CISCO

Official Cert Guide

Learn, prepare, and practice for exam success

- 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

CCDA
640-864

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

ciscopress.com

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

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

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. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact:
U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact:
International Sales 1-317-581-3793 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

Associate Publisher: David Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Andrew Cupp

Senior Project Editor: Tonya Simpson

Cover Designer: Sandra Schroeder

Indexer: Cheryl Lenser

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editors: David Morgan and Farai Tafa

Copy Editor: Keith Cline

Book Designer: Gary Adair

Publishing Coordinator: Vanessa Evans

Composition: Mark Shirar

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

Elements Available on the CD

Contents

Elements Available on the CD

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.

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.

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

Exam Topic	Part
Describe the Methodology Used to Design a Network	
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
Describe Network Structure and Modularity	
Describe the network hierarchy	I
Describe the modular approach in network design	I
Describe network architecture for the enterprise	II
Design Basic Enterprise Campus Networks	
Describe Campus Design considerations	II
Design the enterprise campus network	II
Design the enterprise data center	II
Describe enterprise network virtualization tools	II
Design Enterprise Edge and Remote Network Modules	
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
Design IP Addressing and Routing Protocols	
Describe IPv4 addressing	III
Describe IPv6 addressing	III
Identify Routing Protocol Considerations in an Enterprise Network	III
Design a routing protocol deployment	III

Design Network Services	
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).

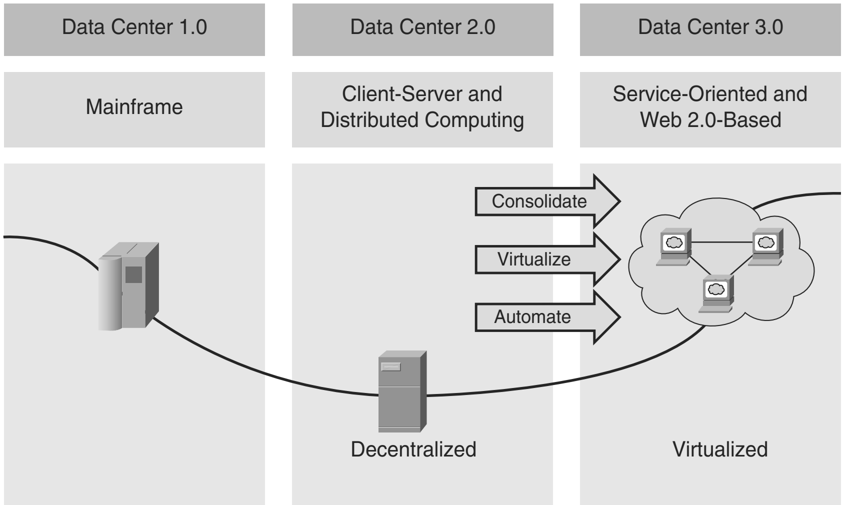

Figure 4-1 *Cisco Data Center Architecture Evolution*

Data Center 3.0 Components

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

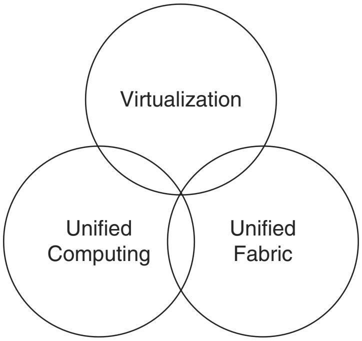

Figure 4-2 *Cisco Data Center 3.0 Architecture Framework*

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:

Key Topic

- 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.

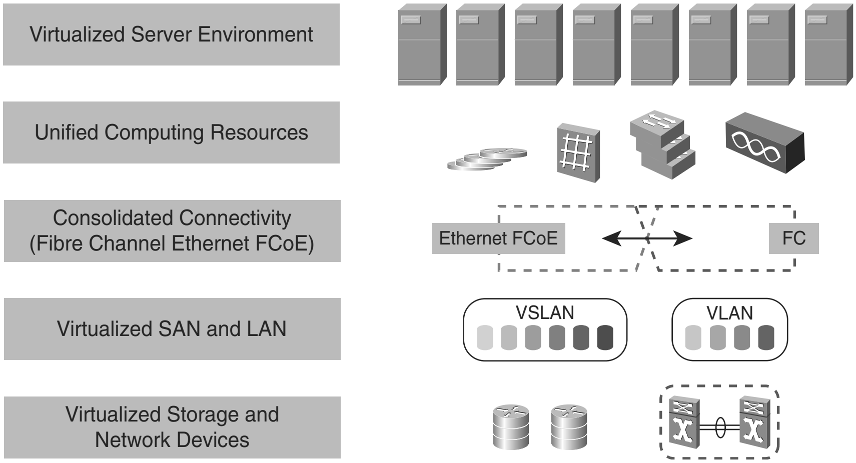

Figure 4-3 *Cisco Data Center 3.0 Topology*

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:

Key Topic

- Power required
- Physical rack space usage

- 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.

Key Topic

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*

Data Center Facility Considerations	Description
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 importance 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 place 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.

Key Topic

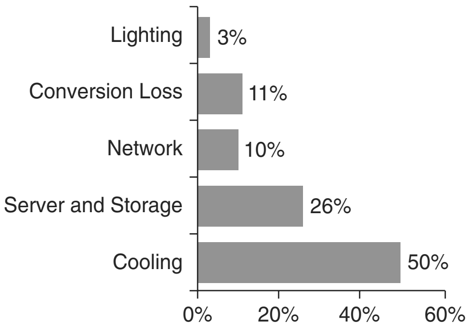

Figure 4-4 *Data Center Power Usage Example*

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.

Key Topic

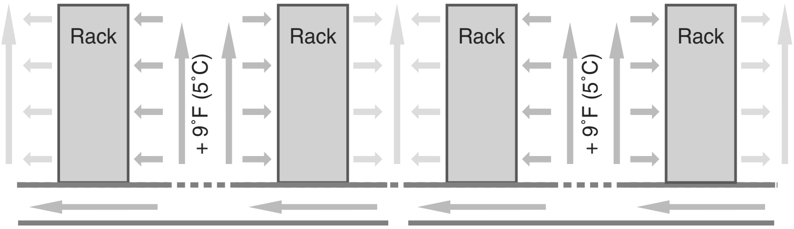

Figure 4-5 *Data Center Cold and Hot Aisles*

> **Note:** 1 watt = 3.41214 British thermal units (BTU). Many manufacturers publish kW, kilovolt ampere (kWA), 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.

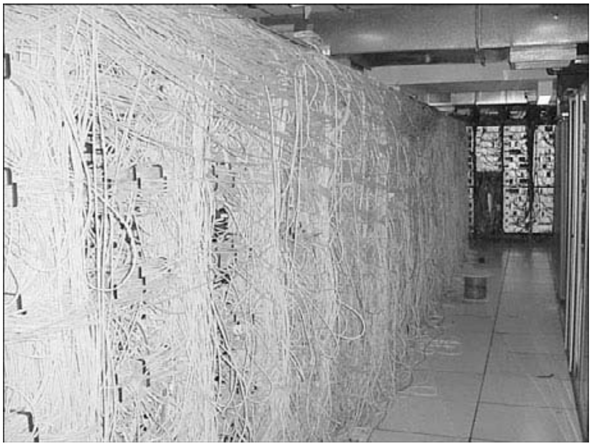

Figure 4-6 *Data Center Cabling the Wrong Way*

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

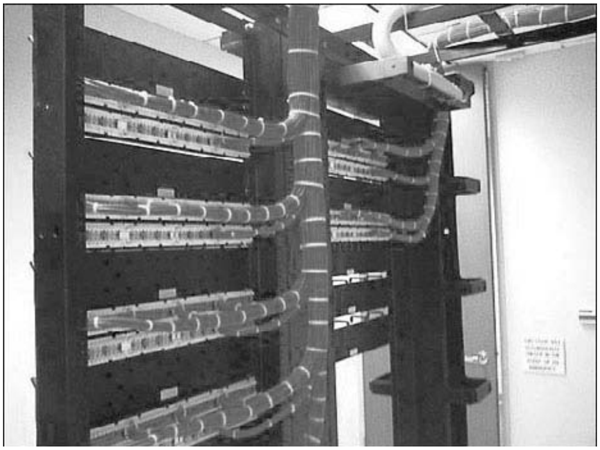

Figure 4-7 *Data Center Cabling the Right Way*

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.

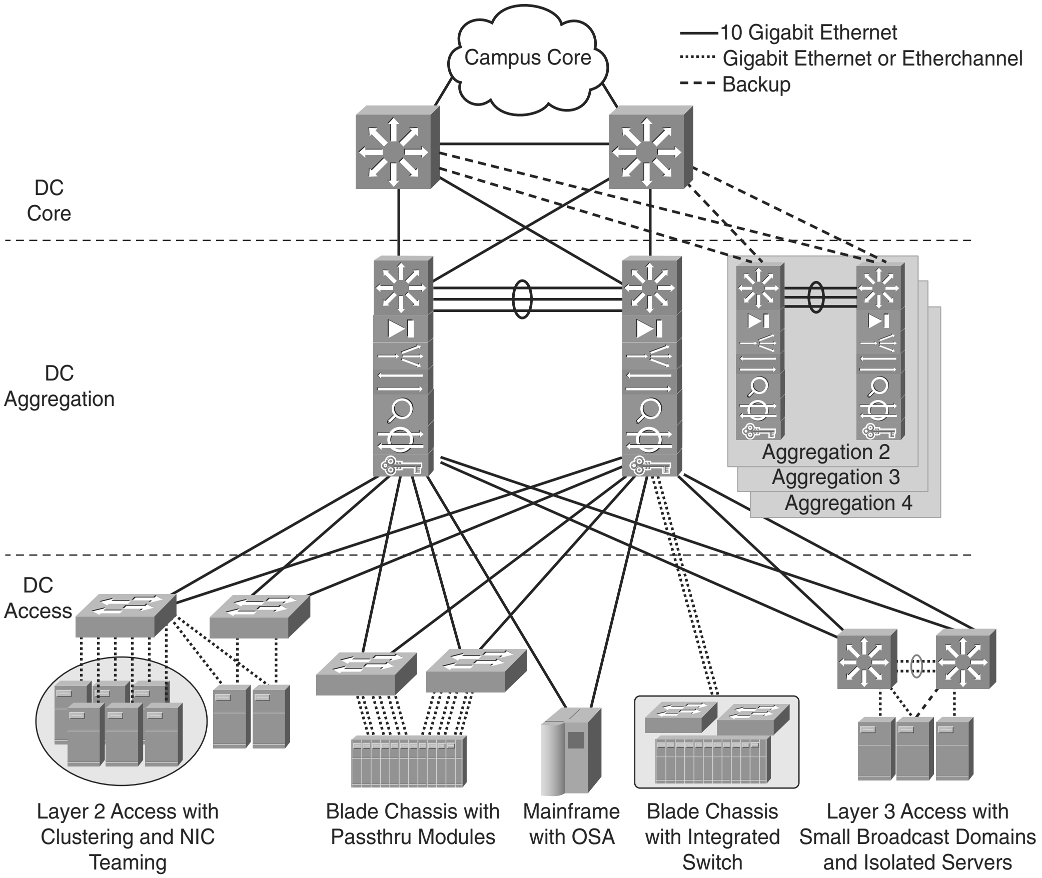

Figure 4-8 *Enterprise Data Center Infrastructure Overview*

Defining the DC Access Layer

Key Topic

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 oversubscription 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.

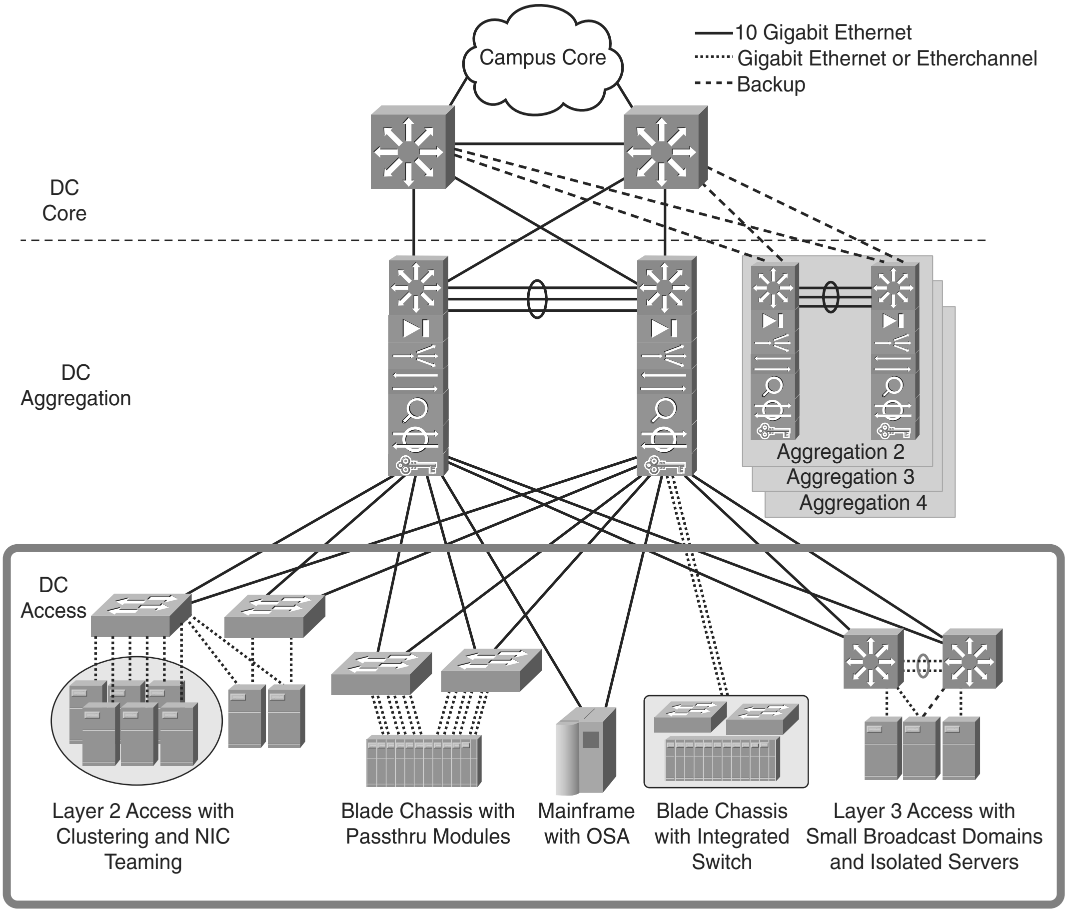

Figure 4-9 *Data Center Access Layer*

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.

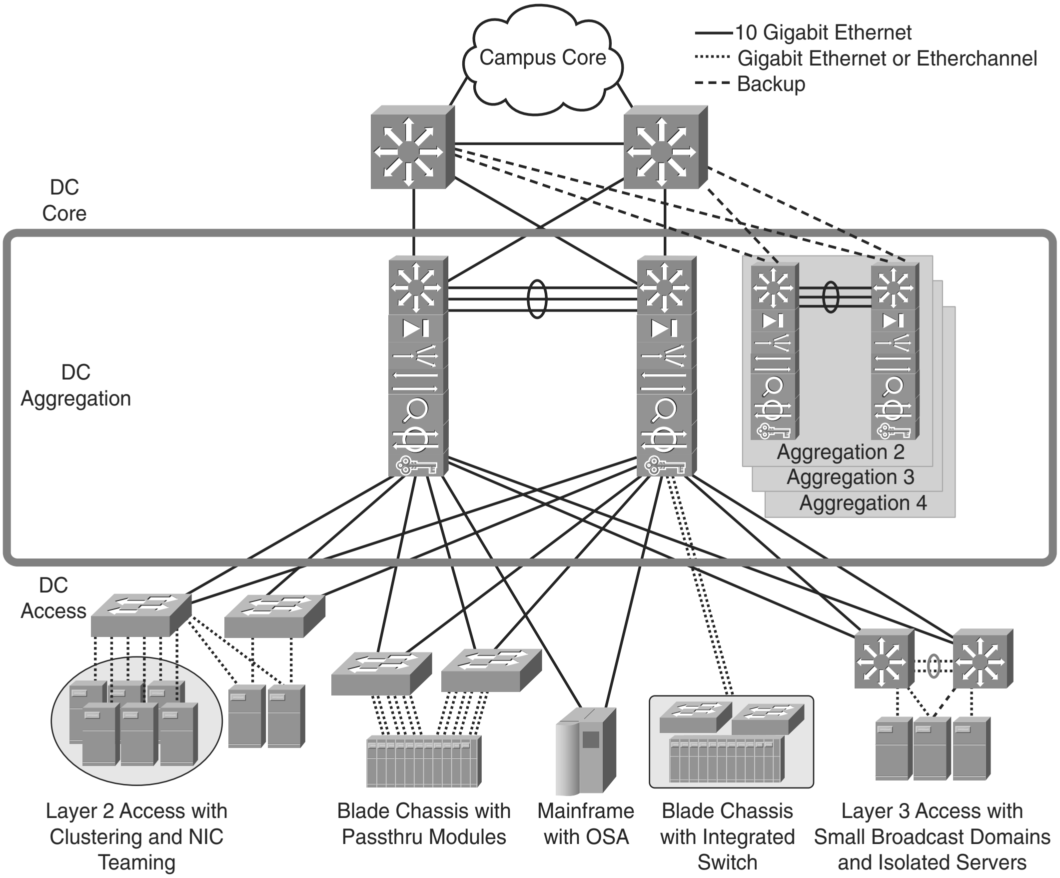

Figure 4-10 *Data Center Aggregation Layer*

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 (HRSP) 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

Key Topic

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*

Data Center Core Drivers	Description
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 sufficent core layers in the beginning.

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

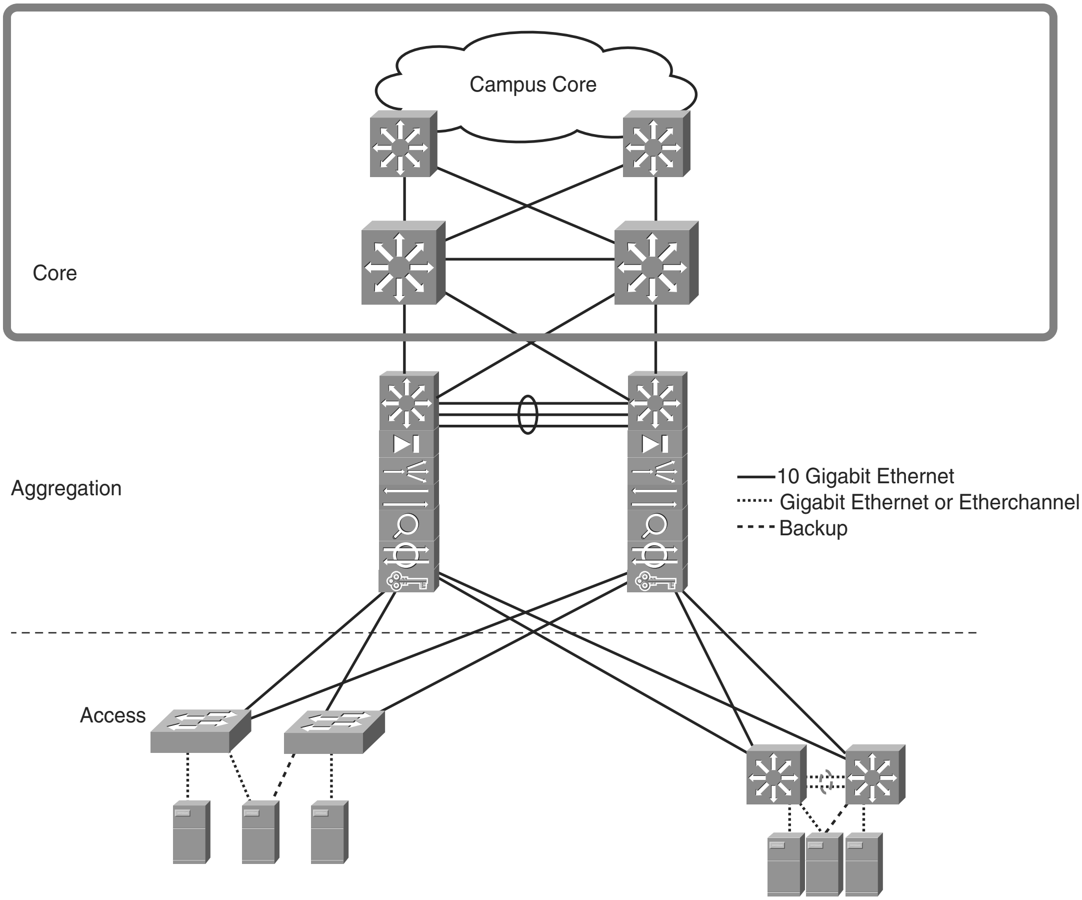

Figure 4-11 *Data Center Core Layer*

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

Key Topic

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*

Virtualization Driving Forces	Description
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:

Key Topic

- **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

Key Topic

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.

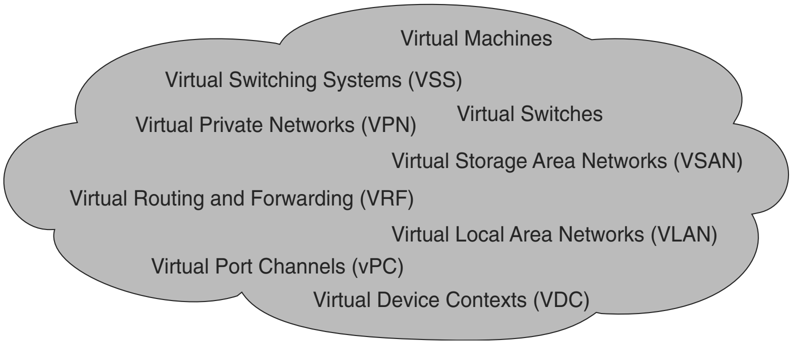

Figure 4-12 *Data Center Virtualization Technologies*

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

Key Topic

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 form 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

Key Topic

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*

Network Virtualization Consideration	Description
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.

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.

Cisco Data Center Infrastructure 2.5 Design Guide, 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.

Examples of Good Cable Management, 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	VRF, 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

A

B

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W