master for the CCDA exam. It starts with a discussion of the enterprise data center architecture and how we have evolved from Data Center 1.0 to Data Center 3.0. The section “Data Center 3.0 Components” covers the virtualization technologies and services that unify network, storage, compute, and virtualization platforms. The section “Data Center 3.0 Topology Components” shows how the virtualization technologies integrate with unified computing and the unified fabric.

The “Challenges in the Data Center” section describes the common server deployment challenges present in the data center. Major facility aspect issues involving rack space, power, cooling, and management are covered. Data center cabling is examined along with the data center cable considerations critical to the proper cable plant management.

Following that, the “Enterprise Data Center Infrastructure” section explores the Cisco multilayer architecture that is used for building out enterprise data centers to support blades servers, 1RU (rack unit) servers, and mainframes. Design aspects of the multilayer architecture involving data center access layer, aggregation layer, and core layer design considerations are also covered.

The chapter wraps up with several sections on virtualization. An overview of virtualization is covered along with key drivers that are pushing the adoption of virtualization in the data center. The section “Virtualization Technologies” compares the two main types of virtualization and provides several examples. Then the section “Network Virtualization Design Considerations” covers access control, path isolation, and services edge.

## Enterprise DC Architectures

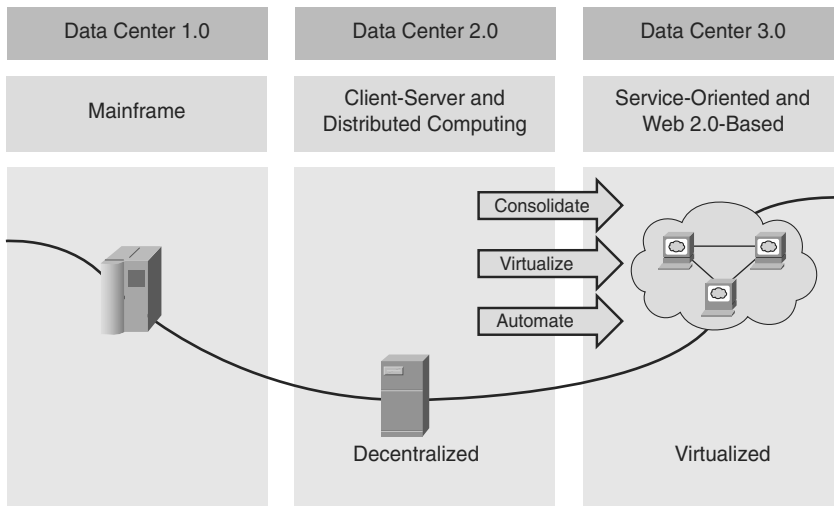
Over the past two decades, we have seen an evolution of data center “architectures”. With Data Center 1.0, data centers were centralized, using mainframes to process and store data. The users of Data Center 1.0 used terminals to access and perform their work on the mainframes. Mainframes are still prevalent in many data centers because of the overall benefits in terms of availability, resiliency, and service level agreements (SLA).

Figure 4-1 illustrates the evolution of data center architectures from Data Center 1.0 to Data Center 3.0.

Data Center 2.0 brought client/server and distributed computing into the mainstream data center. Business applications were installed on servers and were accessed by users with client software on their PCs. Application services were distributed because of high cost of WAN links and application performance. Also, the costs of mainframes were too costly to be used as an alternative for client/server computing.

Currently, we are moving away from Data Center 2.0 and toward Data Center 3.0, where consolidation and virtualization are the key components. The cost of communication equipment is lowering, and there is an increase in computing capacities, which is driving consolidation. Data Center 3.0 centralizes the computing infrastructure and is more cost effective when compared to the distributed approach. The newer architecture takes

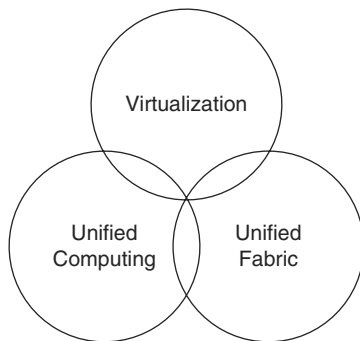
advantage of virtualization, which results in a higher utilization of computing and network resources. In addition, the newer Data Center 3.0 architecture increases the overall return on investment (ROI) and lowers the total cost of ownership (TCO).



**Figure 4-1** Cisco Data Center Architecture Evolution

### Data Center 3.0 Components

Figure 4-2 highlights the Cisco Data Center 3.0 components.



**Figure 4-2** Cisco Data Center 3.0 Architecture Framework

The architectural components of Data Center 3.0 include virtualization technologies and services that unify network, storage, compute, and virtualization platforms. These technologies and network services enable incredible flexibility, visibility, and policy

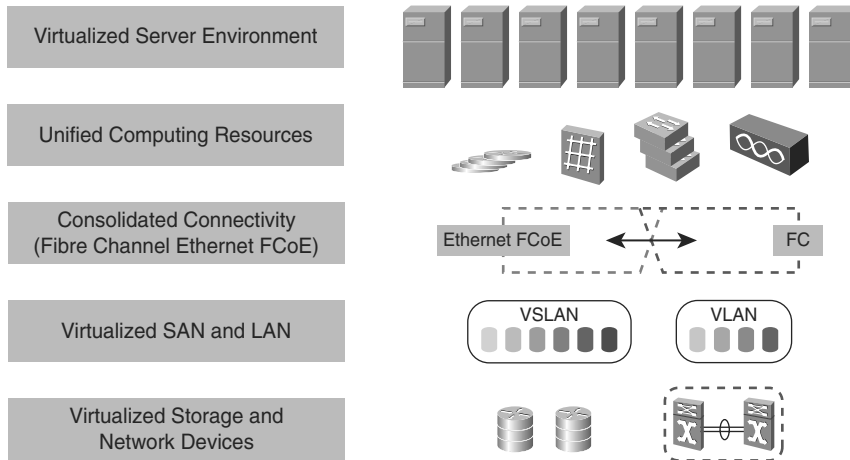
enforcement, which are critical for virtualized data centers. Here are the three main components of Cisco Data Center 3.0 architecture:



- **Virtualization**
  - Virtual local-area network (VLAN), virtual storage-area network (VSAN), and virtual device contexts (VDC) help to segment the LAN, SAN, and network devices instances.
  - Cisco Nexus 1000V virtual switch for VMware ESX and ESXi help to deliver visibility and policy control for virtual machines (VM).
  - Flexible networking options with support for all server form factors and vendors, including support for blade servers from Cisco, Dell, IBM, and HP with integrated Ethernet and Fibre Channel switches.
- **Unified fabric**
  - Fibre Channel over Ethernet (FCoE) and Internet Small Computer Systems Interface (iSCSI) are two methods for implementing unified fabric in the data center over 10 Gigabit Ethernet networks.
  - FCoE is supported on VMware ESX/ESXi vSphere 4.0 and later.
  - The Cisco Catalyst, Cisco Nexus, and Cisco MDS family of switches all support iSCSI. The Cisco Nexus 5000 support unified fabric lossless operation, which improves the performance of iSCSI traffic using 10 Gigabit Ethernet.
  - The Cisco Nexus family of switches was designed to support unified fabric. Currently, the Cisco Nexus 5000 and the Nexus 4000 supports data center bridging (DCB) and FCoE. However, there are future plans for the Cisco Nexus 7000 series and the Cisco MDS family of switches to support FCoE, as well.
  - Converged network adapters (CNA) run at 10GE and support FCoE. CNAs are available from both Emulex and QLogic. Additionally, a software stack is available for certain 10GE network interfaces from Intel.
- **Unified computing**
  - Cisco Unified Computing System (UCS) is an innovative next-generation data center platform that converges computing, network, storage, and virtualization together into one system.
  - Integrates lossless 10GE unified network fabric with x86 architecture-based servers.
  - Allows for Cisco Virtual Interface Card to virtualize your network interfaces on your server.
  - Offers Cisco VN-Link virtualization.
  - Supports Extended Memory Technology patented by Cisco.
  - Increases productivity with just-in-time provisioning using service profiles.

## Data Center 3.0 Topology Components

Figure 4-3 shows the Cisco Data Center 3.0 topology.



**Figure 4-3** *Cisco Data Center 3.0 Topology*

At the top layer, we have virtual machines which are software entities that have hardware level abstraction capable of running a guest OS on top of a resource scheduler also known as a hypervisor.

**Key Topic**

Within the unified computing resources, the service profile defines the identity of the server. The identity contains many items such as memory, CPU, network cards, storage information, and boot image.

10 Gigabit Ethernet, FCoE, and Fibre Channel technologies provide the unified fabric and is supported on the Cisco Nexus 5000. FCoE is one of the key technologies that allow native Fibre Channel frames to be used on 10G Ethernet networks.

Virtualization technologies such as VLANs and VSANs provide for virtualized LAN and SAN connectivity by logically segmenting multiple LANs and SANs on the same physical equipment. Each VLAN and VSAN operates independently from one another.

At the lowest layer, we have virtualized hardware where storage devices can be virtualized into storage pools and network devices are virtualized using virtual device contexts (VDC).

## Challenges in the DC

In the data center, server deployments are of great concern along with facilities and network equipment. Here are some of the challenges that must be dealt with when deploying servers:

- Power required
- Physical rack space usage

**Key Topic**

- Limits to scale
- Management (resources, firmware)
- Server security
- Virtualization support
- Management effort required

Server growth is consistently rising which is requiring more power, which is driving the need for energy efficiency for most data center server deployments. Although rack servers are low cost and provide high performance, unfortunately they take up space and consume a lot of energy to operate. Because both rack space and power cost money, efficiency gains need to be considered in these areas.

Blade servers provide similar computing power when compared to rack mount servers, but require less space, power, and cabling. The chassis in most blade servers allows for shared power, Ethernet LAN, and Fibre Channel SAN connections, which reduce the number of cables needed.

With both rack-mounted servers and blade servers, server virtualization software provides for better utilization of hardware resources, which requires less physical hardware to deploy servers, which in turn increases efficiency. Server virtualization also enables server scalability because more rack and cabinet space is available to deploy new ESX hosts running additional virtual machines.

Server management is a key element for deploying servers, and there are solutions available from OEMs such as Integrated Lights Out (ILO) and VMware Infrastructure Client. These products ease the management of larger server deployments and provide for secure remote management capabilities.

## Data Center Facility Aspects

Multiple facility considerations go into the design and planning for a new data center build out.

During the planning sessions, data center architectural and mechanical specifications help define the following:

- How much space will be available
- How much load the floor can support
- The power and cooling capacity that will be available
- The cabling plant that will be needed and how to manage it

The facility also needs to meet certain environmental conditions, and the data center equipment selections process dictates the operating temperatures and humidity levels that need to be maintained in the data center.



Another important consideration is physical security. Because the data center usually stores data that needs to be secured from third parties, access to the site needs to be well controlled. In addition, fire suppression and alarm systems should be in place to protect equipment and data from natural disasters and theft.

Because the data center facilities are limited in capacity, they need to be designed properly to allow for the best use of employee space for today and into the future.

Most companies must now adhere to regulatory compliance, including environmental requirements, and provide disaster recovery in some form to enable business continuity. Data centers need to provide an infrastructure that can recover network communications, data, and applications and provide high availability.

To build a reliable data center that maximizes the investment, the design needs to be considered early in the building development process. It is important to include team members in several area of expertise, including telecommunications, power, architectural, and heating, ventilating, and air conditioning (HVAC). Each team member needs to work together to ensure that the designed systems interoperate most effectively. The design of the data center needs to incorporate current requirements and support future growth.

Careful planning and close attention to design guidelines is crucial for the data center build out to be successful. Missing critical aspects of the design can cause the data center to be vulnerable to early obsolescence, which can impact data center availability and lead to a loss of revenue or increased cost to remediate.



Table 4-2 describes a number of data center facility considerations.

**Table 4-2** *Summary of Data Center Facility Considerations*

<b>Data Center Facility Considerations</b>	<b>Description</b>
Architectural and mechanical specifications	Space available Load capacity Power and cooling capacity Cabling infrastructure
Environmental conditions	Operating temperature Humidity level
Physical security	Access to the site Fire suppression Security Alarms
Capacity limits	Space for employees
Compliance and regulation	Payment Card Industry (PCI), Sarbannes-Oxley (SOX), and Health Insurance Portability and Accountability Act (HIPAA)

## Data Center Space

The space that the data center occupies makes up the physical footprint and helps answer many questions, including how to size the overall data center, where to position servers, how to make it flexible for future growth, and how to protect the valuable equipment inside.

The data center space element defines the number of racks for servers and telecommunications equipment that can be installed. The floor loading is affected by the rack weight after the racks are populated with equipment. Careful planning is needed to ensure that the floor loading is sufficient for current and future needs of the data center.

Selecting the proper size of the data center has a great influence on the cost, longevity, and flexibility of the data center. Although estimating the size of the data center is challenging, it is also critically important that it be done correctly.

Several factors need to be considered, including the following:

- The number of employees who will be supporting the data center
- The number of servers and the amount of storage gear and networking equipment that will be needed
- The space needed for non-infrastructure areas:
  - Shipping and receiving
  - Server and network staging
  - Storage rooms, break rooms, and bath rooms
  - Employee office space

Keep in mind that if the data center is undersized it will not sufficiently satisfy compute, storage, and network requirements and will negatively impact productivity and cause additional costs for expansion. On the flip side, a data center that is too spacious is a waste of capital and recurring operational expenses.

Right-size data center facilities consider the placement of infrastructure and equipment; and if properly planned, the data center can grow and support the organization into the future without costly upgrades or relocations.

Here are some other rack and cabinet space considerations to keep in mind:

- Weight of the rack and equipment
- Heat expelled from equipment
- Amount and type of power needed
  - Automatic transfer switch for equipment that has single power supplies
  - Uninterruptible power supplies (UPS)
  - Redundant power distribution units (PDU)
- Loading, which determines what and how many devices can be installed

## Data Center Power

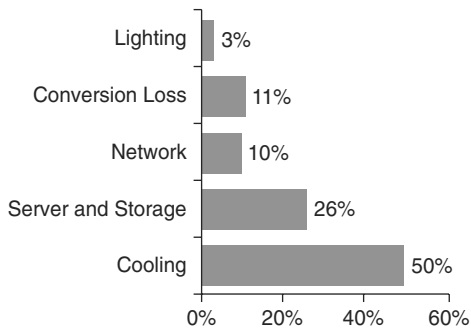
The power in the data center facility is used to power cooling devices, servers, storage equipment, the network, and some lighting equipment. Cooling down the data center requires the most power, next to servers and storage.

Because many variables make up actual power usage, determining power requirements for equipment in the data center can prove difficult. In server environments, the power usage depends on the computing load placed on the server. For example, if the server needs to work harder by processing more data, it has to draw more AC power from the power supply, which in turn creates more heat that needs to be cooled down.

The desired reliability drives the power requirements, which may include multiple power feeds from the power utility, UPS, redundant power circuits, and diesel generators. Depending on the options chosen, various levels of power redundancy can affect both capital and recurring operating expenses. Determining the right amount of power redundancy to meet the requirements takes careful planning to ensure success.

Estimating the power capacity needed involves collecting the requirements for all the current equipment, including the future requirements of the equipment for the data center. The complete power requirements must encompass the UPS, generators, HVAC, lighting, and all the network, server, and storage equipment.

Figure 4-4 shows an example of data center power usage.



**Figure 4-4** *Data Center Power Usage Example*

The designed power system should include electrical components such as PDUs, circuit breaker panels, electrical conduits, and wiring necessary to support the desired amount of physical redundancy. The power system also needs to provide protection for utility power failures, power surges, and other electrical problems by addressing the power redundancy requirements in the design.

Here are some key points related to data center power:

- Defines the overall power capacity.
- Provides physical electrical infrastructure and addresses redundancy.

- Power is consumed by the following:
  - Cooling
  - Servers
  - Storage
  - Network
  - Conversion and lighting

## Data Center Cooling

Devices in the data center produce variable amounts of heat depending on the device load. Heat overtime decreases the reliability of the data center devices. Cooling is used to control the temperature and humidity of the devices, and it is applied to zones, racks, or individual devices.

Environmental conditions need to be considered and measured by using probes to measure temperature changes, hot spots, and relative humidity.

A major issue with high-density computing is overheating. There are more hot spots, and therefore more heat overall is produced. The increase in heat and humidity threatens equipment life spans. Computing power and memory requirements demand more power and thus generate more heat output. Space-saving servers increase the server density possible in a rack, but keep in mind that density = heat. It might not be a big deal for one chassis at 3 kilowatt (kW), but with five or six servers per rack, the heat output increases to 20 kW. In addition, humidity levels can affect static electricity in the data center. So, it is recommended that relative humidity level be in the range of 40 percent to 55 percent. High levels of static electricity can cause damage to data center equipment.

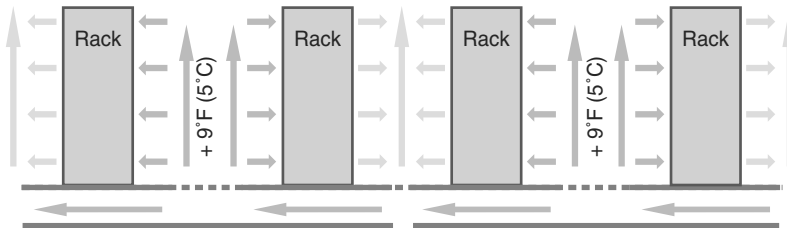
Proper airflow is required to reduce the amount of heat generated by the high-density equipment. Sufficient cooling equipment must be available to produce acceptable temperatures within the data center. The cabinets and racks should be arranged in the data center with an alternating pattern of “cold” and “hot” aisles. The cold aisle should have equipment arranged face to face, and the hot aisle should have equipment arranged back to back. In the cold aisle, there should be perforated floor tiles drawing cold air from the floor into the face of the equipment. This cold air passes through the equipment and flushes out the back into the hot aisle. The hot aisle does not have any perforated tiles, and this design prevents the hot air from mixing with the cold air.

Figure 4-5 illustrates the alternating pattern of cold and hot aisles along with airflow.

For equipment that does not exhaust heat to the rear, here are some other cooling techniques:

- Block unnecessary air escapes to increase airflow.
- Increase the height of the raised floor.
- Spread out equipment into unused racks.
- Use open racks rather than cabinets where security is not a concern.

- Use cabinets with mesh fronts and backs.
- Custom perforated tiles with larger openings.



**Figure 4-5** *Data Center Cold and Hot Aisles*

**Note:** 1 watt = 3.41214 British thermal units (BTU). Many manufacturers publish kW, kilovolt ampere (kVA), and BTU in their equipment specifications. Sometimes dividing the BTU value by 3.413 does not equal the published wattage. Use the manufacturer information if available, if not this can be a helpful conversion formula to use.

## Data Center Heat

Blade server deployments allow for more efficient use of space for servers, which is good, but there is also an increased amount of heat per server, which requires more cooling to maintain consistent temperatures.

The data center design must address the increased use of high density servers and the heat that they produce. During the data center design, considerations for cooling need to be taken into account for the proper sizing of the servers and the anticipated growth of the servers along with their corresponding heat output.

Here are some cooling solutions to address the increasing heat production:

- Increase the number of HVAC units.
- Increase the airflow through the devices.
- Increase the space between the racks and rows.
- Use alternative cooling technologies, such as water-cooled racks.

## Data Center Cabling

The cabling in the data center is known as the passive infrastructure. Data center teams rely on a structured and well-organized cabling plant. Although the active electronics are crucial for keeping server, storage, and network devices up and running, the physical cabling infrastructure is what ties everything together. The cabling in the data center terminates connections between devices and governs how each device communicates with one another.

Cabling has several key characteristics, such as the physical connector, media type, and cable length. Copper and fiber-optic cables are commonly used today. Fiber-optic cabling allows for longer distances and is less prone to interference than copper cabling. The

two main types of optical fiber are single-mode and multi-mode. Copper cabling is widely available, costs less, and generally covers shorter distances (up to 100 meters, about 328 feet). Typical copper cabling found in the data center is CAT 5e/CAT 6 with RJ-45 connectors.

Keep in mind that the emerging 10GBASE-T standard requires CAT6A twisted-pair cabling to support distances up to 100 meters.

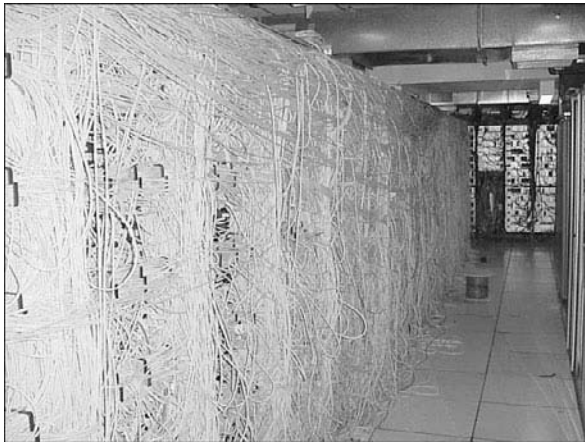
It is important for cabling to be easy to maintain, abundant and capable of supporting various media types and requirements for proper data center operations.

Cable management and simplicity is affected by the following:

- Media selection
- Number of connections
- Type of cable termination organizers
- Space for cables on horizontal and vertical cable trays

These considerations must to be addressed during the data center facility design (for the server, storage, network, and all the associated technologies that are going to be implemented).

Figure 4-6 shows an example of cabling that is out of control.

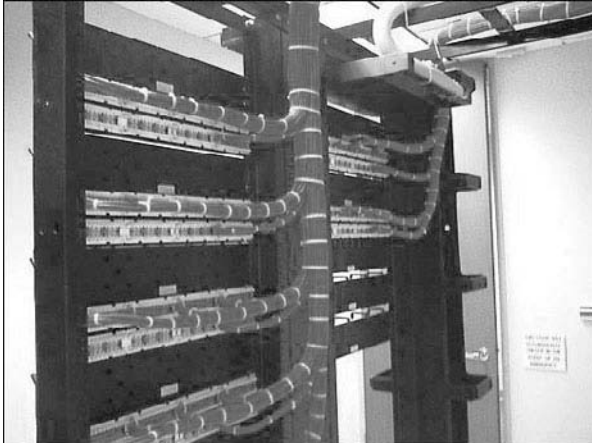


**Figure 4-6** *Data Center Cabling the Wrong Way*

Figure 4-7 shows the proper way to manage copper cabling.

The cabling infrastructure needs to avoid the following pitfalls:

- Inadequate cooling due to restricted airflow
- Outages due to accidental disconnect
- Unplanned dependencies resulting in more downtime
- Difficult troubleshooting options



**Figure 4-7** *Data Center Cabling the Right Way*

For example, using under-floor cabling techniques, especially with a high number of power and data cables can restrict proper airflow. Another disadvantage with this approach is that cable changes require you to lift floor tiles, which changes the airflow and creates cooling inefficiencies.

One solution is a cable management system above the rack for server connectivity. Cables should be located in the front or rear of the rack to simplify cable connections. In most service provider environments, cabling is located in the front of the rack.

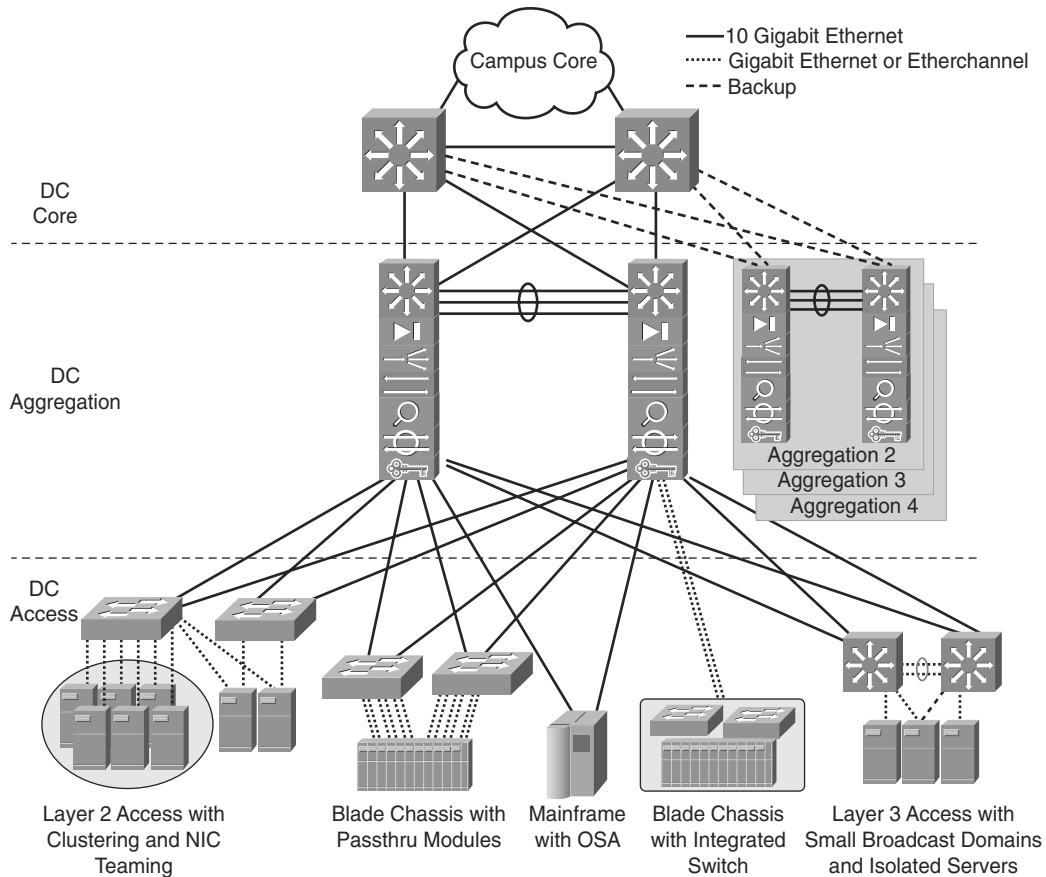
## Enterprise DC Infrastructure

Today's enterprise data center design follows the Cisco multilayer architecture, which includes DC core, DC aggregation, and DC access layers. This multitier model is the most common model used in the enterprise and it supports blade servers, single rack unit (1RU) servers, and mainframes.

Figure 4-8 provides a high-level overview of an enterprise data center infrastructure.

At the edge of the data center infrastructure is the access layer. The data center access layer needs to provide physical port density and both Layer 2 and Layer 3 services for flexible server connectivity options.

The data center aggregation layer ties the DC core and DC access layers together, which provides hierarchy for security and server farm services. Security services such as access control lists (ACL), firewalls, and intrusion prevention systems (IPS) should be implemented in the data center aggregation layer. In addition, server farm services such as content switching, caching, and Secure Sockets Layer (SSL) offloading should be deployed in the data center aggregation. Both the data center aggregation and core layers are commonly implemented in pairs for redundancy, to avoid single points of failure.



**Figure 4-8** *Enterprise Data Center Infrastructure Overview*

### Defining the DC Access Layer

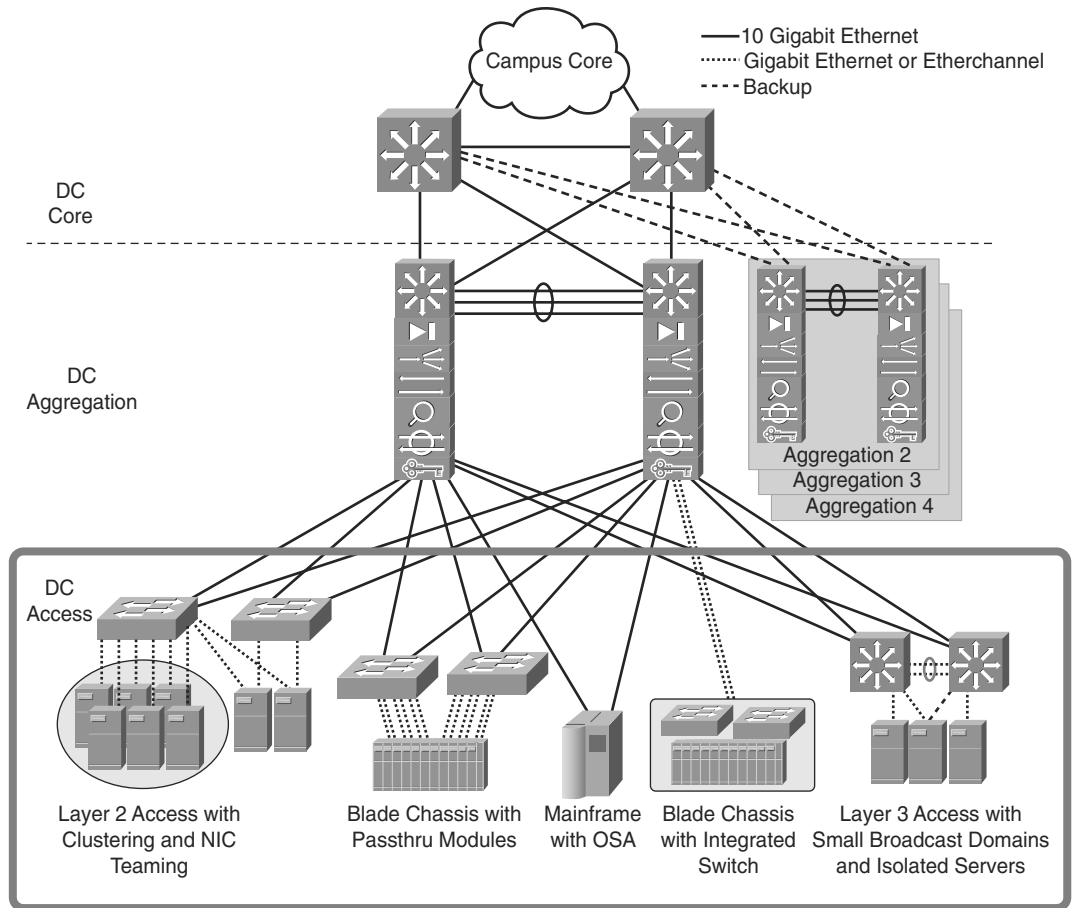


The data center access layer's main purpose is to provide Layer 2 and Layer 3 physical port density for various servers in the data center. In addition, data center access layer switches provide high-performance, low-latency switching and can support a mix of over-subscription requirements. Both Layer 2 and Layer 3 access (also called routed access) designs are available, but most data center access layers are built using Layer 2 connectivity. The Layer 2 access design uses VLAN trunks upstream, which allows data center aggregation services to be shared across the same VLAN and across multiple switches. Other advantages of Layer 2 access are support for NIC teaming and server clustering that requires network connections to be Layer 2 adjacent or on the same VLAN with one another.

Figure 4-9 highlights the data center access layer in the overall enterprise architecture.

The Spanning Tree Protocol (STP) manages physical loops that are present in the Layer 2 design. Currently, the recommended STP mode is Rapid per-VLAN Spanning Tree Plus (RPVST+), which ensures a logical loop-free topology and fast convergence.





**Figure 4-9** *Data Center Access Layer*

New routed access designs aim to contain Layer 2 locally to avoid the use of the STP. With routed access designs, the default gateway function needs to be provided because the access switch becomes the first-hop router in the network.

Designs with both Layer 2 and Layer 3 access provide flexibility for multiple server solutions to be supported, including 1RU servers and modular blade server chassis.

Here are some of the data center access layer benefits:

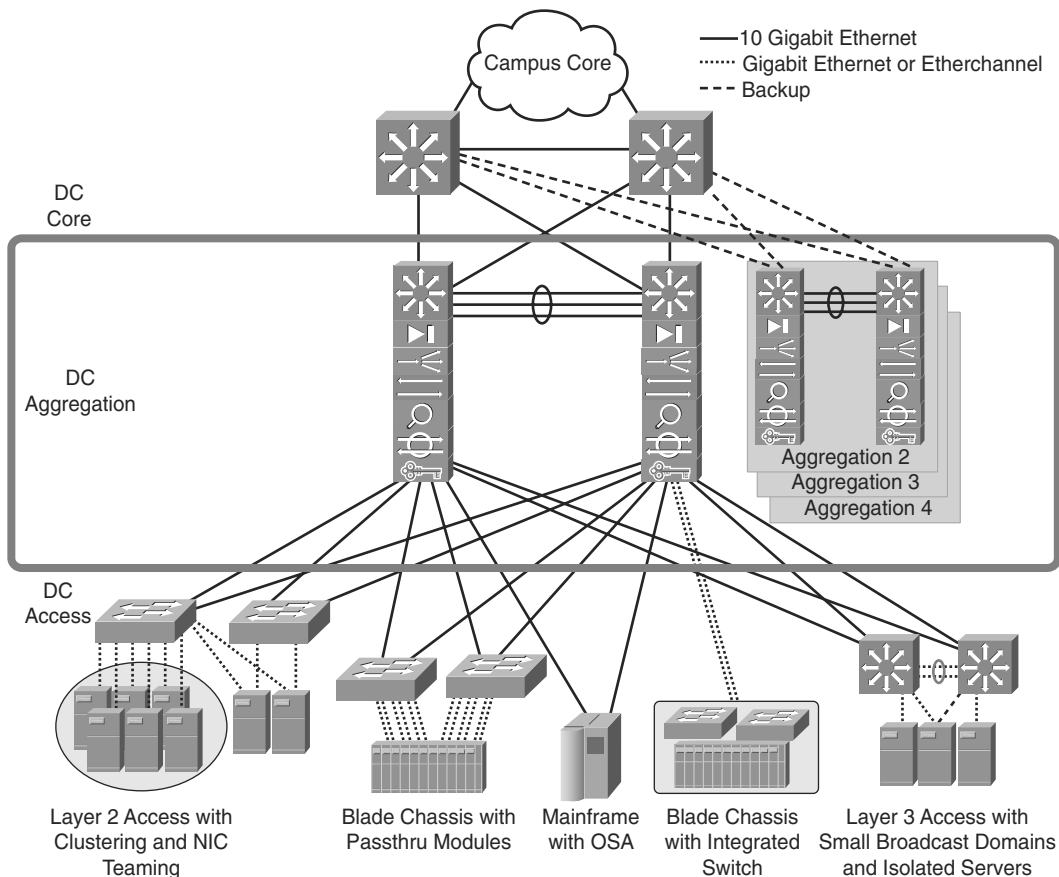
- Provides port density for server farms
- Supports single homed and dual homed servers
- Provides high-performance, low-latency Layer 2 switching
- Supports mix of oversubscription requirements

## Defining the DC Aggregation Layer

### Key Topic

The data center aggregation (distribution) layer aggregates Layer 2/Layer 3 links from the access layer and connects using upstream links to the data center core. Layer 3 connectivity is typically implemented between the data center aggregation and the data center core layers. The aggregation layer is a critical point for security and application services. The Layer 4 security and application services in the data center aggregation layer include server load balancing, SSL offloading, firewalling, and IPS services. These services maintain connection and session state for redundancy purposes and are commonly deployed in pairs using Cisco Catalyst 6500 service modules. This design reduces the total cost of ownership (TCO) and eases the management overhead by simplifying the number of devices that must be managed.

The highlighted section in Figure 4-10 illustrates the data center aggregation layer.



**Figure 4-10** Data Center Aggregation Layer

Depending on the requirements of the design, the boundary between Layer 2 and Layer 3 can be in the multilayer switches, firewalls, or content switching devices in the aggregation layer. Multiple aggregation layers can be built out to support separate network environments, such as production, test, and PCI infrastructure, each with its own security zone and application services. First-hop redundancy protocols Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) are commonly used in the aggregation layer. Many aggregation designs include positioning STP primary and secondary root bridges to help control the loop-free topology and support a larger STP processing load.

Here are some of the data center aggregation layer benefits:

- Aggregates traffic from DC access and connects to DC core.
- Supports advanced application and security services.
- Layer 4 services include firewall, server load balancing, SSL offload, and IPS.
- Large STP processing load.
- Highly flexible and scalable.

## Defining the DC Core Layer

The data center core connects the campus core to the data center aggregation layer using high-speed Layer 3 links. The core is a centralized Layer 3 routing layer in which one or more data center aggregation layers connect. The data center networks are summarized, and the core injects the default route into data center aggregation. The data center core also needs to support IP multicast to provide connectivity to the growing use of IP multicast applications.

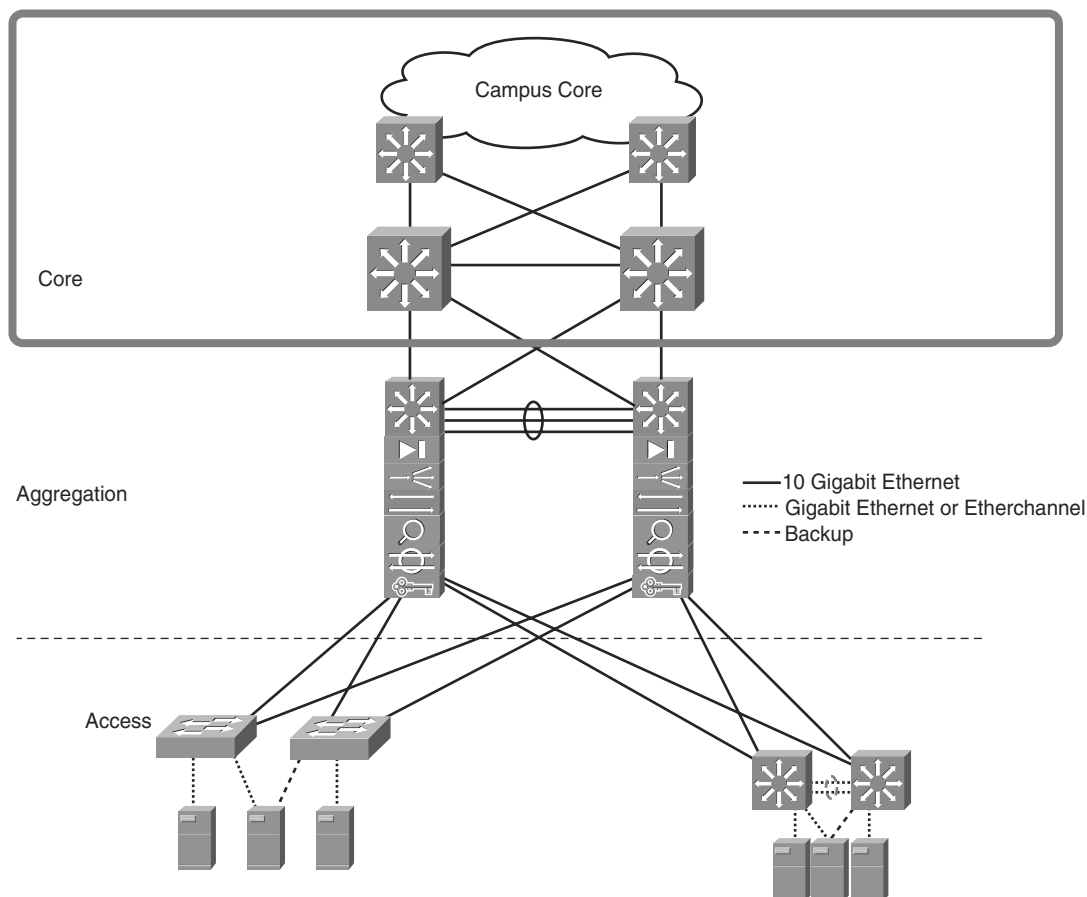


The data center core layer is a best practice component of larger data center networks. Smaller data centers may use a collapsed core design combining the aggregation layer and core layers together. However, if you are building a greenfield data center, it is recommended to implement a data center core in the beginning to avoid network downtime later. Table 4-3 shows some drivers to help you decide whether a data center core is appropriate for your design.

**Table 4-3** *Data Center Core Drivers*

<b>Data Center Core Drivers</b>	<b>Description</b>
10 Gigabit Ethernet density	Are there enough 10GE ports to connect campus core to multiple data center aggregation layers?
Administrative domains and policies	Separate cores help to isolate campus distribution from DC aggregation for troubleshooting and quality of service/access control list (QoS/ACL) policies.
Future growth	The impact and downtime from implementing a core at a later date make it worthwhile to install sufficient core layers in the beginning.

The highlighted section in Figure 4-11 illustrates the data center core layer.



**Figure 4-11** *Data Center Core Layer*

Here are some of the data center core characteristics:

- Low-latency switching
- Distributed forwarding architecture
- 10 Gigabit Ethernet
- Scalable IP multicast support

## Virtualization Overview

As the demand for IT to do more with less while increasing efficiency has risen, virtualization has become a critical component in most enterprise networks. Virtualization technologies allow a physical device to share its resources by acting as multiple versions of itself. Other forms of virtualization can enable multiple physical devices to logically appear as one.

Virtualization is a critical component of the Cisco network architectures for the enterprise data center and is changing the way data centers are architected. The use of virtualization improves network efficiency, provides enhanced flexibility, and reduces operational expenses.

### Challenges

Network designers face many challenges that are driving the need to deploy virtualization technologies in the network. Data centers are growing rapidly, and these challenges directly impact the profitability of the business.



Take a look at some of the key driving forces for virtualization adoption in Table 4-4.

**Table 4-4** *Virtualization Key Drivers*

<b>Virtualization Driving Forces</b>	<b>Description</b>
Operational cost	Need to reduce rising cost of powering and cooling devices in the DC while getting more productivity
Reduce the number of physical devices	DC consolidation of assets performing individual tasks
Traffic isolation	Logical, separate user groups secured from other groups on the same network
Increased performance/price ratio	Eliminate underutilized hardware that exhibits poor performance/price ratio

### Defining Virtualization and Benefits

*Virtualization* is an umbrella term used to represent several different technologies. Virtualization technologies share a common theme in their ability to abstract logical elements from hardware (applications or operating systems) or networks (LANs and SANs) and run them in a virtual state. Virtualization brings many benefits, from consolidation to increased efficiency.

Here are some of the common benefits achieved through virtualization techniques:

- Better use of computing resources, higher server densities, and simplified server migrations
- Provides flexibility for ease of management for adds, reassignments, or repurposing resources
- Separation of users groups on the same physical network, enabling traffic isolation
- Ability to provide per-department security policies
- Reduction in power and space required
- Increased uptime and reduced operational costs

## Types of Virtualization

Enterprise networks consist of two main types of virtualization technologies groupings, called network virtualization and device virtualization:



- **Network virtualization** encompasses logical isolated network segments that share the same physical infrastructure. Each segment operates independently and is logically separate from the other segments. Each network segment appears with its own privacy, security, independent set of policies, QoS levels, and independent routing paths.

Here are some examples of network virtualization technologies:

- **VLAN:** Virtual local-area network
- **VSAN:** Virtual storage-area network
- **VRF:** Virtual routing and forwarding
- **VPN:** Virtual private network
- **vPC:** Virtual Port Channel
- **Device virtualization** allows for a single physical device to act like multiple copies of itself. Device virtualization enables many logical devices to run independently of each other on the same physical piece of hardware. The software creates virtual hardware that can function just like the physical network device. Another form of device virtualization entails using multiple physical devices to act as one logical unit.

Here are some examples of device virtualization technologies:

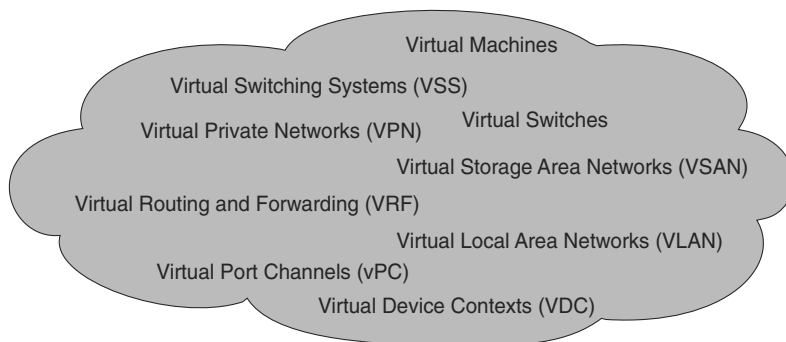
- Server virtualization: Virtual machines (VM)
- Cisco Application Control Engine (ACE) context
- Virtual Switching System (VSS)
- Cisco Adaptive Security Appliance (ASA) firewall context
- Virtual device contexts (VDC)

## Virtualization Technologies

Virtualization is built from abstracting logical entities from pooled physical resources. The Cisco network architectures for the enterprise data center contains many forms of network and device virtualization technologies.



Figure 4-12 illustrates the many virtualization technologies in use today.



**Figure 4-12** *Data Center Virtualization Technologies*

### VSS

Virtual Switching System (VSS) is a network virtualization technology that allows two physical Cisco Catalyst 6500 series switches to act as a single logical virtual switch. The VSS increases operational efficiencies and scales bandwidth up to 1.4 Tb/s. This technology is very similar to StackWise technology used with the Cisco Catalyst 3750 series product line, which enables switches stacked together to operate as one and use a single command-line interface (CLI) for management. However, VSS is limited to two physical chassis connected together.

### VRF

Virtual routing and forwarding (VRF) is a routing virtualization technology that creates multiple logical Layer 3 routing and forwarding instances (route tables) that can function on the same physical router. In Multiprotocol Label Switching (MPLS) VPN environments, the use of VRF technology plays a major role by allowing multiple networks to coexist on the same MPLS network. The routing information is contained inside the VRF and is visible only to routers participating in the same VRF. Because the routing information with VRF is separated, duplicate IP addressing schemes can be used.

### vPC

Virtual Port Channel (vPC) technology works by combining two Cisco Nexus 7000 series switches or two Cisco Nexus 5000 series switches with 10GE links, which are then represented to other switches as a single logical switch for port channeling purposes. With vPC, the spanning-tree topology appears loop-free, although multiple redundant paths are present in the physical topology.



## Device Contexts

Device contexts enable a single physical network device to host multiple virtual network devices. Each device context is an independent configuration with its own policy, network interfaces, and management accounts. The virtualized contexts that run on a single network device operate similarly to standalone network devices. Most of the same features present on the physical device are also supported on the individual device contexts.

The following Cisco network devices support the use of device contexts:

- Cisco Nexus 7000 series switches (VDC)
- Cisco Adaptive Security Appliance (ASA) firewall
- Cisco Catalyst 6500 Firewall Services Module (FWSM)
- Cisco Application Control Engine Appliance
- Cisco Catalyst 6500 Application Control Engine Module
- Cisco Intrusion Prevention System (IPS)

## Server Virtualization

The use of server virtualization has exploded onto the market over the past several years and can be found in most data center environments. Server virtualization is a software technique that abstracts server resources from the hardware to provide flexibility and to optimize the usage of the underlying hardware. As a result, many data center applications are no longer bound to bare-metal hardware resources.

The server virtualized hypervisor provides the foundation for the virtualized environment on the host. The hypervisor controls the hardware and physical resources that can be allocated to virtual machines running on the host. This makes the VMs unaware of the physical hardware, but they can use CPUs, memory, and network infrastructure as shared pools available through the virtualization process.

The following represents several server virtualization vendors and their associated products:

- VMware ESX Server
- Citrix XenServer
- Microsoft Hyper-V

## Network Virtualization Design Considerations

Network solutions are needed to solve the challenges of sharing network resources but keeping users totally separate from one another. Although the users are separate, we still need to ensure that the network is highly available, secure, and can scale along with the business growth. Network virtualization offers solutions to these challenges and provides design considerations around access control, path isolation, and services edge.



## Access Control

Access needs to be controlled to ensure that users and devices are identified and authorized for entry to their assigned network segment. Security at the access layer is critical for protecting the network from threats, both internal and external.

## Path Isolation

Path isolation involves the creation of independent logical network paths over a shared network infrastructure. MPLS VPN is an example of path-isolation technique where devices are mapped to a VRF to access the correct set of network resources. Other segmentation options include VLANs and VSANs, which logically separate LANs and SANs. The main goal when segmenting the network is to improve the scalability, resiliency, and security services as with non-segmented networks.

## Services Edge

The services edge refers to making network services available to the intended users, groups, and devices with an enforced centralized managed policy. Separate groups or devices occasionally need to share information that may be on different VLANs, each with corresponding group policies. For example, traffic from the sales VLAN might need to talk to the engineering VLAN, but it needs to go through the firewall to permit the traffic and might even be tied to certain hours of the day. In such cases, the network should have a central way to manage the policy and control access to the resources. An effective way to address policy enforcement is to use an FWSM in a Cisco Catalyst 6500 series switch providing firewall services for the data center.



Table 4-5 describes network virtualization considerations.

**Table 4-5** *Network Virtualization Design Considerations*

<b>Network Virtualization Consideration</b>	<b>Description</b>
Access control	Ensures users and devices are recognized, classified, and authorized for entry to their assigned network segments
Path isolation	Provides independent logical traffic paths over shared network
Services edge	Ensures the right services are accessible the intended users, groups, or devices

## References and Recommended Readings

Module 3 (Designing Basic Campus and Data Center Networks)—Designing for Cisco Internetwork Solution Course (DESGN) 2.1.

Cisco Design Zone for Data Centers, [www.cisco.com/en/US/netsol/ns743/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html).

Data Center Design – IP Network Infrastructure, [www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/DC\\_3\\_0/DC-3\\_0\\_IPInfra.html#wp1037111](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html#wp1037111).

Cisco Data Center Infrastructure 2.5 Design Guide, [www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/DC\\_Infra2\\_5/DCInfra\\_2.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_2.html).

Security and Virtualization in the Data Center, [www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/DC\\_3\\_0/dc\\_sec\\_design.html#wp1056029](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html#wp1056029).

Examples of Good Cable Management, [www.geekshout.com/media/photos/9-examples-of-good-cable-management-and-1-bad-one/](http://www.geekshout.com/media/photos/9-examples-of-good-cable-management-and-1-bad-one/).

## Exam Preparation Tasks

### Review All Key Topics

Review the most important topics in the chapter, noticed with the Key Topic icon in the outer margin of the page. Table 4-6 lists a reference of these key topics and the page numbers on which each is found.

**Table 4-6** *Key Topics*

Key Topic Element	Description	Page
Data Center 3.0 Components	Virtualization, Unified Fabric, and Unified Computing	126
Data Center 3.0 Topology Components	Virtualized servers, consolidated connectivity, and network devices	127
Challenges in the DC	Power, space, security, and management	127
Data Center Facility Aspects	Architectural and mechanical specifications, environmental conditions, physical security, capacities and compliance	129
Data Center Power	Cooling, server, storage, and network	131
Data Center Cabling	Controls the temperature and humidity of the devices	133
DC Access Layer	Provides Layer 2 and Layer 3 physical port density for devices	136
DC Aggregation Layer	Aggregates L2/L3 links from the access layer and connects using upstream links to the data center core	138
DC Core Layer	Centralized Layer 3 routing layer in which one or more data center aggregation layers connect	139

**Table 4-6** *Key Topics*

Key Topic Element	Description	Page
Challenges	Operational cost, traffic isolation, and increased performance/price ratio	141
Types of Virtualization	Network and device virtualization	142
Virtualization Technologies	VRE, vPC, and VSS	143
Device Contexts	VDC, ASA, and ACE	144
Services Edge	Secure network services available to users and groups with centralized managed policy	145

## Complete Tables and Lists from Memory

Print a copy of Appendix D, “Memory Tables,” (found on the CD), 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 CD, 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:

Cisco Nexus 1000V, Cisco Unified Computing System (UCS), Fibre Channel over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), data center space element, power, cabling, data center access, data center aggregation, data center core, virtualization technologies, network virtualization, device virtualization, access control, path isolation, services edge

## Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the exam engine on the CD-ROM.

1. Which data center architecture was based on client/server and distributed computing?
  - a. Data Center 1.0
  - b. Data Center 2.0
  - c. Data Center 3.0
  - d. Data Center 4.0

2. What Cisco Nexus switch helps deliver visibility and policy control for virtual machines (VM)?
  - a. Nexus 7000
  - b. Nexus 4000
  - c. Nexus 2000
  - d. Nexus 1000V
3. Which of the following is a network adapter that can run at 10GE and support Fibre Channel over Ethernet (FCoE)?
  - a. CNA
  - b. VN-Link
  - c. MDS
  - d. NAS
4. What is an innovative next-generation data center platform that converges computing, network, storage, and virtualization all together into one system? (Select the best answer.)
  - a. Cisco MDS
  - b. Cisco Nexus 7000
  - c. Cisco Nexus 5000
  - d. Cisco UCS
5. Which of the following Cisco Nexus switches support virtual device contexts using (VDCs)?
  - a. Cisco Nexus 7000
  - b. Cisco Nexus 2000
  - c. Cisco Nexus 5000
  - d. Cisco Nexus 4000
6. What services option provides an effective way to address firewall policy enforcement in a Cisco Catalyst 6500 series switch?
  - a. IPS
  - b. FWSM
  - c. Nexus 1000V
  - d. VDCs

7. What has enabled applications to no longer be bound to bare metal hardware resources?
  - a. Unified fabric
  - b. Device virtualization
  - c. Network virtualization
  - d. Server virtualization
8. Which of the following supports network virtualization technology that allows two physical Cisco Catalyst 6500 series switches to act as a single logical virtual switch?
  - a. VN-Link technology
  - b. Unified fabric
  - c. Virtual Switching System (VSS)
  - d. Virtual routing and forwarding (VRF)
9. What enables the spanning-tree topology to appear loop-free although multiple redundant paths are present in the physical topology?
  - a. vPC
  - b. VRF
  - c. VSS
  - d. VDC
10. Which of the following are data center core layer characteristics? (Select all that apply.)
  - a. 10GE
  - b. High-latency switching
  - c. Distributed forwarding architecture
  - d. Service modules
11. Which data center layer provides advanced application and security services and has a large STP processing load?
  - a. Data center access layer
  - b. Data center aggregation layer
  - c. Data center services layer
  - d. Data center core layer

- 12.** Which of the following are drivers for the data center core layer? (Select all that apply.)
- a.** Future growth
  - b.** 10 Gigabit Ethernet density
  - c.** Services edge
  - d.** Administrative domains and policies
- 13.** Benefits such as port density for server farms, high-performance low-latency Layer 2 switching, and a mix of oversubscription requirements belong to which data center layer?
- a.** Core
  - b.** Distribution
  - c.** Access
  - d.** Aggregation
- 14.** Cable management is affected by which of the following? (Select all that apply.)
- a.** Alternative cooling technologies
  - b.** Number of connections
  - c.** Media selection
  - d.** Increase in the number of HVAC units
- 15.** Which of the following best describes how “cold” and “hot” aisles should be arranged in the data center?
- a.** Hot and cold aisles facing each other
  - b.** Alternating pattern of cold and hot aisles
  - c.** Nonalternating pattern of hot and cold aisles
  - d.** None of the above
- 16.** Within the unified computing resources, what defines the identity of the server?
- a.** Virtualization
  - b.** Unified fabric
  - c.** Services profile
  - d.** Virtual machines

# Index

---

## Numerics

---

10 Gigabit Ethernet design rules, 88  
10BASE-2 Ethernet, 83  
10BASE-5 Ethernet, 83  
10BASE-T Ethernet, 83  
100BASE-FX Fast Ethernet, 85  
100BASE-T Ethernet, 83, 85-86  
100BASE-T4 Fast Ethernet, 84-85  
100BASE-TX Fast Ethernet, 84  
100-Mbps Fast Ethernet design rules, 84-86  
1000BASE-CX Gigabit Ethernet over coaxial cable, 87  
1000BASE-LX long-wavelength Gigabit Ethernet, 86-87  
1000BASE-SX short-wavelength Gigabit Ethernet, 87  
1000BASE-T Gigabit Ethernet over UTP, 87

---

## A

---

access control. *See also* unauthorized access  
defined, 466  
firewall ACLs, 487-488  
identity and access control deployments, 489-490  
in network virtualization design, 145  
WLAN access control, 159-160

access layer in hierarchical network models, 43-44  
campus LAN design best practices, 96  
enterprise data center design, 136-137  
access VPNs, 232  
ACD, 528  
address resolution protocol (ARP), 295  
addressing  
in IPv4, 275-295  
    *assignment and name resolution*, 290-295  
    *classes*, 276-278  
    *NAT (Network Address Translation)*, 279-282  
    *private addresses*, 279  
    *subnets*, 282-290  
    *types of*, 278  
in IPv6, 311-319  
    *allocations*, 313-314  
    *anycast addresses*, 316-317  
    *assignment strategies*, 322-324  
    *global aggregatable addresses*, 316  
    *global unicast addresses*, 314-315  
    *IPv4-compatible IPv6 addresses*, 312, 316  
    *link-local addresses*, 315  
    *loopback addresses*, 314  
    *multicast addresses*, 317-319



- prefixes, 312-313, 319*
  - representation of addresses, 311-313*
  - unicast addresses, 314-316*
  - unique local addresses, 315-316*
- addressing digit signaling (voice networks), 526
- adjacencies in OSPFv2, 392-393
- administrative distance, 355-356
- aggregation layer. *See* distribution layer in hierarchical network models
- aggregator attribute in BGP, 413
- allocations of IPv6 addresses, 313-314
- analog-to-digital signal conversion, 540
- analyzing networks, tools for, 22
- AND logical operation, 285
- anycast addresses in IPv6, 316-317
- AP controller equipment scaling, 171
- AP modes in Cisco UWN, 164-166
- application access, accelerating, 13
- application layer (OSI model), 665
- application layer (TCP/IP architecture), 666
- application requirements in WAN design, 214
- application types in campus LAN design, 94-95, 103

- architectures. *See* enterprise architectures
- areas
  - in OSPFv2, 393
  - in OSPFv3, 401
- ARP (address resolution protocol), 59, 295
- assessment. *See* auditing networks, tools for
- assigning
  - IPv4 addresses, 290-295
    - BOOTP, 291*
    - DHCP, 291-292*
    - static versus dynamic assignment, 290-291*
  - IPv6 addresses, 322-324
    - DHCPv6, 324*
    - globally unique addresses, 323*
    - link-local addresses, 322-323*
- atomic aggregate attribute in BGP, 413
- auditing networks, tools for, 18-21
- authentication
  - identity and access control deployments, 489-490
  - IEEE 802.1X-2001 port-based authentication, 159
  - in RIPng, 365
  - in RIPv2, 362
  - router authentication in OSPFv2, 399
  - WLANs (wireless LANs), 167-169

Auto QoS in VoIP, 559

autoconfiguration. *See* stateless autoconfiguration

autonomous system external path types in OSPFv2, 397

autonomous system path attribute in BGP, 412

auto-RP, 429-430

availability. *See* network availability, increasing

## B

---

backups in WAN design, 240-241. *See also* high availability network services

balancing loads, 62

bandwidth comparisons

in IPT design, 550-552

for routing protocols, 357

in WAN design, 215-216

Beauty Things Store scenario, 606-608

best practices

campus LAN design, 94-109

*access layer*, 96

*application type network requirements*, 103

*application types*, 94-95

*core layer*, 98-99

*distribution layer*, 96-98

*edge distribution*, 103

*enterprise campus LAN design*, 102-103

*enterprise data center module*, 105-106

*large-building LAN design*, 101-102

*medium-size LANs*, 103

*multicast traffic considerations*, 108-109

*QoS considerations*, 106-107

*server connectivity options*, 105

*server farms*, 104

*small and remote site LANs*, 103-104

IPT design, 560-561

BGP (Border Gateway Protocol), 404-416

administrative distance, 409

characteristics of, 415-416

confederations, 409

decision process, 414-415

eBGP, 406

iBGP, 406-407

neighbors, 405-406

path attributes, 410-413

route reflectors, 407-409

weight, 414

BGP4 multiprotocol extensions for IPv6, 326

BHT (busy-hour traffic), 529-530

Big Oil and Gas scenario, 604-606

binary numbers

converting decimal to, 673-675

converting hexadecimal to, 672-673

converting to decimal, 673

converting to hexadecimal, 672

decimal and hexadecimal equivalents of, 672

explained, 671

IP and MAC address representation, 671

subnet mask values for, 675

bit masks for subnet masks, 283

blade servers in data center design, 128

blocking probability, 530

BOOTP, 291

bootstrap routers, PIMv2 bootstrap routers, 430

**Border Gateway Protocol.** *See* BGP (Border Gateway Protocol)  
**borderless network architecture,** 9, 58  
**bottom-up approach to network design,** comparison with top-down approach, 24  
**branch LAN design,** 184-186  
     H-REAP, 184-185  
     local MAC support, 184  
     REAP, 184  
     UDP ports used in, 186  
**branch WAN design.** *See* enterprise branch architectures  
**bridges, enterprise LAN design,** 91  
**bridging layer (OSI model),** 663  
**BTUs, wattage conversion,** 133  
**business agility, improving,** 12  
**busy hour,** 529  
**busy-hour traffic (BHT),** 529-530

## C

---

**cabling**  
     dark fiber cabling, 211-212  
     in data center design, 133-135  
     for WANs, 206-207  
**calculating voice bandwidth,** 551-552  
**call detail records (CDR),** 528, 530  
**call seconds,** 529  
**CallManager Express deployment**  
     model for IP telephony networks, 537  
**campus LAN design.** *See also* enterprise LAN design  
     best practices, 94-109  
         *access layer,* 96  
         *application type network requirements,* 103  
         *application types,* 94-95  
         *core layer,* 98-99  
         *distribution layer,* 96-98  
         *edge distribution,* 103  
         *enterprise campus LAN design,* 102-103  
         *enterprise data center module,* 105-106  
         *large-building LAN design,* 101-102  
         *medium-size LANs,* 103  
         *multicast traffic considerations,* 108-109  
         *QoS considerations,* 106-107  
         *server connectivity options,* 105  
         *server farms,* 104  
         *small and remote site LANs,* 103-104  
     resources for information, 109  
     for wireless LANs, 183-184  
**campus media comparison chart,** 89  
**campus security,** 502-503  
**CAPWAP (Control and Provisioning for Wireless Access Point),** 163  
**CAS signaling,** 524  
**case studies.** *See* scenarios  
**Catalyst 6500 service modules,** 500-502  
**CCDA exam updates,** 657-658  
**CCS (Centum call second),** 529  
**CCS signaling,** 524  
**CDP (Cisco Discovery Protocol),** 587  
**CDR (call detail records),** 528, 530  
**cell-switched WANs,** 230  
**Centrex services,** 528  
**Centum call second (CCS),** 529  
**certificates, defined,** 465  
**CGMP (Cisco Group Management Protocol),** 108, 426-427

- checklists, network checklist, 22-23
- circuit-switched WANs, 230
- Cisco 860 ISRs in enterprise teleworker architectures, 254
- Cisco 880 ISRs in enterprise teleworker architectures, 255
- Cisco Discovery Protocol (CDP), 587
- Cisco Easy VPN, 235
- Cisco Enterprise Architecture model, 47-58
  - e-commerce submodule, 50-51
  - enterprise campus module, 48-50
  - enterprise edge area, 50-54
  - enterprise WAN submodule, 53-54
  - hierarchical layers, 44-45
  - Internet connectivity submodule, 51-52
  - remote modules, 55-57
  - resources for information, 65
  - service provider edge module, 54-55
  - VPN/remote access submodule, 52-53
- Cisco Enterprise MAN/WAN architecture, 243
- Cisco Group Management Protocol (CGMP), 108, 426-427
- Cisco Identity-Based Network Services (IBNS), 489
- Cisco IronPort ESA, 493-494
- Cisco IronPort WSA, 494
- Cisco NAC Appliance, 488
- Cisco Radio Resource Management (RRM), 178-179
- Cisco router/switch platform and software comparison, 247
- Cisco SAFE (Security Architecture for the Enterprise), 484-486, 496
- Cisco SCF (Security Control Framework), 486
- Cisco security appliances, 499-500
- Cisco UWN (Unified Wireless Network), 160-176
  - AP controller equipment scaling, 171
  - AP modes, 164-166
  - architectures, 160-161
  - authentication, 167-169
  - CAPWAP, 163
  - local MAC support, 164
  - LWAPP, 162
  - LWAPP discovery of WLC, 166-167
  - roaming, 173-176
  - split-MAC architecture, 163-164
  - WLC components, 169
  - WLC interface types, 169-171
- class A addresses (IPv4), 277
- class B addresses (IPv4), 277
- class C addresses (IPv4), 277
- class C networks, common bits within, 417
- class D addresses (IPv4), 277
- class E addresses (IPv4), 278
- class-based weighted fair queueing in WAN design, 218-219
- classes of IPv4 addresses, 276-278
- classful routing protocols, classless routing protocols versus, 353-354
- classification in WAN design, 218
- classless routing protocols, classful routing protocols versus, 353-354
- codecs, 539-541
  - analog-to-digital signal conversion, 540
  - standards, 540-541
- collaboration architecture, 9-10
- collision domains for 100BASE-T Ethernet, 85
- commands for manual network auditing, 19-21
- communications, layered communication example, 666-667

community attribute in BGP, 413  
 comprehensive scenarios. *See* scenarios  
 confederations in BGP, 409  
 confidentiality  
   breaches, 455-456  
   transmission confidentiality, 469  
 congestion management in WAN design, 218  
 connection modules for WANs, 203-204  
 connection security, 466-470  
   data integrity, 469-470  
   encryption, 466-467  
   transmission confidentiality, 469  
   VPN protocols, 467-469  
 continuous security, 461-462  
 contracts for WAN transport technologies, 212-213  
 Control and Provisioning for Wireless Access Point (CAPWAP), 163  
 converged multiservice networks.  
   *See* IP telephony networks  
 converting  
   binary to decimal numbers, 673  
   binary to hexadecimal numbers, 672  
   decimal to binary numbers, 673-675  
   decimal to hexadecimal numbers, 668-670  
   hexadecimal to binary numbers, 672-673  
   hexadecimal to decimal numbers, 670  
 cooling in data center design, 132-133  
 core layer in hierarchical network models, 41-42  
   campus LAN design best practices, 98-99  
   enterprise data center design, 139-140  
 cost for routing protocols, 358  
 cost of ownership, lowering, 12

counting to infinity (routing protocol loop prevention), 361  
 country codes, list of, 526-527  
 cRTP in VoIP, 556  
 custom queueing in WAN design, 218  
 customer requirements  
   for campus LAN application types, 95, 103  
   identifying, 15-17

## D

---

dark fiber cabling, 211-212  
 Data Center 3.0 components, 125-126  
 Data Center 3.0 topology components, 127  
 data center security, 503-504  
 data center/virtualization architecture, 10  
 data centers. *See* enterprise data center design; enterprise data center module  
 data integrity, 469-470  
 data link layer (OSI model), 663  
 decimal equivalents  
   of binary numbers, 672  
   of hexadecimal numbers, 668  
 decimal numbers  
   converting binary to, 673  
   converting hexadecimal to, 670  
   converting to binary, 673-675  
   converting to hexadecimal, 668-670  
 decision process in BGP, 414-415  
 default metric in route redistribution, 420-421  
 delay components in IP telephony networks, 552-554  
 delay for routing protocols, 359  
 denial of service (DoS) attacks, 450, 454-455

dense multicast distribution, sparse  
multicast distribution versus, 427-428

dense wavelength-division multiplexing  
(DWDM), 212

deploying servers. *See* server  
deployment challenges in data  
center design

deployment models

of IP telephony networks, 535-537

*CallManager Express model*, 537

*multisite WAN with centralized  
call processing model*, 536

*multisite WAN with distributed  
call processing model*, 536-537

*single-site deployment*, 535-536

IPv4 to IPv6, 326-333

*comparison of*, 332

*dual-stack deployment model*, 329

*hybrid deployment model*, 330

*service block deployment model*,  
330

design documents, 25-26

design goals of IP telephony networks,  
534-535

design methodology in PPDIIO life  
cycle, 15. *See also* network design

design of IPv4 subnets, 283-284

Design phase (PPDIIO life cycle), 14

deterministic redundancy, dynamic  
redundancy versus, 176

device contexts in virtualization, 144

device virtualization, 142

DHCP, 291-292

in VoIP, 542

DHCPv6, 324

digital subscriber line (DSL), 206

distance-vector routing protocols,  
351-353

distribution layer in hierarchical network  
models, 42-43

campus LAN design best practices,  
96-98

enterprise data center design, 138-139

distribution trees, 428

DMVPN, 236

DNS (Domain Name System),  
292-294, 542

domains of trust, 463-464

DoS (denial of service) attacks, 450,  
454-455

dotted-decimal format for subnet masks,  
283

DRs in OSPFv2, 395-396

DSCP AF packet-drop precedence  
values in IPv4 headers, 273

DSCP and IP precedence values in IPv4  
headers, 273

DSCP values in IPv4 headers, 274

DSL (digital subscriber line), 206

DTMF frequencies, 526

DUAL, EIGRP and, 368-369

dual-stack deployment model, IPv4 to  
IPv6, 329

dual-stack transitions, IPv4 to IPv6, 326

DVMRP, 430

DWDM (dense wavelength-division  
multiplexing), 212

dynamic IP addressing, 290-291

dynamic redundancy, deterministic  
redundancy versus, 176

dynamic routes, static routes versus,  
348-350

dynamic WEP keys, 159

## E

---

E&M signaling, 523-524

E.164 standard, 526

- eBGP, 406
- echo cancellation, 555
- e-commerce submodule in Cisco Enterprise Architecture model, 50-51
- edge distribution, campus LAN design
  - best practices, 103
- EIGRP, 351-352, 367-375
  - characteristics of, 375
  - components of, 367
  - design, 372
  - DUAL and, 368-369
  - for IPv4, 373
  - for IPv6, 325, 373-374
  - metrics, 370-371
  - neighbor discovery and recovery, 368
  - packet types, 371-372
  - protocol-dependent modules, 368
  - RTP and, 368
  - timers, 369-370
- email threats, IronPort ESA (Email Security Appliances), 493-494
- encryption, 466-467
- endpoint security, 502
- enterprise architectures. *See also* Cisco Enterprise Architecture model
  - benefits of, 10-11
  - borderless network architecture, 9, 58
  - business forces affecting, 8
  - Cisco UWN (Unified Wireless Network), 160-161
  - collaboration architecture, 9-10
  - data center/virtualization architecture, 10, 124-127, 135-140
    - access layer*, 136-137
    - core layer*, 139-140
    - Data Center 3.0 components*, 125-126
    - Data Center 3.0 topology components*, 127
    - distribution layer*, 138-139
  - technology forces affecting, 8
  - traditional voice architectures, 518-530
    - ACD*, 528
    - blocking probability*, 530
    - busy hour*, 529
    - busy-hour traffic (BHT)*, 529-530
    - call detail records (CDR)*, 528, 530
    - Centrex services*, 528
    - Centum call second (CCS)*, 529
    - Erlangs*, 528-529
    - grade of service (GoS)*, 528
    - IVR systems*, 528
    - local loops and trunks*, 519-520
    - ports*, 520-521
    - PSTN, described*, 518
    - PSTN numbering plan*, 526-527
    - PSTN versus PBX switches*, 518-519
    - signaling types*, 521-526
    - voice mail*, 528
  - types of, 9
- enterprise branch architectures, 248-253
  - design rules, 248
  - ISR versus ISR G2 features, 249
  - large branch design, 252-253
  - medium branch design, 250-251
  - profiles, 248-249
  - small branch design, 250
- enterprise branch module in Cisco Enterprise Architecture model, 56
- enterprise campus LAN design, 102-103
- enterprise campus module in Cisco Enterprise Architecture model, 48-50
- enterprise data center design
  - architectures, 124-127, 135-140
    - access layer*, 136-137
    - core layer*, 139-140



- Data Center 3.0 components, 125-126*
- Data Center 3.0 topology components, 127*
- distribution layer, 138-139*
- resources for information, 145-146
- server deployment challenges, 127-135
  - cabling, 133-135*
  - cooling, 132-133*
  - facilities, 128-129*
  - power usage, 131-132*
  - space allotment, 130*
- virtualization, 141-145
  - benefits of, 141-142*
  - challenges, 141*
  - design considerations, 144-145*
  - technologies for, 143-144*
  - types of, 142*
- enterprise data center module**
  - campus LAN design best practices, 105-106
  - in Cisco Enterprise Architecture model, 56
- enterprise edge area**
  - in Cisco Enterprise Architecture model, 50-54
  - security for, 504-506
- enterprise LAN design. *See also* campus LAN design; wireless LAN design**
  - hardware, 89-94
    - bridges, 91*
    - device comparison chart, 94*
    - hubs, 90-91*
    - Layer 3 switches, 93-94*
    - repeaters, 90*
    - routers, 92-93*
    - switches, 91-92*
  - LAN media, 82-89
    - 10 Gigabit Ethernet design rules, 88*
    - campus media comparison chart, 89*
    - EtherChannel, 89*
    - Ethernet design rules, 83*
    - Fast Ethernet design rules, 84-86*
    - Gigabit Ethernet design rules, 86-87*
  - resources for information, 109
- enterprise security, 502-506.**
  - See also* security
  - campus security, 502-503
  - data center security, 503-504
  - enterprise edge and WAN security, 504-506
- enterprise teleworker architectures, 254-255**
- enterprise teleworker module in Cisco Enterprise Architecture model, 56-57**
- enterprise VPNs**
  - Cisco Easy VPN, 235
  - DMVPN, 236
  - GRE (generic routing encapsulation), 236
  - IPsec, 234
  - IPsec direct encapsulation, 234-235
  - IPsec VTI, 237
  - L2TPv3, 237
  - service provider VPNs versus, 233-239
- enterprise WAN architectures, 241-244**
  - Cisco Enterprise MAN/WAN architecture, 243
  - comparison of, 243-244
- enterprise WAN components, 245-247**
- enterprise WAN submodule in Cisco Enterprise Architecture model, 53-54**



EoIP tunnels in wireless LAN design, 181

Erlangs, 528-529

EtherChannel, 89

Ethernet, benefits of handoffs at customer edge, 238

Ethernet design rules, 83

EU Data Protection Directive 95/46/EC, 449

exam engine, 617-618

exams

- study plan, 616-618
- study tools, 613-616

existing network, characterizing, 17-23

explicit configuration, 59

exterior routing protocols, interior routing protocols versus, 350-351

extranet VPNs, 233

## F

---

facilities in data center design, 128-129

Falcon Communications scenarios, 608-610

Fast Ethernet design rules, 84-86

FCAPS (network management processes), 578

fields in IPv4 headers, 270-271

filtering routes, 421-422

firewall ACLs, 487-488

fixed delays in IP telephony networks, 552-553

flat routing protocols, hierarchical routing protocols versus, 353

fragmentation in IPv4 headers, 274-275

Frame Relay for WANs, 208-209

frequencies (WLANs), 156-157

full-mesh networks, 62

full-mesh topology in WAN design, 231

## G

---

gatekeepers, scalability with, 545-546

generic routing encapsulation (GRE), 236

Gigabit Ethernet design rules, 86-87

GLBA (Gramm-Leach-Bliley Act), 449

GLBP, 61

global aggregatable addresses in IPv6, 316

global unicast addresses in IPv6, 314-315

globally unique addresses in IPv6, assigning, 323

GoS (grade of service), 528

grade of service (GoS), 528

Gramm-Leach-Bliley Act (GLBA), 449

GRE (generic routing encapsulation), 236

ground-start signaling, 522-523

## H

---

H.264 standard in VoIP, 547

H.323 standard in VoIP, 544-547

hardware

- enterprise LAN design, 89-94
  - bridges*, 91
  - device comparison chart*, 94
  - hubs*, 90-91
  - Layer 3 switches*, 93-94
  - repeaters*, 90
  - routers*, 92-93
  - switches*, 91-92
- enterprise WAN design, 245-247
- ISR G2 security hardware options, 499

headers

- IPv4, 268-275
  - fields*, 270-271
  - fragmentation*, 274-275

*protocol numbers, 270*

*ToS field, 271-274*

IPv6, 309-311

**Hello timers in OSPFv2, 392-393**

**hexadecimal equivalents of binary numbers, 672**

**hexadecimal format for subnet masks, 283**

**hexadecimal numbers**

converting binary to, 672

converting decimal to, 668-670

converting to binary, 672-673

converting to decimal, 670

decimal equivalents of, 668

representation of, 668

**hierarchical network models, 40-46**

access layer, 43-44

*campus LAN design best practices, 96*

*enterprise data center design, 136-137*

benefits of, 40-41

Cisco Enterprise Architecture model  
hierarchical layers, 44-45

core layer, 41-42

*campus LAN design best practices, 98-99*

*enterprise data center design, 139-140*

distribution layer, 42-43

*campus LAN design best practices, 96-98*

*enterprise data center design, 138-139*

examples of, 45-46

resources for information, 65

route manipulation on, 422

**hierarchical routing protocols, flat routing protocols versus, 353**

**high availability network services, 58-65**

link media redundancy, 64-65

resources for information, 65

route redundancy, 62-63

server redundancy, 61-62

WAN design, 240-241

wireless LAN design, 176-178

workstation-to-router redundancy,  
59-61

**HIPAA (U.S. Health Insurance  
Portability and Accountability Act),  
449**

**hop count, 356-357**

**host-to-host transport layer (TCP/IP  
architecture), 666**

**H-REAP in branch LAN design, 184-185**

**HSRP, 60-61**

**hub-and-spoke topology in WAN design,  
230-231**

**hubs, 90-91**

**hybrid deployment model, IPv4 to IPv6,  
330**

**hybrid REAP in branch LAN design,  
184-185**

## I

**iBGP, 406-407**

**ICMPv6, 320**

**identity, defined, 464**

**identity and access control deployments,  
489-490**

**IEEE 802.1P networks, 556-557**

**IEEE 802.1X-2001 port-based  
authentication, 159**

**IEEE 802.3 networks, design rules, 83**

**IEEE 802.3ab-1999 networks, design  
rules, 86**

**IEEE 802.3ae networks, design rules, 88**

- IEEE 802.3u-1995 networks, design rules, 84-86
- IEEE 802.3z-1998 networks, design rules, 86
- IEEE 802.11 wireless LAN standards, 155-156
- IEEE 802.11i networks, 158
- IGMP (Internet Group Management Protocol), 108, 425-426
- IGMP snooping, 109, 427
- IGMPv1, 425
- IGMPv2, 425-426
- IGMPv3, 426
- Implement phase (PPDIOO life cycle), 14
- infrastructure protection, 471-472
- infrastructures. *See* enterprise architectures
- Integrated Services Digital Network (ISDN), 205-206
- integrity
  - data integrity, 469-470
  - violations of, 455-456
- interface types for WLC (wireless LAN controller), 169-171
- interior routing protocols, exterior routing protocols versus, 350-351
- Internet, WAN backup over, 241
- Internet connectivity submodule in Cisco Enterprise Architecture model, 51-52
- Internet Group Management Protocol (IGMP), 108, 425-426
- Internet layer (TCP/IP architecture), 666
- intracontroller roaming in Cisco UWN, 173
- intranet VPNs, 233
- intrusion prevention, 500
- IOS security, 498
- IP addresses, binary representation of, 671
- IP DSCP values in IPv4 headers, 274
- IP precedence bit values in IPv4 headers, 272
- IP protocol numbers, 310
- IP telephony networks, 530-549
  - codecs, 539-541
    - analog-to-digital signal conversion*, 540
    - standards*, 540-541
  - components of, 532-534
  - deployment models of, 535-537
    - CallManager Express model*, 537
    - multisite WAN with centralized call processing model*, 536
    - multisite WAN with distributed call processing model*, 536-537
    - single-site deployment*, 535-536
  - design considerations, 549-562
    - bandwidth*, 550-552
    - best practices*, 560-561
    - delay components*, 552-554
    - echo cancellation*, 555
    - packet loss*, 555
    - QoS (quality of service) tools*, 555-560
    - service class recommendations*, 561-562
    - VAD*, 550-551
  - design goals of, 534-535
  - resources for information, 562-563
  - subnets for, 288
  - video deployment, 537-539
  - VoIP (voice over IP), 531-532
  - VoIP control and transport protocols, 541-549
    - DHCP, DNS, TFTP*, 542
    - H.264 standard*, 547

*H.323 standard, 544-547*

*MGCP, 544*

*RTP and RTCP, 543*

*SCCP, 542*

*SIP, 548-549*

**IPsec, 234**

**IPsec direct encapsulation, 234-235**

**IPsec VTI, 237**

**IPT. See IP telephony networks**

**IPv4**

addressing, 275-295

*assignment and name resolution, 290-295*

*classes, 276-278*

*NAT (Network Address Translation), 279-282*

*private addresses, 279*

*subnets, 282-290*

*types of, 278*

comparison with IPv6, 333-334

EIGRP, 373

header, 268-275

*fields, 270-271*

*fragmentation, 274-275*

*protocol numbers, 270*

*ToS field, 271-274*

IPv4 to IPv6 transition and deployment, 326-333

*comparison of, 332*

*dual-stack deployment model, 329*

*dual-stack transitions, 326*

*hybrid deployment model, 330*

*IPv6 over IPv4 tunnels, 326-328*

*protocol translation, 328-329*

*service block deployment model, 330*

multicast, 423-431

multicast addresses, 423-424

resources for information, 296

routing protocols, IPv6 routing protocols versus, 354

**IPv4-compatible IPv6 addresses, 312, 316**

**IPv6**

addressing, 311-319

*allocations, 313-314*

*anycast addresses, 316-317*

*assignment strategies, 322-324*

*global aggregatable addresses, 316*

*global unicast addresses, 314-315*

*IPv4-compatible IPv6 addresses, 312, 316*

*link-local addresses, 315*

*loopback addresses, 314*

*multicast addresses, 317-319*

*prefixes, 312-313, 319*

*representation of addresses, 311-313*

*unicast addresses, 314-316*

*unique local addresses, 315-316*

benefits of, 308-309

comparison with IPv4, 333-334

EIGRP, 373-374

header, 309-311

ICMPv6, 320

IPv4 to IPv6 transition and deployment, 326-333

*comparison of, 332*

*dual-stack deployment model, 329*

*dual-stack transitions, 326*

*hybrid deployment model, 330*

*IPv6 over IPv4 tunnels, 326-328*

*protocol translation, 328-329*

*service block deployment model, 330*

multicast, 423-431

- multicast addresses, 423-424, 430-431
- name resolution, 321-322
- ND (Neighbor Discovery) protocol, 320-321
- path MTU discovery, 322
- resources for information, 334-335
- routing protocols, 325-326, 354
- security, 324
- IronPort ESA (Email Security Appliances), 493-494**
- IronPort WSA (Web Security Appliances), 494**
- ISDN (Integrated Services Digital Network), 205-206**
- ISDN BRI service, 205, 524**
- ISDN PRI service, 205-206, 524**
- IS-IS for IPv6, 325**
- ISM frequencies, 156-157**
- ISR G2 security hardware options, 499**
- ISR versus ISR G2 features, 249**
- IVR systems, 528**

## J

---

- joining PIM-SM, 429

## K

---

- keys (encryption), 467

## L

---

- L2TPv3 (Layer 2 Tunneling Protocol Version 3), 237**
- LAN high availability protocols, 59-61**
  - ARP, 59
  - explicit configuration, 59
  - GLBP, 61
  - HSRP, 60-61

- RDP, 59
- RIP, 59-60
- VRRP, 61
- LAN media in enterprise LAN design, 82-89**
  - 10 Gigabit Ethernet design rules, 88
  - campus media comparison chart, 89
  - EtherChannel, 89
  - Ethernet design rules, 83
  - Fast Ethernet design rules, 84-86
  - Gigabit Ethernet design rules, 86-87
- large branch design in enterprise branch architectures, 252-253**
- large-building LAN design, 101-102**
- Layer 2 access method in WLANs, 157**
- Layer 2 intercontroller roaming in Cisco UWN, 173-174**
- Layer 2 Tunneling Protocol Version 3 (L2TPv3), 237**
- Layer 3 intercontroller roaming in Cisco UWN, 174**
- Layer 3 switches, 93-94**
- Layer 3-to-Layer 2 mapping of multicast addresses, 424**
- layered communication example (TCP/IP architecture), 666-667**
- LEAP, 159**
- leased-line WANs, 230**
- legislation concerning security, 448-449**
- LFI in VoIP, 557**
- Lightweight Access Point Protocol (LWAPP), 162, 166-167**
- link characteristics in WAN design, 216-217**
- link efficiency in WAN design, 220**
- link media redundancy, 64-65**
- link-local addresses in IPv6, 315, 322-323**
- link-state routing protocols, 352-353**

- LLQ in VoIP, 557-559
- load balancing, 62, 240
- load for routing protocols, 358-359
- local loops in voice networks, 519-520
- local MAC support
  - in branch LAN design, 184
  - in Cisco UWN, 164
- local preference attribute in BGP, 411
- logical link sublayer (OSI model), 663
- loop prevention for routing protocols, 360-361
- loopback addresses, 288, 314
- loop-start signaling, 522
- low-latency queueing in WAN design, 219
- LSA types
  - in OSPFv2, 396-397
  - in OSPFv3, 401-403
- LWAPP (Lightweight Access Point Protocol), 162, 166-167

## M

---

- MAC addresses, binary representation of, 671
- MAC sublayer (OSI model), 663
- Management Information Base (MIB), 580-581
- masks. *See* subnets (IPv4)
- maximum transmission unit (MTU), 360
- MD5 authentication in RIPv2, 362
- MED attribute in BGP, 412-413
- media. *See* LAN media in enterprise LAN design
- medium branch design in enterprise branch architectures, 250-251
- medium-size LANs, campus LAN design best practices, 103

## memory tables

- 10 Gigabit Ethernet media types, 88
- accelerating access to applications and services, 13
- AND logical operation, 285
- AP modes, 166
- campus LAN application type requirements, 95, 103
- campus LAN application types, 95
- campus layer design best practices, 100
- campus media comparison chart, 89
- campus security, 502-503
- CAS and CCS signaling types, 524
- characterizing the network, 23
- Cisco Enterprise Architecture model enterprise modules, 58
- Cisco Enterprise Architecture model hierarchical layers, 44-45
- Cisco IOS integrated security, 498
- Cisco router/switch platform and software comparison, 247
- Cisco UWN (Unified Wireless Network) architecture, 161
- codec standards, 541
- collision domains for 100BASE-T Ethernet, 85
- common bits within Class C networks, 417
- continuous security steps, 462
- country codes, list of, 526-527
- data center core drivers, 139
- data center facility considerations, 129
- data center security, 504
- default administrative distances for IP routes, 355
- default EIGRP values for bandwidth and delay, 371
- design document contents, 25
- DHCP allocation mechanisms, 292

- DHCP and DNS servers, 294
- distance-vector versus link-state routing protocols, 352
- DNS resource records, 294
- domains of trust, 464
- DoS (denial of service) attacks, managing, 454
- DSCP AF packet-drop precedence values, 273
- DSCP and IP precedence values in IPv4 headers, 273
- DTMF frequencies, 526
- EIGRP protocol characteristics, 375
- enterprise architectures, benefits of, 10-11
- enterprise edge security, 505
- Ethernet handoffs at customer edge, benefits of, 238
- H.264 video bandwidth, 547
- H.323 protocols, 547
- high-order bits of IPv4 address classes, 276
- IGP and EGP protocol selection, 351
- improving business agility, 12
- increasing network availability, 12
- IP address allocation for VoIP networks, 288
- IP DSCP values, 274
- IP precedence bit values, 272
- IP protocol numbers, 310
- IPT functional areas, 534
- IPv4 address classes, 278
- IPv4 address types, 278
- IPv4 and IPv6 routing protocols, 354
- IPv4 default network address masks, 282
- IPv4 private address space, 279
- IPv4 protocol numbers, 270
- IPv6 address autoconfiguration scheme, 324
- IPv6 address prefixes, 319
- IPv6 address types, 319
- IPv6 and IPv4 characteristics, 334
- IPv6 deployment model comparison, 332
- IPv6 deployment models, list of, 333
- IPv6 mechanisms, 324-325
- IPv6 prefix allocation, 314
- IronPort WSA modes, 494
- ISR versus ISR G2 features, 249
- LAN device comparison chart, 94
- link efficiency in WAN design, 220
- lowering cost of ownership, 12
- LSA header S2 S1 bits, 402
- major LSA types, 396-397
- major router types, 395
- multicast addresses, 424
- multicast scope assignments, 318
- NAT concepts, 282
- NetFlow output descriptions, 21
- network delays, 554
- network management elements, 578
- network management protocol comparison, 589
- network security life cycle, 457
- network virtualization design considerations, 145
- OSPF interface costs, 392
- OSPFv3 LSA types, 402-403
- packet loss sensitivities, 538
- PPDIOO life cycle phases, 15
- public versus private addresses (IPv4), 281
- QoS considerations, 217
- QoS scheme summary in IPT design, 560



- redundancy models, 65
- risk index calculation, 461
- RMON1 groups, 584
- RMON2 groups, 585
- routing protocol characteristics, 356
- routing protocols on hierarchical network infrastructure, 422
- scalability constraints for Gigabit Ethernet networks, 86
- scalability constraints for IEEE 802.3 networks, 83
- security legislation, 449
- security policy documents, 459
- security risks, 453
- security threats, 450
- service class recommendations, 562
- SNMP message types, 582
- SNMP security levels, 583
- subnet masks, 283
- summarization of networks, 418
- syslog message levels, 588
- top-down approach to network design, 24
- ToS field values, 272
- UDP ports used by WLAN protocols, 186
- video media application models, 538
- virtualization key drivers, 141
- VoIP bandwidth requirements, 550-551
- VoIP protocols, 549
- VPN protocols, 468-469
- WAN application requirements, 214
- WAN bandwidth comparisons, 215
- WAN link characteristics, 216
- WAN transport technology comparison, 205
- WAN/MAN architecture comparison, 243

- well-known IPv6 multicast addresses, 318-319, 431
- wireless mesh components, 182
- WLAN controller platforms, 167, 171
- WLAN design considerations, 183
- WLAN standards summary, 157
- WLC components, 169
- WLC interface types, 170-171
- WLC redundancy, 178

### **message format**

- in RIPng, 365-366
- in RIPv2, 363-364

### **message levels (syslog protocol), 588**

### **message types (SNMP), 582**

### **metrics**

- default metric in route redistribution, 420-421
- in EIGRP, 370-371
- in OSPFv2, 391-392
- for routing protocols, 356-361
  - bandwidth*, 357
  - cost*, 358
  - delay*, 359
  - hop count*, 356-357
  - load*, 358-359
  - loop prevention*, 360-361
  - MTU parameter*, 360
  - reliability*, 359

### **Metro Ethernet, 209, 237-238**

### **MGCP in VoIP, 544**

### **MIB (Management Information Base), 580-581**

### **mobility groups in Cisco UWN, 174-176**

### **MPLS (multiprotocol label switching), 211, 238-239**

### **MPLS Layer 3, 239**

### **MPPP (Multilink Point-to-Point Protocol), 65**



MTU (maximum transmission unit), 360

multicast addresses, 423-424

- in IPv6, 317-319, 430-431
- Layer 3-to-Layer 2 mapping, 424

multicast distribution trees, 428

multicast traffic, 423-431

- campus LAN design best practices, 108-109
- CGMP (Cisco Group Management Protocol), 426-427
- DVMRP, 430
- IGMP, 425-426
- IGMP snooping, 427
- PIM, 428-430
- sparse versus dense, 427-428

Multilink Point-to-Point Protocol (MPPP), 65

multiprotocol label switching (MPLS), 211, 238-239

multiservice networks. *See* IP telephony networks

multisite WAN with centralized call processing deployment model for IP telephony networks, 536

multisite WAN with distributed call processing deployment model for IP telephony networks, 536-537

## N

---

N+1 WLC redundancy, 176

N+N WLC redundancy, 177

N+N+1 WLC redundancy, 177

name resolution

- in IPv4, 290-295
  - ARP, 295
  - DNS, 292-294
- in IPv6, 321-322

NAT (Network Address Translation), 279-282

ND (Neighbor Discovery) protocol in IPv6, 320-321

neighbor discovery and recovery in EIGRP, 368

Neighbor Discovery (ND) protocol in IPv6, 320-321

neighbors in BGP, 405-406

NetFlow, 21, 585-587

Network Address Translation (NAT), 279-282

network analysis tools, 22

network architectures. *See* enterprise architectures

network audit tools, 18-21

network availability, increasing, 12, 62-63. *See also* DoS (denial of service) attacks

network checklist, 22-23

network delays. *See* delay components in IP telephony networks

network design. *See also* campus LAN design; enterprise LAN design; WAN design

- borderless network architecture, 58
- Cisco Enterprise Architecture model, 47-58
  - e-commerce submodule*, 50-51
  - enterprise campus module*, 48-50
  - enterprise edge area*, 50-54
  - enterprise WAN submodule*, 53-54
  - Internet connectivity submodule*, 51-52
  - remote modules*, 55-57
  - resources for information*, 65
  - service provider edge module*, 54-55
  - VPN/remote access submodule*, 52-53

- customer requirements, identifying, 15-17
- design document, 25-26
- enterprise architectures.
  - See enterprise architectures
- existing network, characterizing, 17-23
- hierarchical network models, 40-46
  - access layer*, 43-44
  - benefits of*, 40-41
  - Cisco Enterprise Architecture model hierarchical layers*, 44-45
  - core layer*, 41-42
  - distribution layer*, 42-43
  - examples of*, 45-46
  - resources for information*, 65
- high availability network services, 58-65
  - link media redundancy*, 64-65
  - resources for information*, 65
  - route redundancy*, 62-63
  - server redundancy*, 61-62
  - workstation-to-router redundancy*, 59-61
- PPDIOO life cycle.
  - See PPDIOO life cycle
- prototype and pilot tests, 24-25
- resources for information, 26
- security policies in, 462
- top-down approach, 23-25
- network devices, security integration with**, 497-502
  - Catalyst 6500 service modules, 500-502
  - Cisco security appliances, 499-500
  - endpoint security, 502
  - intrusion prevention, 500
  - IOS security, 498
  - ISR G2 security hardware options, 499
- network interface layer (TCP/IP architecture)**, 666

- network layer (OSI model)**, 663-664
- network life cycle**. See PPDIOO life cycle
- network management**
  - CDP (Cisco Discovery Protocol), 587
  - comparison of protocols, 589
  - elements of, 578
  - FCAPS, 578
  - NetFlow, 585-587
  - resources for information, 589-590
  - RMON1, 583-584
  - RMON2, 584-585
  - SNMP (Simple Network Management Protocol), 579-583
    - components of*, 579-580
    - MIB (Management Information Base)*, 580-581
    - SNMPv1*, 581-582
    - SNMPv2*, 582
    - SNMPv3*, 582-583
  - syslog protocol, 588-589
- network portion of address, determining**, 285
- network requirements**.
  - See customer requirements
- network security**. See security
- network virtualization**, 142, 144-145
- next-hop attribute in BGP**, 411
- nibbles**, 672
- NSSAs in OSPFv2**, 398-399
- numbering plan (PSTN)**, 526-527

## O

---

- octets**, 672
- Open Shortest Path First**. See OSPFv2; OSPFv3

**Open Systems Interconnection model.**  
     See OSI (Open Systems Interconnection) model

**Operate phase (PPDIOO life cycle), 14**

**Optimize phase (PPDIOO life cycle), 14**

**optional attributes in BGP, 411**

**ordering WAN transport technologies, 212-213**

**origin attribute in BGP, 411-412**

**OSI (Open Systems Interconnection) model, 661-665**

- application layer, 665
- data link layer, 663
- layered communication example, 666-667
- network layer, 663-664
- physical layer, 662
- presentation layer, 665
- session layer, 664
- TCP/IP architecture mapping to, 665
- transport layer, 664

**OSPFv2, 391-400**

- adjacencies and Hello timers, 392-393
- areas, 393
- autonomous system external path types, 397
- characteristics of, 400
- DRs, 395-396
- LSA types, 396-397
- metrics, 391-392
- NSSAs, 398-399
- route redistribution, 421
- router authentication, 399
- router types, 394-395
- stub area types, 397-398
- virtual links, 399

**OSPFv3, 325, 400-404**

- areas and router types, 401
- changes from OSPFv2, 400-401

- characteristics of, 404
- LSA types, 401-403
- route redistribution, 421

**outdoor wireless with wireless mesh design, 181-182**

**output descriptions in NetFlow, 21**

**overheating in data center design, 132-133**

## P

---

**packet loss sensitivities, 538, 555**

**packet types in EIGRP, 371-372**

**packet-switched WANs, 230**

**partial-mesh networks, 63**

**partial-mesh topology in WAN design, 231-232**

**passwords, defined, 464**

**path attributes in BGP, 410-413**

**path isolation in network virtualization design, 145**

**path MTU discovery in IPv6, 322**

**Payment Card Industry Data Security Standard (PCI DSS), 449**

**PBR (policy-based routing), 416**

**PBX, PSTN switches versus, 518-519.**  
     *See also* voice networks

**PCI DSS (Payment Card Industry Data Security Standard), 449**

**Pearland Hospital scenario, 599-604**

**Pearson Cert Practice Test engine, 617-618**

**phases in PPDIOO life cycle, 15**

**physical layer (OSI model), 662**

**physical security, 470-471**

**pilot network tests, 24-25**

**PIM, 428-430**

**PIM DR, 429**

**PIM-SM, 429**

**PIMv2 bootstrap routers**, 430  
**Plan phase (PPDIOO life cycle)**, 14  
**platforms**  
     for network security, 485-486  
     for security management, 495-496  
**poison reverse**, 361  
**policies**. *See* security policies  
**policing in WAN design**, 219  
**policy-based routing (PBR)**, 416  
**port scanning tools**, 450-451  
**ports in voice networks**, 520-521  
**power usage in data center design**, 131-132  
**PPDIOO life cycle**, 11-15  
     accelerating access to applications and services, 13  
     benefits of, 11  
     design methodology, 15  
     Design phase, 14  
     Implement phase, 14  
     improving business agility, 12  
     increasing network availability, 12  
     lowering cost of ownership, 12  
     Operate phase, 14  
     Optimize phase, 14  
     phases in, 15  
     Plan phase, 14  
     Prepare phase, 13  
     in WAN design, 213  
**precedence bit values in IPv4 headers**, 272  
**prefixes in IPv6 addresses**, 312-314, 319  
**Prepare phase (PPDIOO life cycle)**, 13  
**presentation layer (OSI model)**, 665  
**priority queueing in WAN design**, 218  
**private addresses (IPv4)**, 279-282

**processing delay in IP telephony networks**, 553  
**profiles, enterprise branch architectures**, 248-249  
**propagation delay in IP telephony networks**, 553  
**protocol numbers, IPv4 headers**, 270  
**protocol translation, IPv4 to IPv6**, 328-329  
**protocol-dependent modules in EIGRP**, 368  
**protocols**. *See also* routing protocols  
     VoIP control and transport protocols, 541-549  
         *DHCP, DNS, TFTP*, 542  
         *H.264 standard*, 547  
         *H.323 standard*, 544-547  
         *MGCP*, 544  
         *RTP and RTCP*, 543  
         *SCCP*, 542  
         *SIP*, 548-549  
     VPN protocols, 467-469  
**prototype network tests**, 24-25  
**pruning PIM-SM**, 429  
**PSTN**. *See also* voice networks  
     call detail records (CDR), 528  
     Centrex services, 528  
     described, 518  
     numbering plan, 526-527  
     PBX switches versus, 518-519  
     voice mail, 528  
**public addresses (IPv4), private addresses (IPv4) versus**, 280-282

## Q

---

**QoS (quality of service)**  
     campus LAN design best practices, 106-107

in IPT design, 555-560

*Auto QoS*, 559

*cRTP*, 556

*IEEE 802.1P*, 556-557

*LFI*, 557

*LLQ*, 557-559

*RSVP*, 557

in WAN design, 217

**Q.SIG signaling**, 524-525

## R

---

**rack servers in data center design**, 128

**radio management in wireless LAN design**, 178-180

RF groups, 179

RF site surveys, 179-180

**RDP**, 59

**REAP in branch LAN design**, 184

**reconnaissance**, 450

port scanning tools, 450-451

vulnerability scanning tools, 451-452

**redistribution of routes**, 419-421

default metric, 420-421

OSPF redistribution, 421

**redundancy. See high availability network services**

**Regional Internet Registries (RIR)**, 276

**reliability**

for routing protocols, 359

in WAN design, 215

**remote modules in Cisco Enterprise Architecture model**, 55-57

**remote-access network design**, 232

**repeaters**

100BASE-T Ethernet, 85-86

enterprise LAN design, 90

**requirements, application requirements in WAN design**, 214

**resource records (DNS)**, 294

**Resource Reservation Protocol (RSVP) in VoIP**, 557

**resources for information**

campus LAN design, 109

CCDA exam updates, 657-658

Cisco Enterprise Architecture model, 65

enterprise data center design, 145-146

enterprise LAN design, 109

hierarchical network models, 65

high availability network services, 65

IP telephony networks, 562-563

IPv4, 296

IPv6, 334-335

network design, 26

network management, 589-590

OSI (Open Systems Interconnection) model, 675

routing protocols, 375-376, 431-432

security, 473, 507

TCP/IP architecture, 675

voice networks, 562-563

WAN design, 255

WANs (wide area networks), 220

WLANs (wireless LANs), 186

**response time in WAN design**, 214

**RF groups in wireless LAN design**, 179

**RF site surveys in wireless LAN design**, 179-180

**RIP**, 59-60

**RIPng**, 325, 362, 365-367

authentication, 365

characteristics of, 366-367

design, 366

message format, 365-366

timers, 365

**RIPv2, 362**

- authentication, 362
- characteristics of, 364-365
- design, 364
- message format, 363-364
- routing database, 362
- timers, 364

**RIR (Regional Internet Registries), 276****risk assessments, 459-460****risk index calculation, 460-461****risks to security, 453****RMON1, 583-584, 586-587****RMON2, 584-587****roaming in Cisco UWN, 173-176****route manipulation, 416-422**

- filtering, 421-422
- on hierarchical network infrastructure, 422
- PBR (policy-based routing), 416
- redistribution, 419-421
  - default metric, 420-421*
  - OSPF redistribution, 421*
- summarization, 416-419

**route redundancy, 62-63****route reflectors in BGP, 407-409****routed hierarchical network designs, 45****router authentication in OSPFv2, 399****router types**

- in OSPFv2, 394-395
- in OSPFv3, 401

**routers in enterprise LAN design, 92-93****routing database in RIPv2, 362****routing protocols**

- administrative distance, 355-356
- BGP, 404-416
  - administrative distance, 409*
  - characteristics of, 415-416*

- confederations, 409*

- decision process, 414-415*

- eBGP, 406*

- iBGP, 406-407*

- neighbors, 405-406*

- path attributes, 410-413*

- route reflectors, 407-409*

- weight, 414*

- classless versus classful routing protocols, 353-354

- design characteristics of, 348, 356

- distance-vector routing protocols, 351-353

**EIGRP, 351-352, 367-375**

- characteristics of, 375*

- components of, 367*

- design, 372*

- DUAL and, 368-369*

- for IPv4, 373*

- for IPv6, 373-374*

- metrics, 370-371*

- neighbor discovery and recovery, 368*

- packet types, 371-372*

- protocol-dependent modules, 368*

- RTP and, 368*

- timers, 369-370*

- on hierarchical network infrastructure, 422

- hierarchical versus flat routing protocols, 353

- interior versus exterior protocols, 350-351

- IPv4 versus IPv6 routing protocols, 354

- in IPv6, 325-326

- link-state routing protocols, 352-353

- list of, 349-350

## metrics, 356-361

*bandwidth, 357**cost, 358**delay, 359**hop count, 356-357**load, 358-359**loop prevention, 360-361**MTU parameter, 360**reliability, 359*

## OSPFv2, 391-400

*adjacencies and Hello timers, 392-393**areas, 393**autonomous system external path types, 397**characteristics of, 400**DRs, 395-396**LSA types, 396-397**metrics, 391-392**NSSAs, 398-399**router authentication, 399**router types, 394-395**stub area types, 397-398**virtual links, 399*

## OSPFv3, 400-404

*areas and router types, 401**changes from OSPFv2, 400-401**characteristics of, 404**LSA types, 401-403*resources for information,  
375-376, 431-432

## RIPng, 362, 365-367

*authentication, 365**characteristics of, 366-367**design, 366**message format, 365-366**timers, 365*

## RIPv2, 362

*authentication, 362**characteristics of, 364-365**design, 364**message format, 363-364**routing database, 362**timers, 364*static versus dynamic assignment,  
348-350RSVP (Resource Reservation Protocol)  
in VoIP, 557

## RTCP in VoIP, 543

## RTP

EIGRP and, 368

in VoIP, 543

---

**S**

## Sarbanes-Oxley (SOX), 449

## scalability constraints

for Gigabit Ethernet networks, 86

for IEEE 802.3 networks, 83

## scalability with gatekeepers, 545-546

## scanning tools

port scanning, 450-451

vulnerability scanning, 451-452

## SCCP in VoIP, 542

## scenarios

Beauty Things Store, 606-608

Big Oil and Gas, 604-606

Falcon Communications, 608-610

Pearland Hospital, 599-604

## SCF (Security Control Framework), 486

## secure connectivity, 466-470

data integrity, 469-470

encryption, 466-467

transmission confidentiality, 469

VPN protocols, 467-469

**security**

- Cisco SAFE (Security Architecture for the Enterprise), 484-486
- Cisco SCF (Security Control Framework), 486
- DoS (denial of service) attacks, 454-455
- enterprise security, 502-506
  - campus security*, 502-503
  - data center security*, 503-504
  - enterprise edge and WAN security*, 504-506
- integration with network devices, 497-502
  - Catalyst 6500 service modules*, 500-502
  - Cisco security appliances*, 499-500
  - endpoint security*, 502
  - intrusion prevention*, 500
  - IOS security*, 498
  - ISR G2 security hardware options*, 499
- integrity violations and confidentiality breaches, 455-456
- in IPv6, 324
- legislation concerning, 448-449
- management solutions, 472, 495-496
- network security life cycle, 457
- overview, 448
- platforms for, 485-486
- port scanning tools, 450-451
- resources for information, 473, 507
- risks, 453
- secure connectivity, 466-470
  - data integrity*, 469-470
  - encryption*, 466-467
  - transmission confidentiality*, 469
  - VPN protocols*, 467-469

- security policies, 456-462
  - components of*, 459
  - continuous security*, 461-462
  - creating*, 458
  - defined*, 457-458
  - in network design*, 462
  - purpose of*, 458
  - risk assessments*, 459-460
  - risk index calculation*, 460-461
- targets, 453-454
- threat defense, 470-472
  - infrastructure protection*, 471-472
  - physical security*, 470-471
- threat detection and mitigation, 490-494
- threat types, 450
- trust and identity management, 462-466
  - access control*, 466
  - certificates*, 465
  - domains of trust*, 463-464
  - identity*, *defined*, 464
  - passwords*, 464
  - technologies for*, 486-490
  - tokens*, 464-465
  - trust*, *defined*, 463
- unauthorized access, 452-453
- vulnerability scanning tools, 451-452
- in WLANs, 157-160
- security appliances**, 499-500
- Security Control Framework (SCF)**, 486
- security levels (SNMP)**, 583
- security policies**, 456-462
  - components of*, 459
  - continuous security*, 461-462
  - creating*, 458
  - defined*, 457-458
  - in network design*, 462



- purpose of, 458
- risk assessments, 459-460
- risk index calculation, 460-461
- serialization delay in IP telephony networks, 553**
- server connectivity options, campus LAN design best practices, 105**
- server deployment challenges in data center design, 127-135**
  - cabling, 133-135
  - cooling, 132-133
  - facilities, 128-129
  - power usage, 131-132
  - space allotment, 130
- server farms, campus LAN design best practices, 104**
- server redundancy, 61-62**
- server virtualization, 144**
- servers, WLAN access control, 159-160**
- service access, accelerating, 13**
- service block deployment model, IPv4 to IPv6, 330**
- service class recommendations in IPT design, 561-562**
- service provider edge module in Cisco Enterprise Architecture model, 54-55**
- service provider VPNs**
  - enterprise VPNs versus, 233-239
  - Metro Ethernet, 237-238
  - MPLS, 238-239
  - MPLS Layer 3, 239
  - VPLS, 238
- service set identifier (SSID), 157**
- services edge in network virtualization design, 145**
- session layer (OSI model), 664**
- shared distribution trees, 428**
- show version command, 20-21**
- signaling types in voice networks, 521-526**
  - addressing digit signaling, 526
  - CAS and CCS signaling, 524
  - E&M signaling, 523-524
  - ground-start signaling, 522-523
  - ISDN PRI/BRI service, 524
  - loop-start signaling, 522
  - Q.SIG signaling, 524-525
  - SS7 signaling, 525
  - T1/E1 CAS signaling, 524
- single-site deployment model for IP telephony networks, 535-536**
- SIP in VoIP, 548-549**
- small and remote site LANs, campus LAN design best practices, 103-104**
- small branch design in enterprise branch architectures, 250**
- SNMP (Simple Network Management Protocol), 579-583**
  - components of, 579-580
  - MIB (Management Information Base), 580-581
  - NetFlow versus, 586-587
  - SNMPv1, 581-582
  - SNMPv2, 582
  - SNMPv3, 582-583
- SNMPv1, 581-582**
- SNMPv2, 582**
- SNMPv3, 582-583**
- software, enterprise WAN design, 245-247**
- SONET/SDH, 209-210**
- source distribution trees, 428**
- SOX (Sarbanes-Oxley), 449**
- space allotment in data center design, 130**
- Spanning Tree Protocol (STP), 91**

sparse multicast distribution, dense multicast distribution versus, 427-428  
 split horizon, 360  
 split-MAC architecture in Cisco UWN, 163-164  
 SS7 signaling, 525  
 SSID (service set identifier), 157  
 stateless autoconfiguration  
   of globally unique IPv6 addresses, 323  
   of link-local IPv6 addresses, 322-323  
 static IP addressing, 290-291  
 static routes, dynamic routes versus, 348-350  
 STP (Spanning Tree Protocol), 91  
 stub area types in OSPFv2, 397-398  
 study plan, 616-618  
 study tools, 613-616  
 subnet mask values for binary numbers, 675  
 subnets (IPv4), 282-290  
   default network address masks, 282  
   design, 283-284  
   IP telephony networks, 288  
   loopback addresses, 288  
   network portion of address, determining, 285  
   representation of, 283  
   variable-length subnet masks (VLSM), 286-288  
 subnetting practice, 616-617  
 summarization in routing protocols, 361, 416-419  
 switched hierarchical network designs, 45  
 switches  
   enterprise LAN design, 91-92  
   PSTN versus PBX, 518-519  
 syslog protocol, 588-589

## T

---

T1/E1 CAS signaling, 524  
 tables. *See* memory tables  
 targets of security threats, 453-454  
 TCP/IP architecture, 665-667  
   application layer, 666  
   host-to-host transport layer, 666  
   Internet layer, 666  
   layered communication example, 666-667  
   network interface layer, 666  
   OSI (Open Systems Interconnection) model mapping to, 665  
 TDM (time-division multiplexing), 209  
 teleworkers. *See* enterprise teleworker architectures  
 tests, prototype and pilot network tests, 24-25  
 TFTP in VoIP, 542  
 threats  
   defense against, 470-472  
     *infrastructure protection*, 471-472  
     *physical security*, 470-471  
   detection and mitigation, 490-494  
   types of, 450  
 throughput in WAN design, 214-215  
 time-division multiplexing (TDM), 209  
 timers  
   in EIGRP, 369-370  
   in OSPFv2, 392-393  
   in RIPng, 365  
   in RIPv2, 364  
 tokens, defined, 464-465  
 tools  
   network analysis tools, 22  
   network audit tools, 18-21

- port scanning tools, 450-451
- vulnerability scanning tools, 451-452
- top-down approach to network design, 23-25**
- topologies**
  - Data Center 3.0 topology components, 127
  - WAN design, 230-232
    - full-mesh topology, 231*
    - hub-and-spoke topology, 230-231*
    - partial-mesh topology, 231-232*
- ToS field in IPv4 headers, 271-274**
  - DSCP AF packet-drop precedence values, 273
  - DSCP and IP precedence values, 273
  - IP DSCP values, 274
  - IP precedence bit values, 272
  - values, 272
- totally stubby areas in OSPFv2, 398**
- traditional voice architectures, 518-530**
  - ACD, 528
  - blocking probability, 530
  - busy hour, 529
  - busy-hour traffic (BHT), 529-530
  - call detail records (CDR), 528, 530
  - Centrex services, 528
  - Centum call second (CCS), 529
  - Erlangs, 528-529
  - grade of service (GoS), 528
  - IVR systems, 528
  - local loops and trunks, 519-520
  - ports, 520-521
  - PSTN
    - described, 518*
    - numbering plan, 526-527*
    - PBX switches versus, 518-519*
  - signaling types, 521-526
    - addressing digit signaling, 526*
    - CAS and CCS signaling, 524*
    - E&M signaling, 523-524*
    - ground-start signaling, 522-523*
    - ISDN PRI/BRI service, 524*
    - loop-start signaling, 522*
    - Q.SIG signaling, 524-525*
    - SS7 signaling, 525*
    - T1/E1 CAS signaling, 524*
  - voice mail, 528
- traffic shaping in WAN design, 219**
- transition mechanisms, IPv4 to IPv6, 326-333**
  - dual-stack transitions, 326
  - IPv6 over IPv4 tunnels, 326-328
  - protocol translation, 328-329
- transmission confidentiality, 469**
- transport layer (OSI model), 664**
- transport technologies for WANs, 204-213**
  - cable, 206-207
  - comparison of, 205
  - dark fiber cabling, 211-212
  - DSL, 206
  - DWDM, 212
  - Frame Relay, 208-209
  - ISDN, 205-206
  - Metro Ethernet, 209
  - MPLS, 211
  - ordering, 212-213
  - SONET/SDH, 209-210
  - TDM, 209
  - wireless, 207-208
- triggered updates, 361**
- trunks in voice networks, 519-520**

**trust**

- defined, 463
- domains of, 463-464

**trust and identity management, 462-466**

- access control, 466
- certificates, 465
- domains of trust, 463-464
- identity, defined, 464
- passwords, 464
- technologies for, 486-490
- tokens, 464-465
- trust, defined, 463

**tunneling, IPv6 over IPv4 tunnels, 326-328. *See also* VPNs (virtual private networks)**

---

**U****UDP ports, WLAN protocols and, 186****unauthorized access, 158, 450, 452-453.  
*See also* access control****unicast addresses in IPv6, 314-316****unified computing as Data Center 3.0 component, 126****unified fabric as Data Center 3.0 component, 126****UNII frequencies, 156-157****unique local addresses in IPv6, 315-316****updates to CCDA exam, 657-658****U.S. Health Insurance Portability and Accountability Act (HIPAA), 449**

---

**V****VAD in IPT design, 550-551****variable delays in IP telephony networks, 553-554****variable-length subnet masks (VLSM), 286-288****video deployment over IP telephony networks, 537-539****virtual links in OSPFv2, 399****Virtual Port Channel (vPC), 143****Virtual Private LAN Services (VPLS), 238****virtual private networks. *See* VPNs (virtual private networks)****virtual routing and forwarding (VRF), 143****Virtual Switching System (VSS), 45-46, 98, 143****virtual tunnel interface (VTI), 237****virtualization, 141-145**

- benefits of, 141-142
- challenges, 141
- as Data Center 3.0 component, 126
- design considerations, 144-145
- technologies for, 143-144
- types of, 142

**VLSM (variable-length subnet masks), 286-288****voice bandwidth, calculating, 551-552****voice mail, 528****voice networks**

- IP telephony networks, 530-549
  - codecs, 539-541*
  - components of, 532-534*
  - deployment models of, 535-537*
  - design considerations, 549-562*
  - design goals of, 534-535*
  - video deployment, 537-539*
  - VoIP (voice over IP), 531-532*
  - VoIP control and transport protocols, 541-549*

**resources for information, 562-563****traditional voice architectures, 518-530*****ACD, 528******blocking probability, 530***

- busy hour*, 529
  - busy-hour traffic (BHT)*, 529-530
  - call detail records (CDR)*, 528, 530
  - Centrex services*, 528
  - Centum call second (CCS)*, 529
  - Erlangs*, 528-529
  - grade of service (GoS)*, 528
  - IVR systems*, 528
  - local loops and trunks*, 519-520
  - ports*, 520-521
  - PSTN, described*, 518
  - PSTN numbering plan*, 526-527
  - PSTN versus PBX switches*, 518-519
  - signaling types*, 521-526
  - voice mail*, 528
  - VoIP (voice over IP)**, 531-532
    - control and transport protocols, 541-549
      - DHCP, DNS, TFTP*, 542
      - H.264 standard*, 547
      - H.323 standard*, 544-547
      - MGCP*, 544
      - RTP and RTCP*, 543
      - SCCP*, 542
      - SIP*, 548-549
  - vPC (Virtual Port Channel)**, 143
  - VPLS (Virtual Private LAN Services)**, 238
  - VPN/remote access submodule in Cisco Enterprise Architecture model**, 52-53
  - VPNs (virtual private networks)**
    - benefits of, 239
    - Cisco Easy VPN, 235
    - DMVPN, 236
    - enterprise VPN versus service provider VPN, 233-239
    - GRE (generic routing encapsulation), 236
    - IPsec, 234
      - IPsec direct encapsulation, 234-235
      - IPsec VTI, 237
      - L2TPv3, 237
      - Metro Ethernet, 237-238
      - MPLS, 238-239
      - MPLS Layer 3, 239
      - network design, 232-233
      - protocols, 467-469
      - VPLS, 238
    - VRF (virtual routing and forwarding), 143
    - VRRP, 61
    - VSS (Virtual Switching System), 45-46, 98, 143
    - vulnerability scanning tools, 451-452
- 
- ## W
- 
- WAN design**, 202, 213-220
    - application requirements, 214
    - bandwidth comparisons, 215-216
    - class-based weighted fair queueing, 218-219
    - classification, 218
    - congestion management, 218
    - custom queueing, 218
    - enterprise branch architectures, 248-253
      - design rules*, 248
      - ISR versus ISR G2 features*, 249
      - large branch design*, 252-253
      - medium branch design*, 250-251
      - profiles*, 248-249
      - small branch design*, 250
    - enterprise teleworker architectures, 254-255
    - enterprise WAN architectures, 241-244
      - Cisco Enterprise MAN/WAN architecture*, 243
      - comparison of*, 243-244

- enterprise WAN components, 245-247
- link characteristics, 216-217
- link efficiency, 220
- low-latency queueing, 219
- priority queueing, 218
- QoS (quality of service), 217
- redundancy, 240-241
- reliability, 215
- remote-access network design, 232
- resources for information, 220, 255
- response time, 214
- throughput, 214-215
- topologies, 230-232
  - full-mesh topology*, 231
  - hub-and-spoke topology*, 230-231
  - partial-mesh topology*, 231-232
- traditional technologies for, 230-232
- traffic shaping and policing, 219
- VPNs (virtual private networks)
  - benefits of*, 239
  - Cisco Easy VPN*, 235
  - DMVPN*, 236
  - enterprise VPN versus service provider VPN*, 233-239
  - GRE (generic routing encapsulation)*, 236
  - IPsec*, 234
  - IPsec direct encapsulation*, 234-235
  - IPsec VTI*, 237
  - L2TPv3*, 237
  - Metro Ethernet*, 237-238
  - MPLS*, 238-239
  - MPLS Layer 3*, 239
  - network design*, 232-233
  - VPLS*, 238
- weighted fair queueing, 218
- window size, 220

## WANs (wide area networks).

- See also* WAN design
- connection modules, 203-204
- defined, 202
- enterprise WAN submodule in Cisco Enterprise Architecture model, 53-54
- resources for information, 220
- security for, 504-506
- transport technologies, 204-213
  - cable*, 206-207
  - comparison of*, 205
  - dark fiber cabling*, 211-212
  - DSL*, 206
  - DWDM*, 212
  - Frame Relay*, 208-209
  - ISDN*, 205-206
  - Metro Ethernet*, 209
  - MPLS*, 211
  - ordering*, 212-213
  - SONET/SDH*, 209-210
  - TDM*, 209
  - wireless*, 207-208
- watts, BTU conversion, 133
- Web sites, CCDA exam updates, 657
- weight in BGP, 414
- weighted fair queueing in WAN design, 218
- well-known attributes in BGP, 410
- well-known IPv6 multicast addresses, 318-319, 431
- wide area networks. *See* WANs (wide area networks)
- window size in WAN design, 220
- wireless LAN design, 176-186
  - branch LAN design, 184-186
  - H-REAP*, 184-185
  - local MAC support*, 184

- REAP*, 184
- UDP ports used in*, 186
- campus LAN design, 183-184
- EoIP tunnels, 181
- outdoor wireless with wireless mesh design, 181-182
- radio management, 178-180
  - RF groups*, 179
  - RF site surveys*, 179-180
- resources for information, 186
- WLC redundancy design, 176-178
- wireless LANs (WLANs). *See* WLANs (wireless LANs)
- wireless mesh for outdoor wireless, 181-182
- wireless technologies for WANs, 207-208
- WLANs (wireless LANs).**
  - See also* wireless LAN design
  - Cisco UWN (Unified Wireless Network), 160-176
    - AP controller equipment scaling*, 171
    - AP modes*, 164-166
    - architectures*, 160-161
    - authentication*, 167-169
    - CAPWAP*, 163
    - local MAC support*, 164
    - LWAPP*, 162
    - LWAPP discovery of WLC*, 166-167
    - roaming*, 173-176
    - split-MAC architecture*, 163-164
    - WLC components*, 169
    - WLC interface types*, 169-171
  - controller platforms, 167, 171
  - ISM and UNII frequencies, 156-157
  - Layer 2 access method, 157
  - resources for information, 186
  - security, 157-160
  - SSID (service set identifier), 157
  - standards, 155-157
- WLC (wireless LAN controller)**
  - components, 169
  - interface types, 169-171
  - LWAPP discovery of, 166-167
  - redundancy design, 176-178
- workstation-to-router redundancy,** 59-61
  - ARP, 59
  - explicit configuration, 59
  - GLBP, 61
  - HSRP, 60-61
  - RDP, 59
  - RIP, 59-60
  - VRRP, 61