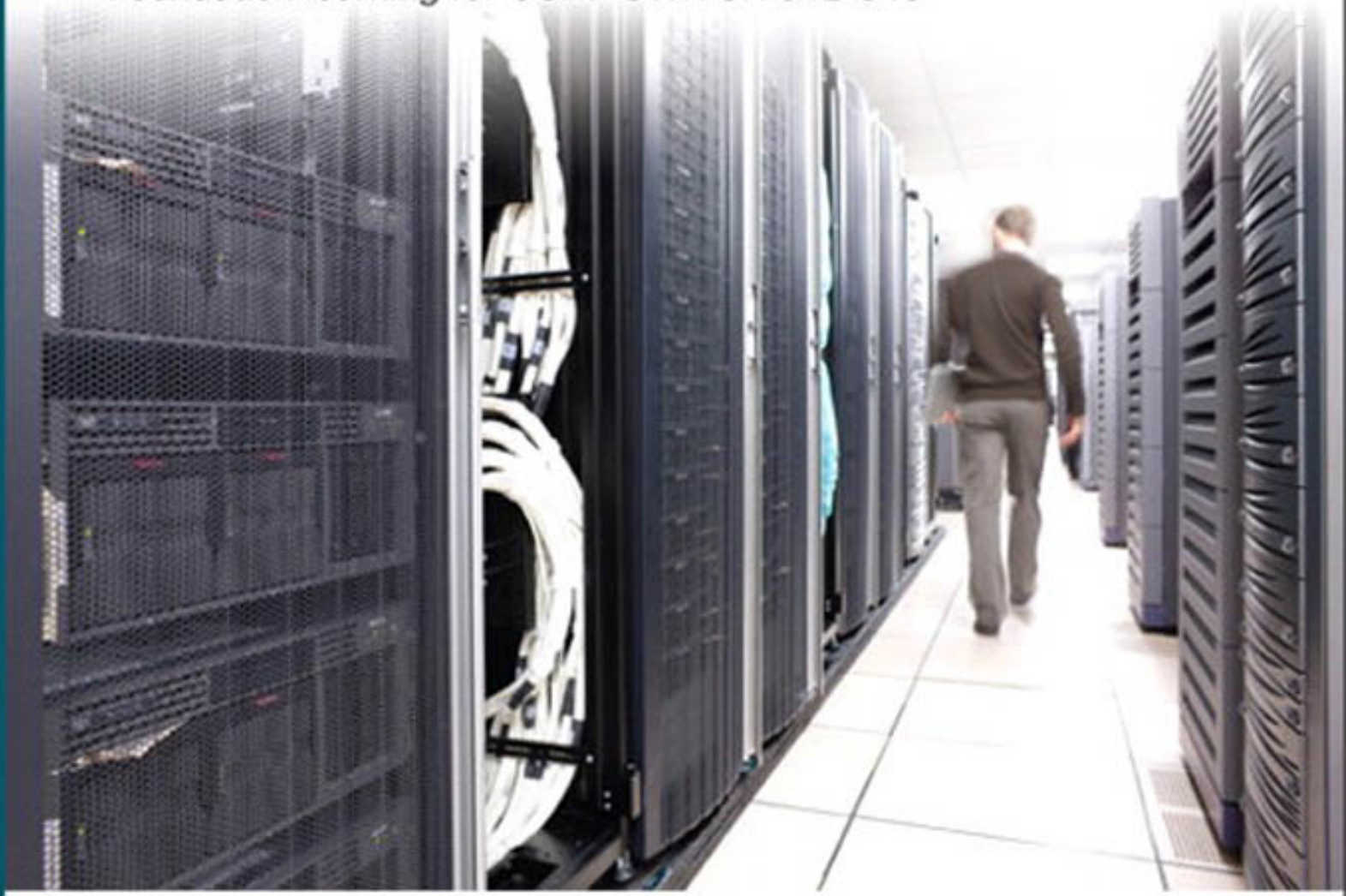
Implementing Cisco Switched Networks (SWITCH)

Foundation Learning Guide

Foundation learning for CCNP SWITCH 642-813



Richard Froom, CCIE No. 5102
Balaji Sivasubramanian • **Erum Frahim**, CCIE No. 7549

ciscopress.com

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide

Richard Froom, CCIE No. 5102
Balaji Sivasubramanian
Erum Frahim, CCIE No. 7549

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide

Richard Froom, CCIE No. 5102

Balaji Sivasubramanian

Erum Frahim, CCIE No. 7549

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

Printed in the United States of America

Fifth Printing: August 2012

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

ISBN-13: 978-1-58705-884-4

ISBN-10: 1-58705-884-7

Warning and Disclaimer

This book is designed to provide information about the Implementing Cisco IP Switched Networks (SWITCH) course in preparation for taking the SWITCH 642-813 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Feedback Information

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

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Andrew Cupp

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Cover Designer: Sandra Schroeder

Composition: Mark Shirar

Indexer: Tim Wright

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Geoff Tagg, Sonya Coker, Jeremy Creech, Rick Graziani, David Kotfila, Wayne Lewis, Jim Lorenz, Snezhy Neshkova, Allan Reid, Bob Vachon

Copy Editor: Apostrophe Editing Services

Proofreader: Sheri Cain

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Authors

Richard E. Froom, CCIE No. 5102, attended Clemson University where he majored in computer engineering. While attending Clemson, Richard held positions at different times for the university network team, IBM, and Scientific Research Corporation. After graduation, Richard joined Cisco. Richard's first role within Cisco was as a TAC engineer supporting Cisco Catalyst switches. After several years in the TAC, Richard moved into a testing role supporting Cisco MDS and SAN technologies. In 2009, Richard moved into the Enhanced Customer Aligned Testing Services (ECATS) organization within Cisco as a test manager of a team focused on testing customer deployments of UCS and Nexus.

Balaji Sivasubramanian is a product line manager in the Cloud Services and Switching Technology Group focusing on upcoming products in the cloud services and Data Center virtualization area. Before this role, Balaji was a senior product manager for the Catalyst 6500 switches product line, where he successfully launched the Virtual Switching System (VSS) technology worldwide. He started his Cisco career in Cisco Technical Assistant Center working in the LAN switching products and technologies. Balaji has been a speaker at various industry events such as Cisco Live and VMworld. Balaji has a Master of Science degree in computer engineering from the University of Arizona and a Bachelor of Engineering degree in electrical and electronics from the College of Engineering, Guindy, Anna University (India).

Erum Frahim, CCIE No. 7549, is a technical leader working for Enhanced Customer Aligned Testing Services (ECATS) at Cisco. In her current role, Erum is leading efforts to test Datacenter solutions for several Cisco high-profile customers. Prior to this, Erum managed the Nexus platform escalation group and served as a team lead for Datacenter SAN Test lab under the Cisco Datacenter Business Unit. Erum joined Cisco in 2000 as a technical support engineer. Erum has a Master of Science degree in electrical engineering from Illinois Institute of Technology and also holds a Bachelor of Engineering degree from NED University, Karachi Pakistan. Erum also authors articles in *Certification* Magazine and Cisco.com.

About the Technical Reviewers

Geoff Tagg runs a small U.K. networking company and has worked in the networking industry for nearly 30 years. Before that, he had 15 years of experience with systems programming and management on a wide variety of installations. Geoff has clients ranging from small local businesses to large multinationals and has combined implementation with training for most of his working life. Geoff's main specialties are routing, switching, and networked storage. He lives in Oxford, England, with his wife, Christine, and family and is a visiting professor at nearby Oxford Brookes University.

Sonya Coker has worked in the Cisco Networking Academy program since 1999 when she started a local academy. She has taught student and instructor classes locally and internationally in topics ranging from IT Essentials to CCNP. As a member of the Cisco Networking Academy development team she has provided subject matter expertise on new courses and course revisions.

Jeremy Creech is a learning and development manager for Cisco with more than 13 years experience in researching, implementing, and managing data and voice networks. Currently, he is a curriculum development manager for the Cisco Networking Academy

Program leveraging his experience as the content development manager for CCNP Certification exams. He has recently completed curriculum development initiatives for ROUTE, SWITCH, TSHOOT, and CCNA Security.

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Rick has worked and taught in the computer networking and information technology field for almost 30 years. Prior to teaching Rick worked in IT for various companies including Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds a Master of Arts degree in computer science and systems theory from California State University Monterey Bay. Rick also does consulting work for Cisco and other companies. When Rick is not working, he is most likely surfing. Rick is an avid surfer who enjoys surfing at his favorite Santa Cruz breaks.

David Kotfila, CCNA, CCDA, CCNP, CCDP, CCSP, CCVP, CCAI, teaches in the computer science department at Rensselaer Polytechnic Institute, Troy, New York. More than 550 of his students have received their CCNA, 200 have received their CCNP, and 14 have received their CCIE. David likes to spend time with his wife Kate, his daughter Charis, and his son Chris. David enjoys hiking, kayaking, and reading.

Dr. Wayne Lewis has been a faculty member at Honolulu Community College since receiving a Ph.D. in math from the University of Hawaii at Manoa in 1992, specializing in finite rank torsion-free modules over a Dedekind domain. Since 1992, he served as a math instructor, as the state school-to-work coordinator, and as the legal main contact for the Cisco Academy Training Center (CATC). Dr. Lewis manages the CATC for CCNA, CCNP, and Security, based at Honolulu Community College, which serves Cisco Academies at universities, colleges, and high schools in Hawaii, Guam, and American Samoa. Since 1998, he has taught routing, multilayer switching, remote access, troubleshooting, network security, and wireless networking to instructors from universities, colleges, and high schools in Australia, Britain, Canada, Central America, China, Germany, Hong Kong, Hungary, Indonesia, Italy, Japan, Korea, Mexico, Poland, Singapore, Sweden, Taiwan, and South America both onsite and at Honolulu Community College.

Jim Lorenz is an instructor and curriculum developer for the Cisco Networking Academy Program. Jim has co-authored Lab Companions for the CCNA courses and the textbooks for the Fundamentals of UNIX course. He has more than 25 years of experience in information systems, ranging from programming and database administration to network design and project management. Jim has developed and taught computer and networking courses for both public and private institutions. As the Cisco Academy Manager at Chandler-Gilbert College in Arizona, he was instrumental in starting the Information Technology Institute (ITI) and developed a number of certificates and degree programs. Jim co-authored the CCNA Discovery online academy courses, *Networking for Home and Small Businesses* and *Introducing Routing and Switching in the Enterprise*, with Allan Reid. Most recently, he developed the hands-on labs for the CCNA Security course and the CCNPv6 Troubleshooting course.

Snezhy Neshkova, CCIE No. 11931, has been a Cisco Certified Internetwork Expert since 2003. She has more than 20 years of networking experience, including IT field services and support, management of information systems, and all aspects of networking education. Snezhy has developed and taught CCNA and CCNP networking courses to instructors from

universities, colleges, and high schools in Canada, the United States, and Europe. Snezhy's passion is to empower students to become successful and compassionate lifelong learners. Snezhy holds a Master of Science degree in computer science from Technical University, Sofia.

Allan Reid, CCNA, CCNA-W, CCDA, CCNP, CCDP, CCAI, MLS, is a professor in information and communications engineering technology and the lead instructor at the Centennial College CATC in Toronto, Canada. He has developed and taught networking courses for both private and public organizations and has been instrumental in the development and implementation of numerous certificate, diploma, and degree programs in networking. Outside his academic responsibilities, Allan has been active in the computer and networking fields for more than 25 years and is currently a principal in a company specializing in the design, management, and security of network solutions for small and medium-sized companies. Allan is a curriculum and assessment developer for the Cisco Networking Academy Program and has authored several Cisco Press titles.

Bob Vachon, CCNP, CCNA-S, CCAI, is a professor in the computer systems technology program at Cambrian College and has more than 20 years of experience in the networking field. In 2001 he began collaborating with the Cisco Networking Academy on various curriculum development projects including CCNA, CCNA Security, and CCNP courses. For 3 years Bob was also part of an elite team authoring CCNP certification exam questions. In 2007, Bob co-authored the Cisco Press book *CCNA Exploration: Accessing the WAN*.

Dedications

This book is dedicated to my wife Beth and my son Nathan. I appreciate their support for the extra time that went into completing this book. —Richard

This book is dedicated to my wife Swapna, who has been very supportive and encouraging in me writing this book. —Balaji

This book is dedicated to my husband Faraz and my dearest daughter Alisha, who were very supportive as I wrote this book. I would like to say extra thanks to my mom and grandmother for remembering me in their prayers. I would also like to dedicate this book to my niece and nephew Shayan and Shiza and a very new member Zayan, who are the love of my life, and finally, my siblings, sister-in-law, and father, who are always there to help me out in any situation. —Erum

Acknowledgments

Richard: I'd like to give special recognition to the entire Cisco Press team for the patience and support in producing this title.

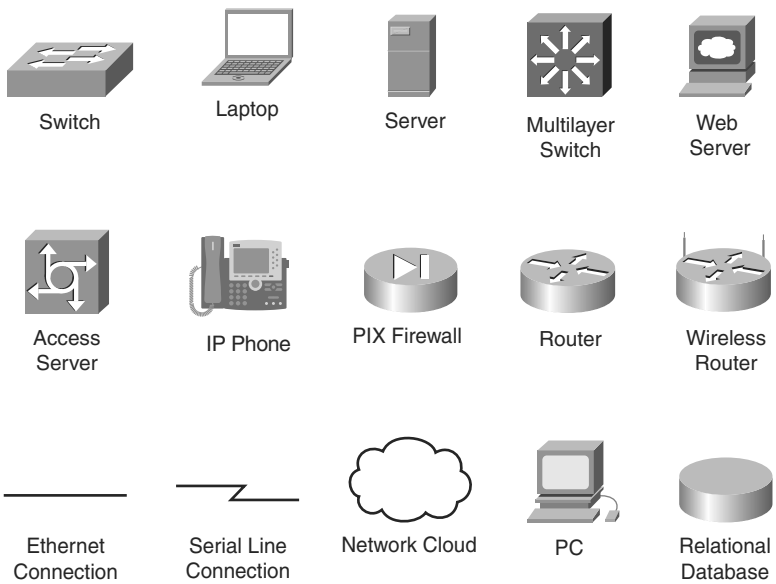
Balaji: I would like to acknowledge Mary Beth and Andrew from the Cisco Press team for their patience and support during the development of the book.

Erum: I would like to give my thanks to Cisco Press—especially to Mary Beth for being understanding during the development of the book. In addition, I would like to acknowledge all the reviewers who helped make the book more valuable.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *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

Over the past several years, switching has evolved from simple Layer 3 switches to switches supporting Layer 4 through Layer 7 features, such as server load balancing, URL inspection, firewalls, VPNs, access-based control, and so on, with large port densities. The multilayer switch has become an all-in-one component of the network infrastructure. As a result of this evolution, enterprise and service providers are deploying multilayer switches in place of multiple network components, such as routers and network appliances. Switching is no longer a part of the network infrastructure; it is now *the* network infrastructure, with wireless as the latest evolution.

As enterprises, service providers, and even consumers deploy multilayer switching, the need for experienced and knowledgeable professionals to design, configure, and support the multilayer switched networks has grown significantly. CCNP and CCDP certifications offer the ability for network professionals to prove their competency.

CCNP and CCDP are more than résumé keywords. Individuals who complete the CCNP and CCDP certifications truly prove their experience, knowledge, and competency in networking technologies. A CCNP certification demonstrates an individual's ability to install, configure, and operate LAN, WAN, and dial access services for midsize to large networks deploying multiple protocols. A CCDP certification demonstrates an individual's ability to design high-performance, scalable, and highly available routed and switched networks involving LAN, WAN, wireless, and dial access services.

Both the CCNP and CCDP certification tracks require you to pass the SWITCH 642-813 exam. For the most up-to-date information about Cisco certifications, visit the following website: www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html.

Objectives and Methods

This book's content is based on the Cisco SWITCH course that has recently been introduced as part of the CCNP curriculum; it provides knowledge and examples in the area of implementing Cisco switched networks. It is assumed that the reader possesses as much Cisco background as is covered in the Cisco ROUTE and TSHOOT courses. The content of this book is enough to prepare the reader for the SWITCH exam, too. Note that the e-learning content of the Cisco SWITCH course has been integrated into this book.

To accomplish these tasks, this text includes in-depth theoretical explanations of SWITCH topics and provides illustrative design and configuration examples. The theoretical explanations of SWITCH topics include background information, standards references, and document listings from Cisco.com. This book goes beyond just presenting the necessary information found on the certification exam and in the SWITCH course. This book attempts to present topics, theory, and examples in such a way that you truly understand the topics that are necessary to build multilayer switched networks in today's demanding networks. The examples and questions found in the chapters of this book

make you contemplate and apply concepts found in each chapter. The goal is to have you understand the topics and then apply your understanding when you attempt the certification exam or take the SWITCH course.

Chapter review questions help readers evaluate how well they absorbed the chapter content. The questions are also an excellent supplement for exam preparation.

Who Should Read This Book?

Those individuals who want to learn about modern switching techniques and want to see several relevant examples will find this book very useful. This book is most suitable for those who have some prior routing and switching knowledge but would like to learn or enhance their switching skill set. Readers who want to pass the Cisco SWITCH exam can find all the content they need to successfully do so in this book. The Cisco Networking Academy CCNP SWITCH course students use this book as their official book.

Cisco Certifications and Exams

Cisco offers four levels of routing and switching certification, each with an increasing level of proficiency: Entry, Associate, Professional, and Expert. These are commonly known by their acronyms CCENT (Cisco Certified Entry Networking Technician), CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional), and CCIE (Cisco Certified Internetworking Expert). There are others, too, but this book focuses on the certifications for enterprise networks.

For the CCNP certification, you must pass exams on a series of CCNP topics, including the SWITCH, ROUTE, and TSHOOT exams. For most exams, Cisco does not publish the scores needed for passing. You need to take the exam to find that out for yourself.

To see the most current requirements for the CCNP certification, go to Cisco.com and click **Training and Events**. There you can find out other exam details such as exam topics and how to register for an exam.

The strategy you use to prepare for the SWITCH exam might differ slightly from strategies used by other readers, mainly based on the skills, knowledge, and experience you have already obtained. For instance, if you have attended the SWITCH course, you might take a different approach than someone who learned switching through on-the-job training. Regardless of the strategy you use or the background you have, this book helps you get to the point where you can pass the exam with the least amount of time required.

How This Book Is Organized

This book is organized such that the fundamentals of multilayer switched network design are covered in the first chapters. Thereafter, the book continues with a discussion of implementation of the design features such as VLAN, Spanning Tree, and inter-VLAN routing in the multilayer switched environment. This book is organized as follows:

- **Chapter 1, "Analyzing the Cisco Enterprise Campus Architecture"**—This chapter opens with a brief introdution to Cisco campus network architectures and designs. The chapter continues with a brief review of switching terminology for campus networks, followed by an introduction to Cisco switches. The chapter then continues with a of discussion of campus design fundamentals. Lastly, the chapter closes by introducting the PPDIOO Lifecycle Approach to Network Design and Implementation.
- **Chapter 2, "Implementing VLANs in Campus Network**s"—This chapter covers implemenation of virtual LANs (VLAN) in a given campus network, including discussions on private VLANs, VTP, and 802.1Q trunking. In addition, this chapter covers implementation of EtherChannel in an enterpruse network.
- **Chapter 3, "Implementing Spanning Tree"**—This chapter discusses the various Spanning Tree protocols, such as PVRST+ and MST, with overview and configuration samples. This chapter also continues the discussion with advanced Cisco STP enhancements and spanning-tree troubleshooting methodology.
- **Chapter 4, "Implementing Inter-VLAN Routing"**—This chapter transitions into discussing Layer 3 switching by covering inter-VLAN routing. The chapter then continues with the discussion on Dynamic Host Configuration Protocol (DHCP). In addition, it discusses Cisco Express Forwarding (CEF)–based multilayer switching.
- **Chapter 5, "Implementing High Availability and Redundancy in a Campus Network"**—This chapter covers the introduction to high availability in campus networks, followed by methodology on how to build resilient networks. This chapter continues to describe the tools available to monitor high availability such as SNMP and IP Service Level Agreement (SLA). This chapter concludes with available high availability options for switch supervisor engine and gateway redundancy protocols such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP).
- **Chapter 6, "Securing the Campus Infrastructure"**—This chapter covers the potential campus security risks and how to mitigate them through features such as DCHP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard. The chapter then continues to cover how to secure the switch device, and troubleshooting tools and techniques such as Switched Port Analyzer (SPAN) and Remote SPAN.

- **Chapter 7, "Preparing the Campus Infrastructure for Advanced Services"**—This chapter discusses the application of advanced services to Cisco switches. The three main services discussed in this chapter are IP telephony (voice), video, and wireless. Moreover, because these advanced services require additional switch features for implementation, topics such as QoS and IP multicast are also discussed.
- **Appendix A, "Answers to Chapter Review Questions"**—This appendix provides answers for the review questions that appear at the end of each chapter.

Chapter 1

Analyzing the Cisco Enterprise Campus Architecture

This chapter covers the following topics:

- Introduction to Enterprise Campus Network Design
- Enterprise Campus Design
- PPDIOO Lifecycle Approach to Network Design and Implementation

Over the last half century, businesses have achieved improving levels of productivity and competitive advantages through the use of communication and computing technology. The enterprise campus network has evolved over the last 20 years to become a key element in this business computing and communication infrastructure. The interrelated evolution of business and communications technology is not slowing, and the environment is currently undergoing another stage of evolution. The complexity of business and network requirements creates an environment where a fixed model no longer completely describes the set of capabilities and services that comprise the enterprise campus network today.

Nevertheless, designing an enterprise campus network is no different than designing any large, complex system—such as a piece of software or even something as sophisticated as the international space station. The use of a guiding set of fundamental engineering principles serves to ensure that the campus design provides for the balance of availability, security, flexibility, and manageability required to meet current and future business and technological needs. This chapter introduces you to the concepts of enterprise campus designs, along with an implementation process that can ensure a successful campus network deployment.

Introduction to Enterprise Campus Network Design

Cisco has several different design models to abstract and modularize the enterprise network. However, for the content in this book the enterprise network is broken down into the following sections:

- Core Backbone
- Campus
- Data Center
- Branch/WAN
- Internet Edge

Figure 1-1 illustrates at a high level a sample view of the enterprise network.

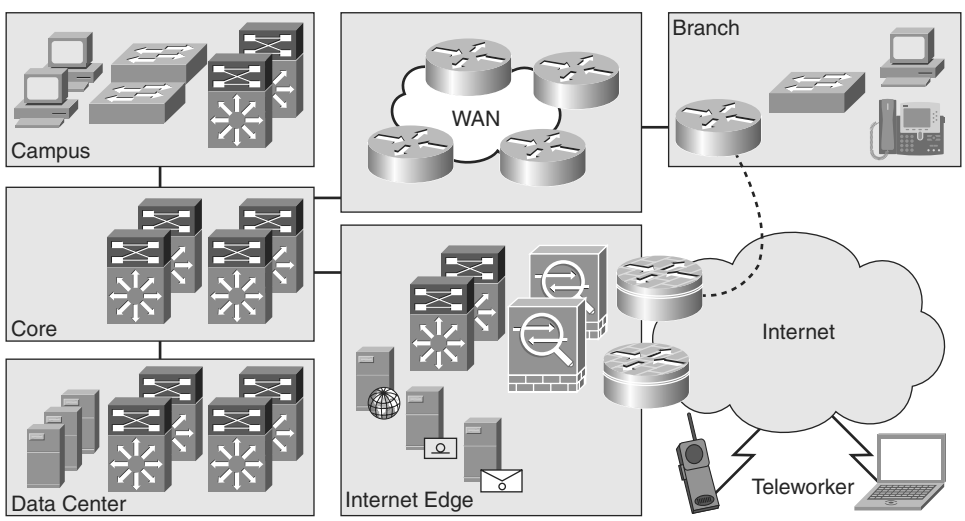


Figure 1-1 *High-Level View of the Enterprise Network*

The campus, as a part of the enterprise network, is generally understood as that portion of the computing infrastructure that provides access to network communication services and resources to end users and devices spread over a single geographic location. It might span a single floor, a building, or even a large group of buildings spread over an extended geographic area. Some networks have a single campus that also acts as the core or backbone of the network and provides interconnectivity between other portions of the overall network. The campus core can often interconnect the campus access, the data center, and WAN portions of the network. In the largest enterprises, there might be multiple campus sites distributed worldwide with each providing both end-user access and local backbone connectivity. Figure 1-1 depicts the campus and the campus core as separate functional areas. Physically, the campus core is generally self contained. The campus itself may be

physically spread out through an enterprise to reduce the cost of cabling. For example, it might be less expensive to aggregate switches for end-user connectivity in wiring closets dispersed throughout the enterprise.

The data center, as a part of the enterprise network, is generally understood to be a facility used to house computing systems and associated components. Examples of computing systems are servers that house mail, database, or market data applications. Historically, the data center was referred to as the server farm. Computing systems in the data center are generally used to provide services to users in the campus, such as algorithmic market data. Data center technologies are evolving quickly and imploring new technologies centered on virtualization. Nonetheless, this book focuses exclusively on the campus network of the enterprise network; consult Cisco.com for additional details about the Cisco data center architectures and technologies.

Note The campus section of the enterprise network is generally understood as that portion of the computing infrastructure that provides access to network communication services and resources to end users and devices spread over a single geographic location.

The data center module of the enterprise network is generally understood to be a facility used to house computing systems and associated components.

Note For the remainder of this text, the term *enterprise campus network* is referred to as simply *campus network*. The remainder of this text implies that all *campus* references are related to enterprise networks.

The branch/WAN portion of the enterprise network contains the routers, switches, and so on to interconnect a main office to branch offices and interconnect multiple main sites. Keep in mind, many large enterprises are composed of multiple campuses and data centers that interconnect. Often in large enterprise networks, connecting multiple enterprise data centers requires additional routing features and higher bandwidth links to interconnect remote sites. As such, Cisco designs now partition these designs into a grouping known as Data Center Interconnect (DCI). Branch/WAN and DCI are both out of scope of CCNP SWITCH and this book.

Internet Edge is the portion of the enterprise network that encompasses the routers, switches, firewalls, and network devices that interconnect the enterprise network to the Internet. This section includes technology necessary to connect telecommuters from the Internet to services in the enterprise. Generally, the Internet Edge focuses heavily on network security because it connects the private enterprise to the public domain. Nonetheless, the topic of the Internet Edge as part of the enterprise network is outside the scope of this text and CCNP SWITCH.

Tip The terms *design* and *architecture* are used loosely in most published texts. In this text, the term *architecture* implies a model. Consequently, the term *design* implies the actual network topology designed by a person or persons.

In review, the enterprise network is composed of five distinct areas: core backbone, campus, data center, branch/WAN, and Internet edge. These areas can have subcomponents, and additional areas can be defined in other publications or design documents. For the purpose of CCNP SWITCH and this text, focus is only the campus section of the enterprise network. The next section discusses regulatory standards that drive enterprise networks designs and models holistically, especially the data center. This section defines early information that needs gathering before designing a campus network.

Regulatory Standards Driving Enterprise Architectures

Many regulatory standards drive enterprise architectures. Although most of these regulatory standards focus on data and information, they nonetheless drive network architectures. For example, to ensure that data is as safe as the Health Insurance Portability and Accountability Act (HIPAA) specifies, integrated security infrastructures are becoming paramount. Furthermore, the Sarbanes-Oxley Act, which specifies legal standards for maintaining the integrity of financial data, requires public companies to have multiple redundant data centers with synchronous, real-time copies of financial data.

Because the purpose of this book is to focus on campus design applied to switching, additional detailed coverage of regulatory compliance with respect to design is not covered. Nevertheless, regulatory standards are important concepts for data centers, disaster recovery, and business continuance. In designing any campus network, you need to review any regulatory standards applicable to your business prior to beginning your design. Feel free to review the following regulatory compliance standards as additional reading:

- Sarbanes-Oxley (http://www.sarbanes-oxley.com)
- HIPAA (http://www.hippa.com)
- SEC 17a-4, “Records to Be Preserved by Certain Exchange Members, Brokers and Dealers”

Moreover, the preceding list is not an exhaustive list of regulatory standards but instead a list of starting points for reviewing compliance standards. If regulatory compliance is applicable to your enterprise, consult internally within your organization for further information about regulatory compliance before embarking on designing an enterprise network. The next section describes the motivation behind sound campus designs.

Campus Designs

Properly designed campus architectures yield networks that are module, resilient, and flexible. In other words, properly designed campus architectures save time and money, make IT engineers' jobs easier, and significantly increase business productivity.

To restate, adhering to design best-practices and design principles yield networks with the following characteristics:

- **Modular:** Campus network designs that are modular easily support growth and change. By using building blocks, also referred to as pods or modules, scaling the network is eased by adding new modules instead of complete redesigns.
- **Resilient:** Campus network designs deploying best practices and proper high-availability (HA) characteristics have uptime of near 100 percent. Campus networks deployed by financial services might lose millions of dollars in revenue from a simple 1-second network outage.
- **Flexibility:** Change in business is a guarantee for any enterprise. As such, these business changes drive campus network requirements to adapt quickly. Following campus network designs yields faster and easier changes.

The next section of this text describes legacy campus designs that lead to current generation campus designs published today. This information is useful as it sets the ground work for applying current generation designs.

Legacy Campus Designs

Legacy campus designs were originally based on a simple flat Layer-2 topology with a router-on-a-stick. The concept of *router-on-a-stick* defines a router connecting multiple LAN segments and routing between them, a legacy method of routing in campus networks.

Nevertheless, simple flat networks have many inherit limitations. Layer 2 networks are limited and do not achieve the following characteristics:

- Scalability
- Security
- Modularity
- Flexibility
- Resiliency
- High Availability

A later section, "Layer 2 Switching In-Depth" provides additional information about the limitations of Layer 2 networks.

One of the original benefits of Layer 2 switching, and building Layer 2 networks, was speed. However, with the advent of high-speed switching hardware found on Cisco Catalyst and Nexus switches, Layer 3 switching performance is now equal to Layer 2 switching performance. As such, Layer 3 switching is now being deployed at scale. Examples of Cisco switches that are capable of equal Layer 2 and Layer 3 switching performance are the Catalyst 3000, 4000, and 6500 family of switches and the Nexus 7000 family of switches.

Note With current-generation Cisco switches, Layer 3 switching performance is equal to Layer 2 switching performance in terms of throughput.

Note The Nexus families of switches are relatively new switches targeted for deployment in the data center. As such, these switches support high bandwidth in hundreds of gigabits per second. In addition, Nexus switches optionally offer low-latency switching for market data applications, Fibre Channel over Ethernet (FCOE), and advanced high-availability features. Unfortunately, because Nexus switches are targeted for data centers, they lack some features found in Catalyst switches, such as support for inline power for IP phones.

Since Layer 3 switching performance of Cisco switches allowed for scaled networks, hierarchical designs for campus networks were developed to handle this scale effectively. The next section introduces, briefly, the hierarchical concepts in the campus. These concepts are discussed in more detail in later sections; however, a brief discussion of these topics is needed before discussing additional campus designs concepts.

Hierarchical Models for Campus Design

Consider the Open System Interconnection (OSI) reference model, which is a layered model for understanding and implementing computer communications. By using layers, the OSI model simplifies the task required for two computers to communicate.

Cisco campus designs also use layers to simplify the architectures. Each layer can be focused on specific functions, thereby enabling the networking designer to choose the right systems and features for the layer. This model provides a modular framework that enables flexibility in network design and facilitates implementation and troubleshooting. The Cisco Campus Architecture fundamentally divides networks or their modular blocks into the following access, distribution, and core layers with associated characteristics:

- **Access layer:** Used to grant the user, server, or edge device access to the network. In a campus design, the access layer generally incorporates switches with ports that provide connectivity to workstations, servers, printers, wireless access points, and so on. In the WAN environment, the access layer for telecommuters or remote sites might provide access to the corporate network across a WAN technology. The access layer is the most feature-rich section of the campus network because it is a best practice to

apply features as close to the edge as possible. These features that include security, access control, filters, management, and so on are covered in later chapters.

- **Distribution layer:** Aggregates the wiring closets, using switches to segment workgroups and isolate network problems in a campus environment. Similarly, the distribution layer aggregates WAN connections at the edge of the campus and provides a level of security. Often, the distribution layer acts as a service and control boundary between the access and core layers.
- **Core layer (also referred to as the backbone):** A high-speed backbone, designed to switch packets as fast as possible. In current generation campus designs, the core backbone connects other switches a minimum of 10 Gigabit Ethernet. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes quickly. This layer's design also provides for scalability and fast convergence

This hierarchical model is not new and has been consistent for campus architectures for some time. In review, the hierarchical model is advantageous over nonhierarchical modes for the following reasons:

- Provides modularity
- Easier to understand
- Increases flexibility
- Eases growth and scalability
- Provides for network predictability
- Reduces troubleshooting complexity

Figure 1-2 illustrates the hierarchical model at a high level as applied to a modeled campus network design.

The next section discusses background information on Cisco switches and begins the discussion of the role of Cisco switches in campus network design.

Impact of Multilayer Switches on Network Design

Understanding Ethernet switching is a prerequisite to building a campus network. As such, the next section reviews Layer 2 and Layer 3 terminology and concepts before discussing enterprise campus designs in subsequent sections. A subset of the material presented is a review of CCNA material.

Ethernet Switching Review

Product marketing in the networking technology field uses many terms to describe product capabilities. In many situations, product marketing stretches the use of technology terms to distinguish products among multiple vendors. One such case is the terminology

of Layers 2, 3, 4, and 7 switching. These terms are generally exaggerated in the networking technology field and need careful review.

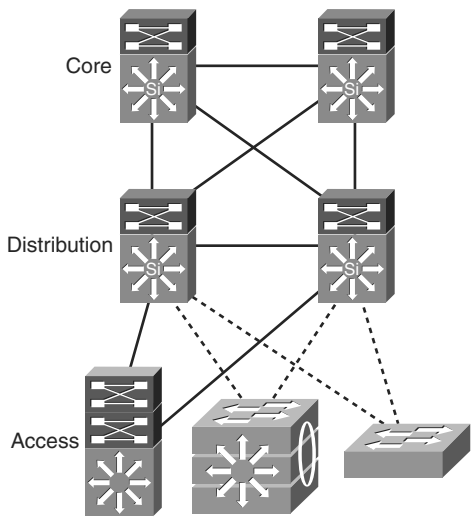


Figure 1-2 *High-Level Example of the Hierarchical Model as Applied to a Campus Network*

The Layers 2, 3, 4, and 7 switching terminology correlates switching features to the OSI reference model. Figure 1-3 illustrates the OSI reference model and its relationship to protocols and network hardware.

The next section provides a CCNA review of Layer 2 switching. Although this section is a review, it is a critical subject for later chapters.

Layer 2 Switching

Product marketing labeling a Cisco switch as either as a Layer 2 or as a Layer 3 switching is no longer black and white because the terminology is not consistent with product capabilities. In review, Layer 2 switches are capable of switching packets based only on MAC addresses. Layer 2 switches increase network bandwidth and port density without much complexity. The term *Layer 2 switching* implies that frames forwarded by the switch are not modified in any way; however, Layer 2 switches such as the Catalyst 2960 are capable of a few Layer 3 features, such as classifying packets for quality of service (QoS) and network access control based on IP address. An example of QoS marking at Layer 4 is marking the differentiated services code point (DSCP) bits in the IP header based on the TCP port number in the TCP header. Do not be concerned with understanding the QoS technology at this point as highlighted in the proceeding sentence in this chapter; this terminology is covered in more detail in later chapters. To restate, Layer 2-only switches are not capable of routing frames based on IP address and are limited to

forwarding frames only based on MAC address. Nonetheless, Layer 2 switches might support features that read Layer 3 information of a frame for specific features.

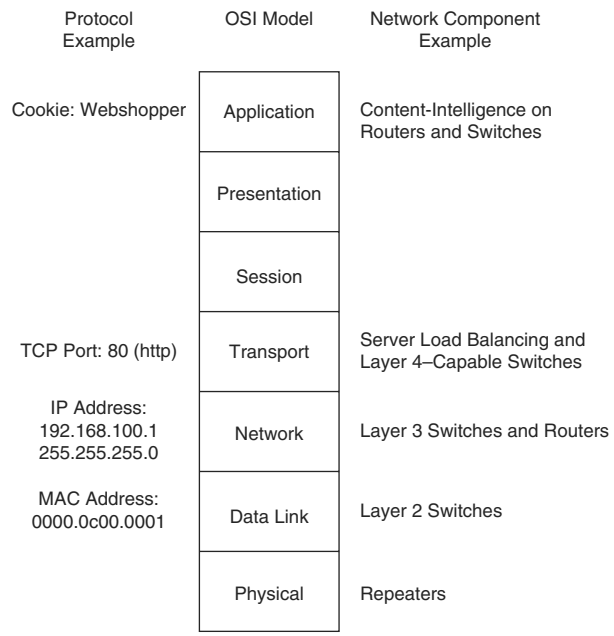


Figure 1-3 *OSI Layer Relationship to Protocols and Networking Hardware*

Legacy Layer 2 switches are limited in network scalability due to many factors. Consequently, all network devices on a legacy Layer 2 switch must reside on the same subnet and, as a result, exchange broadcast packets for address resolution purposes. Network devices grouped together to exchange broadcast packets constitute a broadcast domain. Layer 2 switches flood unknown unicast, multicast, and broadcast traffic throughout the entire broadcast domain. As a result, all network devices in the broadcast domain process all flooded traffic. As the size of the broadcast domain grows, its network devices become overwhelmed by the task of processing this unnecessary traffic. This caveat prevents network topologies from growing to more than a few legacy Layer 2 switches. Lack of QoS and security features are other features that can prevent the use of low-end Layer 2 switches in campus networks and data centers.

However, all current and most legacy Cisco Catalyst switches support virtual LANs (VLAN), which segment traffic into separate broadcast domains and, as a result, IP subnets. VLANs overcome several of the limitations of the basic Layer 2 networks, as discussed in the previous paragraph. This book discusses VLANs in more detail in the next chapter.

Figure 1-4 illustrates an example of a Layer 2 switch with workstations attached. Because the switch is only capable of MAC address forwarding, the workstations must reside on the same subnet to communicate.

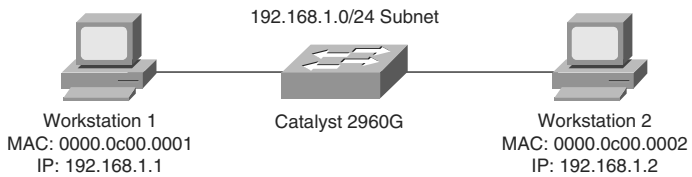


Figure 1-4 *Layer 2 Switching*

Layer 3 Switching

Layer 3 switches include Layer 3 routing capabilities. Many of the current-generation Catalyst Layer 3 switches can use routing protocols such as BGP, RIP, OSPF, and EIGRP to make optimal forwarding decisions. A few Cisco switches that support routing protocols do not support BGP because they do not have the memory necessary for large routing tables. These routing protocols are reviewed in later chapters. Figure 1-5 illustrates a Layer 3 switch with several workstations attached. In this example, the Layer 3 switch routes packets between the two subnets.

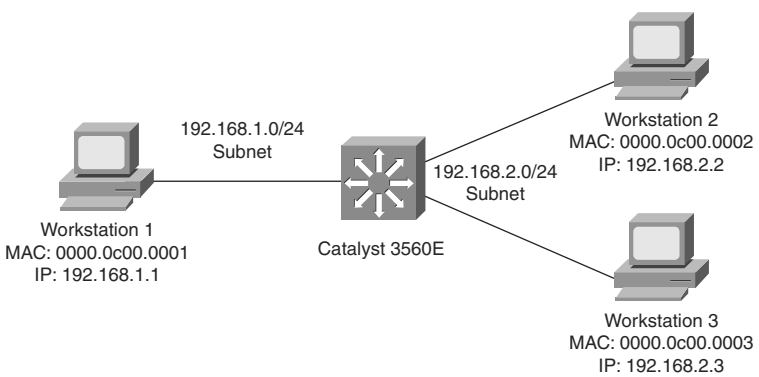


Figure 1-5 *Layer 3 Switching*

Note Layer 2 switching:

- Switching based on MAC address
- Restricts scalability to a few switches in a domain
- May support Layer 3 features for QoS or access-control

Layer 3 switching:

- Switching based on IP address
- Interoperates with Layer 2 features
- Enables highly scalable designs

Layer 4 and Layer 7 Switching

Layers 4 and 7 switching terminology is not as straightforward as Layers 2 and 3 switching terminology. Layer 4 switching implies switching based on protocol sessions. In other words, Layer 4 switching uses not only source and destination IP addresses in switching decisions, but also IP session information contained in the TCP and User Datagram Protocol (UDP) portions of the packet. The most common method of distinguishing traffic with Layer 4 switching is to use the TCP and UDP port numbers. Server load balancing, a Layer 4 to Layer 7 switching feature, can use TCP information such as TCP SYN, FIN, and RST to make forwarding decisions. (Refer to RFC 793 for explanations of TCP SYN, FIN, and RST.) As a result, Layer 4 switches can distinguish different types of IP traffic flows, such as differentiating the FTP, Network Time Protocol (NTP), HTTP, Secure HTTP (S-HTTP), and Secure Shell (SSH) traffic.

Layer 7 switching is switching based on application information. Layer 7 switching capability implies content-intelligence. Content-intelligence with respect to web browsing implies features such as inspection of URLs, cookies, host headers, and so on. Content-intelligence with respect to VoIP can include distinguishing call destinations such as local or long distance.

Table 1-1 summarizes the layers of the OSI model with their respective protocol data units (PDU), which represent the data exchanged at each layer. Note the difference between frames and packets and their associated OSI level. The table also contains a column illustrating sample device types operating at the specified layer.

Table 1-1 *PDU and Sample Device Relationship to the OSI Model*

OSI Level	OSI Layer	PDU Type	Device Example	Address
1	Physical	Electrical signals	Repeater, transceiver	None
2	Data link	Frames	Switches	MAC address
3	Network	Packet	Router, multilayer switches	IP address
4	Transport	TCP or UDP data segments	Multilayer switch load balancing based on TCP port number	TCP or UDP port numbering
7	Application	Embedded application information in data payload	Multilayer switch using Network-Based Application Recognition (NBAR) to permit or deny traffic based on data passed by an application	Embedded information in data payload

Layer 2 Switching In-Depth

Layer 2 switching is also referred to as hardware-based bridging. In a Layer 2-only switch, ASICs handle frame forwarding. Moreover, Layer 2 switches deliver the ability to increase bandwidth to the wiring closet without adding unnecessary complexity to the network. At Layer 2, no modification is required to the frame content when going between Layer 1 interfaces, such as Fast Ethernet to 10 Gigabit Ethernet.

In review, the network design properties of current-generation Layer 2 switches include the following:

- Designed for near wire-speed performance
- Built using high-speed, specialized ASICs
- Switches at low latency
- Scalable to a several switch topology without a router or Layer 3 switch
- Supports Layer 3 functionality such as Internet Group Management Protocol (IGMP) snooping and QoS marking
- Offers limited scalability in large networks without Layer 3 boundaries

Layer 3 Switching In-Depth

Layer 3 switching is hardware-based routing. Layer 3 switches overcome the inadequacies of Layer 2 scalability by providing routing domains. The packet forwarding in Layer 3 switches is handled by ASICs and other specialized circuitry. A Layer 3 switch performs everything on a packet that a traditional router does, including the following:

- Determines the forwarding path based on Layer 3 information
- Validates the integrity of the Layer 3 packet header via the Layer 3 checksum
- Verifies and decrements packet Time-To-Live (TTL) expiration
- Rewrites the source and destination MAC address during IP rewrites
- Updates Layer 2 CRC during Layer 3 rewrite
- Processes and responds to any option information in the packet such as the Internet Control Message Protocol (ICMP) record
- Updates forwarding statistics for network management applications
- Applies security controls and classification of service if required

Layer 3 routing requires the ability of packet rewriting. Packet rewriting occurs on any routed boundary. Figure 1-6 illustrates the basic packet rewriting requirements of Layer 3 routing in an example in which two workstations are communicating using ICMP.

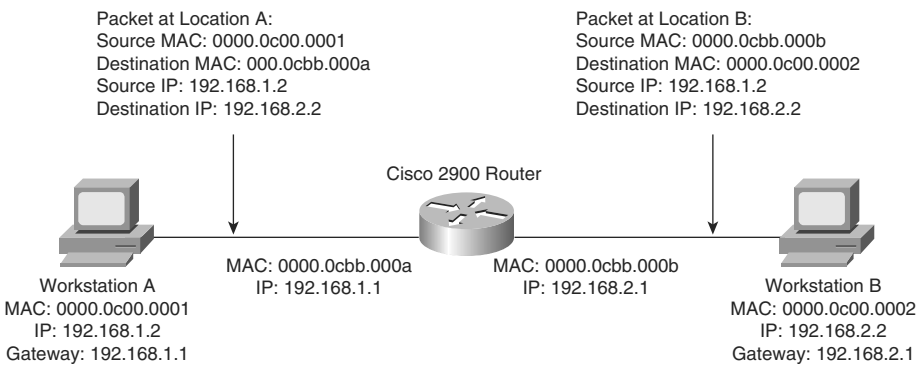


Figure 1-6 *Layer 3 Packet Rewriting*

Address Resolution Protocol (ARP) plays an important role in Layer 3 packet rewriting. When Workstation A in Figure 1-6 sends five ICMP echo requests to Workstation B, the following events occur (assuming all the devices in this example have yet to communicate, use static addressing versus DHCP, and there is no event to trigger a gratuitous ARP):

1. Workstation A sends an ARP request for its default gateway. Workstation A sends this ARP to obtain the MAC address of the default gateway. Without knowing the MAC address of the default gateway, Workstation A cannot send any traffic outside the local subnet. Note that, in this example, Workstation A's default gateway is the Cisco 2900 router with two Ethernet interfaces.
2. The default gateway, the Cisco 2900, responds to the ARP request with an ARP reply, sent to the unicast MAC address and IP address of Workstation A, indicating the default gateway's MAC address. The default gateway also adds an ARP entry for Workstation A in its ARP table upon receiving the ARP request.
3. Workstation A sends the first ICMP echo request to the destination IP address of Workstation B with a destination MAC address of the default gateway.
4. The router receives the ICMP echo request and determines the shortest path to the destination IP address.
5. Because the default gateway does not have an ARP entry for the destination IP address, Workstation B, the default gateway drops the first ICMP echo request from Workstation A. The default gateway drops packets in the absence of ARP entries to

avoid storing packets that are destined for devices without ARP entries as defined by the original RFCs governing ARP.

6. The default gateway sends an ARP request to Workstation B to get Workstation B's MAC address.
7. Upon receiving the ARP request, Workstation B sends an ARP response with its MAC address.
8. By this time, Workstation A is sending a second ICMP echo request to the destination IP of Workstation B via its default gateway.
9. Upon receipt of the second ICMP echo request, the default gateway now has an ARP entry for Workstation B. The default gateway in turn rewrites the source MAC address to itself and the destination MAC to Workstation B's MAC address, and then forwards the frame to Workstation B.
10. Workstation B receives the ICMP echo request and sends an ICMP echo reply to the IP address of Workstation A with the destination MAC address of the default gateway.

Figure 1-6 illustrates the Layer 2 and Layer 3 rewriting at different places along the path between Workstation A and B. This figure and example illustrate the fundamental operation of Layer 3 routing and switching.

The primary difference between the packet-forwarding operation of a router and Layer 3 switching is the physical implementation. Layer 3 switches use different hardware components and have greater port density than traditional routers.

These concepts of Layer 2 switching, Layer 3 forwarding, and Layer 3 switching are applied in a single platform: the multilayer switch. Because it is designed to handle high-performance LAN traffic, a Layer 3 switch is locatable when there is a need for a router and a switch within the network, cost effectively replacing the traditional router and router-on-a-stick designs of the past.

Understanding Multilayer Switching

Multilayer switching combines Layer 2 switching and Layer 3 routing functionality. Generally, the networking field uses the terms Layer 3 switch and multilayer switch interchangeably to describe a switch that is capable of Layer 2 and Layer 3 switching. In specific terms, multilayer switches move campus traffic at wire speed while satisfying Layer 3 connectivity requirements. This combination not only solves throughput problems but also helps to remove the conditions under which Layer 3 bottlenecks form. Moreover, multilayer switches support many other Layer 2 and Layer 3 features besides routing and switching. For example, many multilayer switches support QoS marking. Combining both Layer 2 and Layer 3 functionality and features allows for ease of deployment and simplified network topologies.

Moreover, Layer 3 switches limit the scale of spanning tree by segmenting Layer 2, which eases network complexity. In addition, Layer 3 routing protocols enable load-balancing, fast convergence, scalability, and control compared to traditional Layer 2 features.

In review, multilayer switching is a marketing term used to refer to any Cisco switch capable of Layer 2 switching and Layer 3 routing. From a design perspective, all enterprise campus designs include multilayer switches in some aspect, most likely in the core or distribution layers. Moreover, some campus designs are evolving to include an option for designing Layer 3 switching all the way to the access layer with a future option of supporting Layer 3 network ports on each individual access port. Over the next few years, the trend in the campus is to move to a pure Layer 3 environment consisting of inexpensive Layer 3 switches.

Note The remainder of this text uses the term *multilayer switch* and *Layer 3 switch* interchangeably.

Introduction to Cisco Switches

Cisco has a plethora of Layer 2 and Layer 3 switch models. For brevity, this section highlights a few popular models used in the campus, core backbone, and data center. For a complete list of Cisco switches, consult product documentation at Cisco.com.

Cisco Catalyst 6500 Family of Switches

The Cisco Catalyst 6500 family of switches are the most popular switches Cisco ever produced. They are found in a wide variety of installs not only including campus, data center, and backbone, but also found in deployment of services, WAN, branch, and so on in both enterprise and service provider networks. For the purpose of CCNP SWITCH and the scope of this book, the Cisco Catalyst 6500 family of switches are summarized as follows:

- Scalable modular switch up to 13 slots
- Supports up to 16 10-Gigabit Ethernet interfaces per slot in an over-subscription model
- Up to 80 Gbps of bandwidth per slot in current generation hardware
- Supports Cisco IOS with a plethora of Layer 2 and Layer 3 switching features
- Optionally supports up to Layer 7 features with specialized modules
- Integrated redundant and high-available power supplies, fans, and supervisor engineers
- Supports Layer 3 Non-Stop Forwarding (NSF) whereby routing peers are maintained during a supervisor switchover.
- Backward capability and investment protection have lead to a long life cycle

Cisco Catalyst 4500 Family of Switches

The Cisco Catalyst 4500 family of switches is a vastly popular modular switch found in many campus networks at the distribution layer or in collapsed core networks of small to medium-sized networks. Collapsed core designs combine the core and distribution layers

into a single area. The Catalyst 4500 is one step down from the Catalyst 6500 but does support a wide array of Layer 2 and Layer 3 features. In summary, the Cisco Catalyst 4500 family of switches are summarized as follows:

- Scalable module switch with up to 10 slots
- Supports multiple 10 Gigabit Ethernet interfaces per slot
- Supports Cisco IOS
- Supports both Layer 2 switching and Layer 3 switching
- Optionally supports integrated redundant and high-available power supplies and supervisor engines

Cisco Catalyst 4948G, 3750, and 3560 Family of Switches

The Cisco Catalyst 4948G, 3750, and 3560 family of switches are popular switches used in campus networks for fixed-port scenarios, most often the access layer. These switches are summarized as follows:

- Available in a variety of fixed port configurations with up to 48 1-Gbps access layer ports and 4 10-Gigabit Ethernet interfaces for uplinks to distribution layer
- Supports Cisco IOS
- Supports both Layer 2 and Layer 3 switching
- Not architected with redundant hardware

Cisco Catalyst 2000 Family of Switches

The Cisco Catalyst 2000 family of switches are Layer 2-only switches capable of few Layer 3 features aside from Layer 3 routing. These features are often found in the access layer in campus networks. These switches are summarized as follows:

- Available in a variety of fixed port configurations with up to 48 1-Gbps access layer ports and multiple 10-Gigabit Ethernet uplinks
- Supports Cisco IOS
- Supports only Layer 2 switching
- Not architected with redundant hardware

Nexus 7000 Family of Switches

The Nexus 7000 family of switches are the Cisco premier data center switches. The product launch in 2008; and thus, the Nexus 7000 software does not support all the features of Cisco IOS yet. Nonetheless, the Nexus 7000 is summarized as follows:

- Modular switch with up to 18 slots
- Supports up to 230 Gbps per slot

- Supports Nexus OS (NX-OS)
- 10-slot chassis is built on front-to-back airflow
- Supports redundant supervisor engines, fans, and power supplies

Nexus 5000 and 2000 Family of Switches

The Nexus 5000 and 2000 family of switches are low-latency switches designed for deployment in the access layer of the data center. These switches are Layer 2-only switches today but support cut-through switching for low latency. The Nexus 5000 switches are designed for 10-Gigabit Ethernet applications and also support Fibre Channel over Ethernet (FCOE).

Hardware and Software-Switching Terminology

This book refers to the terms hardware-switching and software-switching regularly throughout the text. The industry term *hardware-switching* refers to the act of processing packets at any Layers 2 through 7, via specialized hardware components referred to as application-specific integrated circuits (ASIC). ASICs can generally reach throughput at wire speed without performance degradation for advanced features such as QoS marking, ACL processing, or IP rewriting.

Note Other terms used to describe hardware-switching are in-hardware, using ASICs, and hardware-based. These terms are used interchangeably throughout the text. Multilayer switching (MLS) is another term commonly used to describe hardware-switching. The term MLS can be confusing; for example, with the Catalyst 5500, the term MLS described a legacy hardware-switching method and feature. With today's terminology, MLS describes the capability to route and switch frames at line-rate (the speed of all ports sending traffic at the same time, full-duplex, at the maximum speed of the interface) with advanced features such as Network Address Translation (NAT), QoS, access controls, and so on using ASICs.

Switching and routing traffic via hardware-switching is considerably faster than the traditional software-switching of frames via a CPU. Many ASICs, especially ASICs for Layer 3 routing, use specialized memory referred to as ternary content addressable memory (TCAM) along with packet-matching algorithms to achieve high performance, whereas CPUs simply use higher processing rates to achieve greater degrees of performance. Generally, ASICs can achieve higher performance and availability than CPUs. In addition, ASICs scale easily in switching architecture, whereas CPUs do not. ASICs integrate not only on Supervisor Engines, but also on individual line modules of Catalyst switches to hardware-switch packets in a distributed manner.

ASICs do have memory limitations. For example, the Catalyst 6500 family of switches can accommodate ACLs with a larger number of entries compared to the Catalyst 3560E

family of switches due to the larger ASIC memory on the Catalyst 6500 family of switches. Generally, the size of the ASIC memory is relative to the cost and application of the switch. Furthermore, ASICs do not support all the features of the traditional Cisco IOS. For instance, the Catalyst 6500 family of switches with a Supervisor Engine 720 and an MSFC3 (Multilayer Switch Feature Card) must software-switch all packets requiring Network Address Translation (NAT) without the use of specialized line modules. As products continue to evolve and memory becomes cheaper, ASICs gain additional memory and feature support.

For the purpose of CCNP SWITCH and campus network design, the concepts in this section are overly simplified. Use the content in this section as information for sections that refer to the terminology. The next section changes scope from switching hardware and technology to campus network types.

Campus Network Traffic Types

Campus designs are significantly tied to network size. However, traffic patterns and traffic types through each layer hold significant importance on how to shape a campus design. Each type of traffic represents specific needs in terms of bandwidth and flow patterns. Table 1-2 lists several different types of traffic that might exist on a campus network. As such, indentifying traffic flows, types, and patterns is a prerequisite to designing a campus network.

Table 1-2 highlights common traffic types with a description, common flow patterns, and a denotation of bandwidth (BW). The BW column highlights on a scale of low to very high the common rate of traffic for the corresponding traffic type for comparison purposes. Note: This table illustrates common traffic types and common characteristics; it is not uncommon to find scenarios of atypical traffic types.

For the purpose of enterprise campus design, note the traffic types in your network, particularly multicast traffic. Multicast traffic for servers-centric applications is generally restricted to the data center; however, whatever multicast traffics spans into the campus needs to be accounted for because it can significantly drive campus design. The next sections delve into several types of applications in more detail and their traffic flow characteristics.

Note IP multicast traffic requirements in the campus need careful review prior to any campus network design because of its high-bandwidth requirements.

Figure 1-7 illustrates a sample enterprise network with several traffic patterns highlighted as dotted lines to represent possible interconnects that might experience heavy traffic utilization.

Table 1-2 *Common Traffic Types*

Traffic Type	Description	Traffic Flow	BW
Network Management	Many different types of network management traffic may be present on the network. Examples include bridge protocol data units (BPDU), Cisco Discovery Protocol (CDP) updates, Simple Network Management Protocol (SNMP), Secure Shell (SSH), and Remote Monitoring (RMON) traffic. Some designers assign a separate VLAN to the task of carrying certain types of network management traffic to make network troubleshooting easier.	Traffic is found flowing in all layers.	Low
Voice (IP Telephony)	There are two types of voice traffic: signaling information between the end devices (for example, IP phones and soft switches, such as Cisco CallManager) and the data packets of the voice conversation itself. Often, the data to and from IP phones is configured on a separate VLAN for voice traffic because the designer wants to apply QoS measures to give high priority to voice traffic.	Traffic generally moves from access layer to servers in core layer or data center.	Low
IP Multicast	IP multicast traffic is sent from a particular source address to group MAC addresses. Examples of applications that generate this type of traffic are video such as IP/TV broadcasts and market data applications used to configure analysis trading market activities. Multicast traffic can produce a large amount of data streaming across the network. Switches need to be configured to keep this traffic from flooding to devices that have not requested it, and routers need to ensure that multicast traffic is forwarded to the network areas where it is requested.	Market data applications are usually contained within the data center. Other traffic such as IP/TV and user data flows from access layer to core layers and to the data center.	Very High

continues

Table 1-2 *Common Traffic Types (continued)*

Traffic Type	Description	Traffic Flow	BW
Normal Data	This is typical application traffic related to file and print services, email, Internet browsing, database access, and other shared network applications. You may need to treat this data the same or in different ways in different parts of the network, based on the volume of each type. Examples of this type of traffic are Server Message Block, Netware Core Protocol (NCP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), and HTTP.	Traffic usually flows from the access layer to core layer and to the data center.	Low to Mid
Scavenger class	Scavenger class includes all traffic with protocols or patterns that exceed their normal data flows. It is used to protect the network from exceptional traffic flows that might be the result of malicious programs executing on end-system PCs. Scavenger class is also used for less than best-effort type traffic, such as peer-to-peer traffic.	Traffic patterns vary.	Mid to High

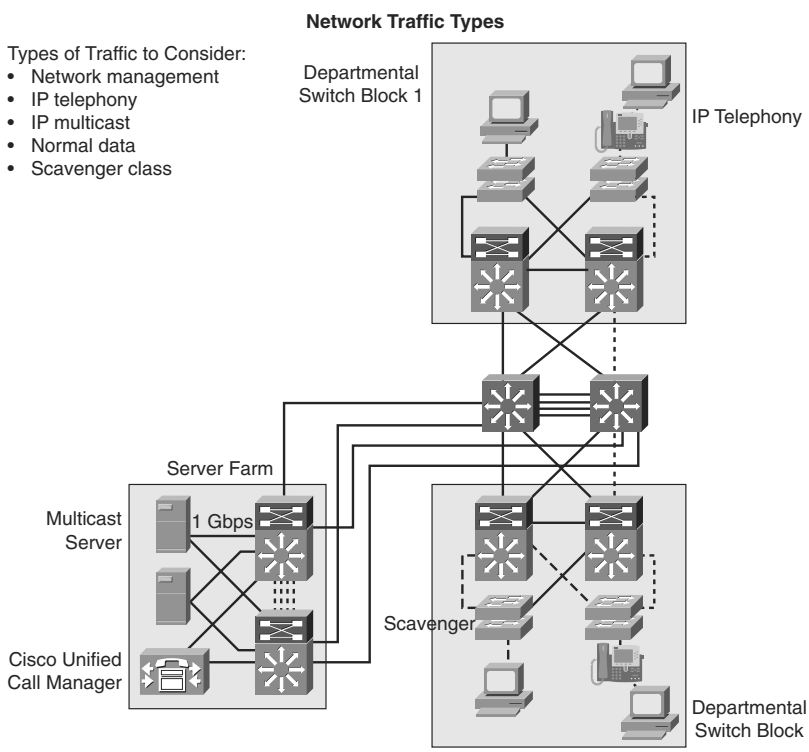


Figure 1-7 *Network Traffic Types*

Peer-to-Peer Applications

Some traffic flows are based on a peer-to-peer model, where traffic flows between endpoints that may be far from each other. Peer-to-peer applications include applications where the majority of network traffic passes from one end device, such as a PC or IP phone, to another through the organizational network. (See Figure 1-8.) Some traffic flows are not sensitive to bandwidth and delay issues, whereas some others require real-time interaction between peer devices. Typical peer-to-peer applications include the following:

- **Instant messaging:** Two peers establish communication between two end systems. When the connection is established, the conversation is direct.
- **File sharing:** Some operating systems or applications require direct access to data on other workstations. Fortunately, most enterprises are banning such applications because they lack centralized or network-administered security.
- **IP phone calls:** The network requirements of IP phone calls are strict because of the need for QoS treatment to minimize jitter.
- **Video conference systems:** The network requirements of video conferencing are demanding because of the bandwidth consumption and class of service (CoS) requirements.

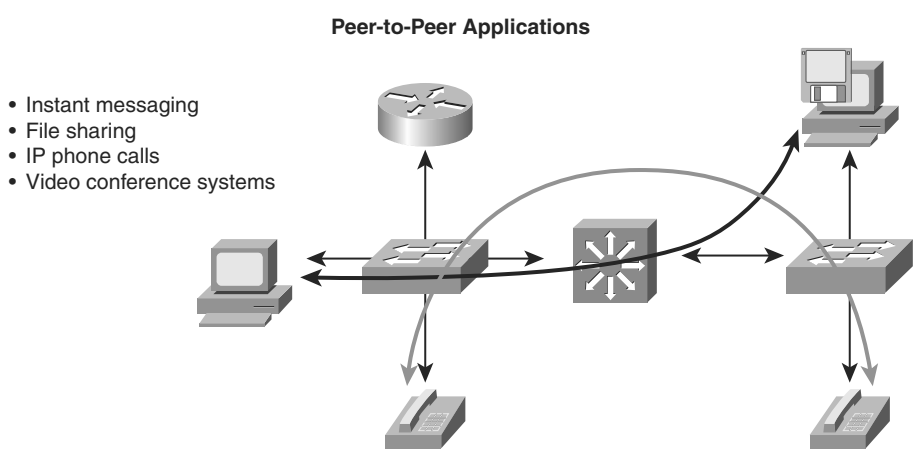


Figure 1-8 *High-Level Peer-to-Peer Application*

Client/Server Applications

Many enterprise traffic flows are based on a client/server model, where connections to the server might become bottlenecks. Network bandwidth used to be costly, but today, it is cost-effective compared to the application requirements. For example, the cost of Gigabit Ethernet and 10 Gigabit is advantageous compared to application bandwidth requirements that rarely exceed 1 Gigabit Ethernet. Moreover, because the switch delay is

insignificant for most client/server applications with high-performance Layer 3 switches, locating the servers centrally rather than in the workgroup is technically feasible and reduces support costs. Latency is extremely important to financial and market data applications, such as 29 West and Tibco. For situations in which the lowest latency is necessary, Cisco offers low-latency modules for the Nexus 7000 family of switches and the Nexus 5000 and 2000 that are low-latency for all variants. For the purpose of this book and CCNP SWITCH, the important take-away is that data center applications for financials and market trade can require a low latency switch, such as the Nexus 5000 family of switches.

Figure 1-9 depicts, at a high level, client/server application traffic flow.

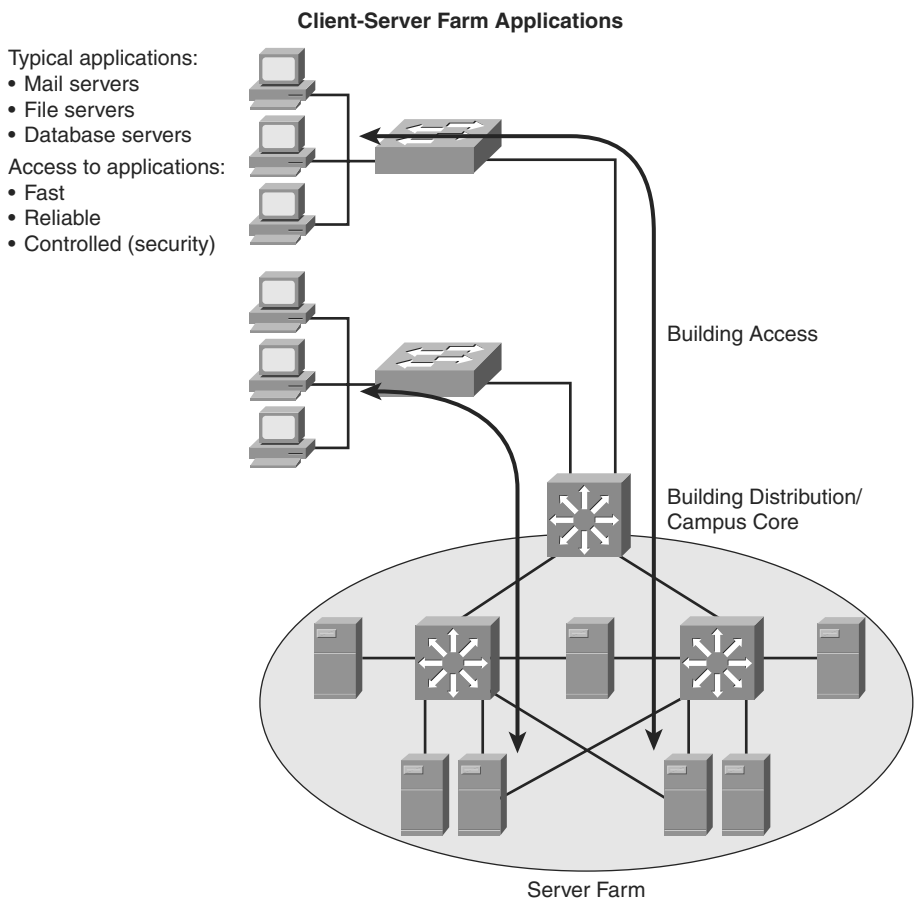


Figure 1-9 *Client/Server Traffic Flow*

In large enterprises, the application traffic might cross more than one wiring closet or LAN to access applications to a server group in a data center. Client-server farm applications apply the 20/80 rule, in which only 20 percent of the traffic remains on the local LAN segment, and 80 percent leaves the segment to reach centralized servers, the Internet, and so on. Client-server farm applications include the following:

- Organizational mail servers
- Common file servers
- Common database servers for organizational applications such as human resource, inventory, or sales applications

Users of large enterprises require fast, reliable, and controlled access to critical applications. For example, traders need access to trading applications anytime with good response times to be competitive with other traders. To fulfill these demands and keep administrative costs low, the solution is to place the servers in a common server farm in a data center. The use of server farms in data centers requires a network infrastructure that is highly resilient and redundant and that provides adequate throughput. Typically, high-end LAN switches with the fastest LAN technologies, such as 10 Gigabit Ethernet, are deployed. For Cisco switches, the current trend is to deploy Nexus switches while the campus deploys Catalyst switches. The use of the Catalyst switches in the campus and Nexus in the data center is a market transition from earlier models that used Catalyst switches throughout the enterprise. At the time of publication, Nexus switches do not run the traditional Cisco IOS found on Cisco routers and switch. Instead, these switches run Nexus OS (NX-OS), which was derived from SAN-OS found on the Cisco MDS SAN platforms.

Nexus switches have a higher cost than Catalyst switches and do not support telephony, inline power, firewall, or load-balancing services, and so on. However, Nexus switches do support higher throughput, lower latency, high-availability, and high-density 10-Gigabit Ethernet suited for data center environments. A later section details the Cisco switches with more information.

Client-Enterprise Edge Applications

Client-enterprise edge applications use servers on the enterprise edge to exchange data between the organization and its public servers. Examples of these applications include external mail servers and public web servers.

The most important communication issues between the campus network and the enterprise edge are security and high availability. An application that is installed on the enterprise edge might be crucial to organizational process flow; therefore, outages can result in increased process cost.

The organizations that support their partnerships through e-commerce applications also place their e-commerce servers in the enterprise edge. Communications with the servers

located on the campus network are vital because of two-way data replication. As a result, high redundancy and resiliency of the network are important requirements for these applications.

Figure 1-10 illustrates traffic flow for a sample client-enterprise edge application with connections through the Internet.

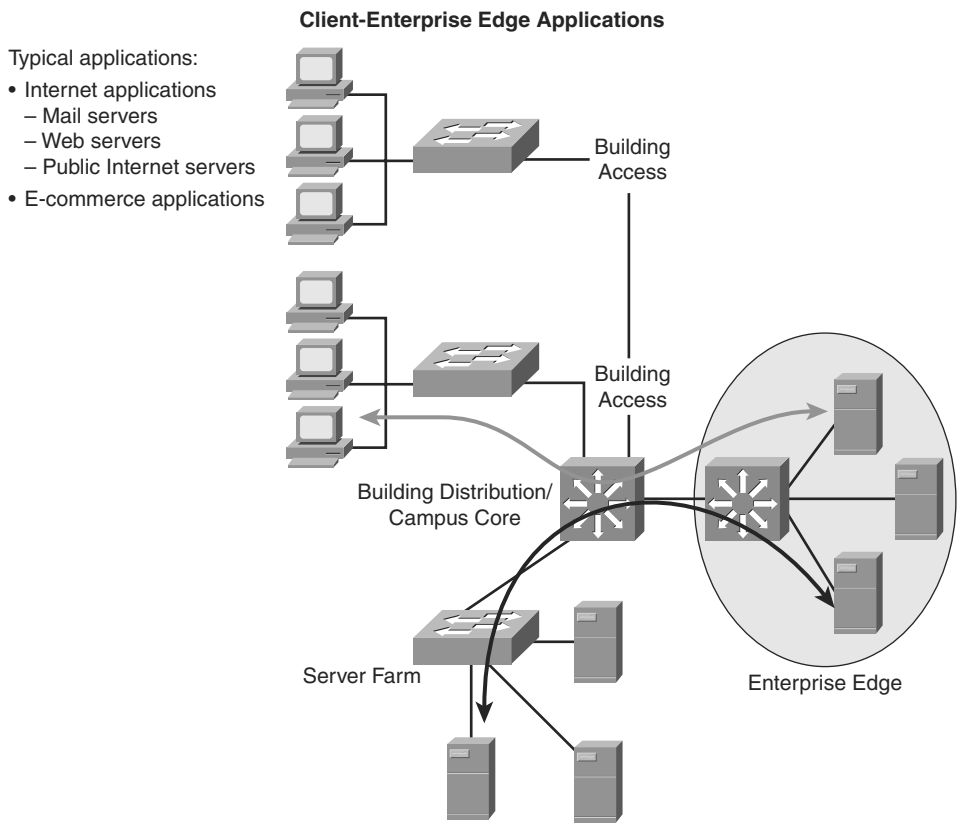


Figure 1-10 *Client-Enterprise Edge Application Traffic Flow*

Recall from earlier sections that the client-enterprise edge applications in Figure 1-10 pass traffic through the Internet edge portion of the Enterprise network.

In review, understanding traffic flow and patterns of an enterprise are necessary prior to designing a campus network. This traffic flow and pattern ultimately shapes scale, features, and use of Cisco switches in the campus network. Before further discussion on designing campus networks, the next section highlights two Cisco network architecture models that are useful in understanding all the elements that make a successful network deployment.

Overview of the SONA and Borderless Networks

Proper network architecture helps ensure that business strategies and IT investments are aligned. As the backbone for IT communications, the network element of enterprise architecture is increasingly critical. Service-Oriented Network Architecture (SONA) is the Cisco architectural approach to designing advanced network capabilities.

Figure 1-11 illustrates SONA pictorially from a marketing perspective.

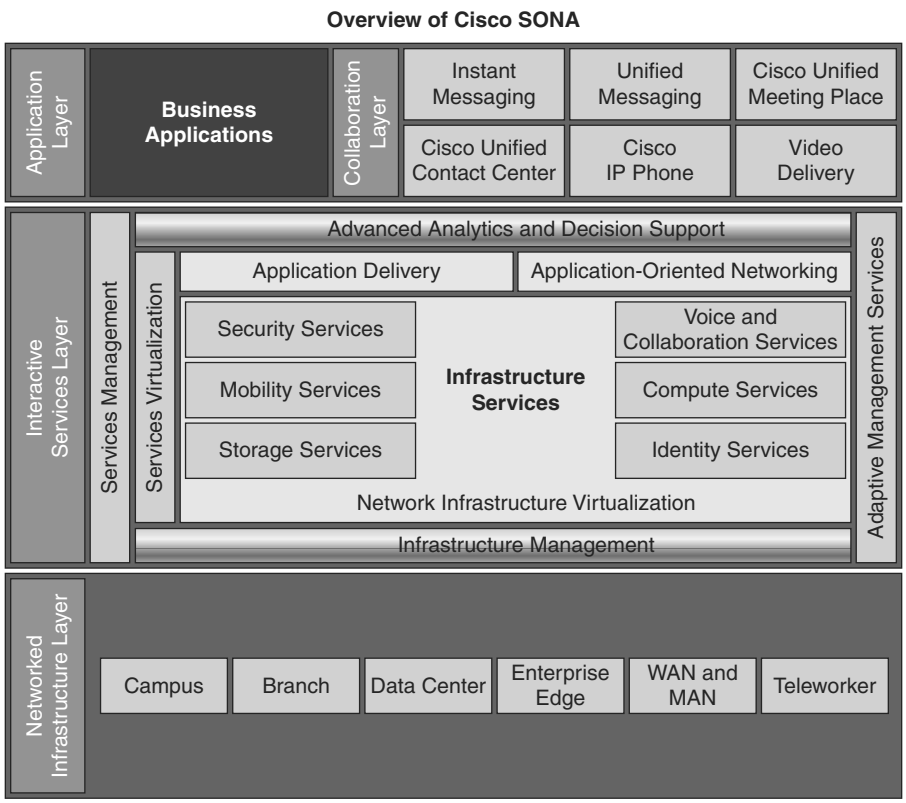


Figure 1-11 *SONA Overview*

SONA provides guidance, best practices, and blueprints for connecting network services and applications to enable business solutions. The SONA framework illustrates the concept that the network is the common element that connects and enables all components of the IT infrastructure. SONA outlines these three layers of intelligence in the enterprise network:

- **The Networked Infrastructure Layer:** Where all the IT resources are interconnected across a converged network foundation. The IT resources include servers, storage, and clients. The network infrastructure layer represents how these resources exist in

different places in the network, including the campus, branch, data center, WAN, metropolitan-area network (MAN), and telecommuter. The objective for customers in this layer is to have anywhere and anytime connectivity.

- **The Interactive Services Layer:** Enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure.
- **The Application Layer:** Includes business applications and collaboration applications. The objective for customers in this layer is to meet business requirements and achieve efficiencies by leveraging the interactive services layer.

The common thread that links the layers is SONA embeds application-level intelligence into the network infrastructure elements so that the network can recognize and better support applications and services.

Deploying a campus design based on the Cisco SONA framework yields several benefits:

- **Convergence, virtualization, intelligence, security, and integration in all areas of the network infrastructure:** The Cisco converged network encompasses all IT technologies, including computing, data, voice, video, and storage. The entire network now provides more intelligence for delivering all applications, including voice and video. Employees are more productive because they can use a consistent set of Unified Communications tools from almost anywhere in the world.
- **Cost savings:** With the Cisco SONA model, the network offers the power and flexibility to implement new applications easily, which reduces development and implementation costs. Common network services are used on an as-needed basis by voice, data, and video applications.
- **Increased productivity:** Collaboration services and product features enable employees to share multiple information types on a rich-media conferencing system. For example, agents in contact centers can share a Web browser with a customer during a voice call to speed up problem resolution and increase customer knowledge using a tool such as Cisco WebEX. Collaboration has enabled contact center agents to reduce the average time spent on each call, yet receive higher customer satisfaction ratings. Another example is cost saving associated with hosting virtual meetings using Cisco WebEx.
- **Faster deployment of new services and applications:** Organizations can better deploy services for interactive communications through virtualization of storage, cloud computing, and other network resources. Automated processes for provisioning, monitoring, managing, and upgrading voice products and services help Cisco IT achieve greater network reliability and maximize the use of IT resources. Cloud computing is the next wave of new technology to be utilized in enterprise environments.
- **Enhanced business processes:** With the SONA, IT departments can better support and enhance business processes and resilience through integrated applications and intelligent network services. Examples include change-control processes that enable 99.999 percent of network uptimes.

Keep in mind, SONA is strictly a model to guide network designs. When designing the campus portion of the enterprise network, you need to understand SONA only from a high level as most of the focus of the campus design is centered on features and functions of Cisco switching.

Cisco.com contains additional information and readings on SONA for persons seeking more details.

In October 2009, Cisco launched a new enterprise architecture called Borderless Networks. As with SONA, the model behind Borderless Networks enables businesses to transcend borders, access resources anywhere, embrace business productivity, and lower business and IT costs. One enhancement added to Borderless Networks over SONA is that the framework focuses more on growing enterprises into global companies, noted in the term "borderless." In terms of CCNP SWITCH, focus on a high-level understanding of SONA because Borderless Networks is a new framework. Consult Cisco.com for additional information on Borderless Networks.

In review, SONA and Borderless Networks are marketing architectures that form high-level frameworks for designing networks. For the purpose of designing a campus network, focus on terms from building requirements around traffic flow, scale, and general requirements. The next section applies a life-cycle approach to campus design and delves into more specific details about the campus designs.

Enterprise Campus Design

The next subsections detail key enterprise campus design concepts. The access, distribution, and core layers introduced earlier in this chapter are expanded on with applied examples. Later subsections of this chapter define a model for implementing and operating a network.

The tasks of implementing and operating a network are two components of the Cisco Lifecycle model. In this model, the life of the network and its components are taught with a structural angle, starting from the preparation of the network design to the optimization of the implemented network. This structured approach is key to ensure that the network always meets the requirements of the end users. This section describes the Cisco Lifecycle approach and its impact on network implementation.

The enterprise campus architecture can be applied at the campus scale, or at the building scale, to allow flexibility in network design and facilitate ease of implementation and troubleshooting. When applied to a building, the Cisco Campus Architecture naturally divides networks into the building access, building distribution, and building core layers, as follows:

- **Building access layer:** This layer is used to grant user access to network devices. In a network campus, the building access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations and servers. In the WAN

environment, the building access layer at remote sites can provide access to the corporate network across WAN technology.

- **Building distribution layer:** Aggregates the wiring closets and uses switches to segment workgroups and isolate network problems.
- **Building core layer:** Also known as the campus backbone, this is a high-speed backbone designed to switch packets as fast as possible. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes quickly.

Figure 1-12 illustrates a sample enterprise network topology that spans multiple buildings.

The enterprise campus architecture divides the enterprise network into physical, logical, and functional areas. These areas enable network designers and engineers to associate specific network functionality on equipment based upon its placement and function in the model.

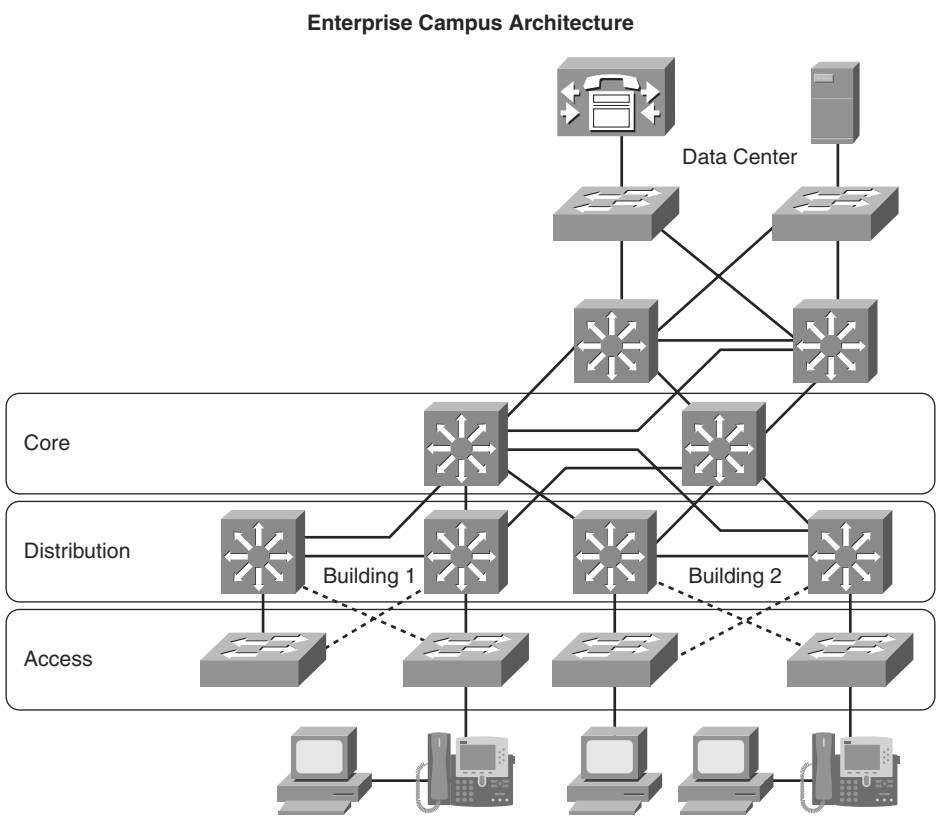


Figure 1-12 *Enterprise Network with Applied Hierarchical Design*

Access Layer In-Depth

The building access layer aggregates end users and provides uplinks to the distribution layer. With the proper use of Cisco switches, the access layer may contain the following benefits:

- **High availability:** The access layer is supported by many hardware and software features. System-level redundancy using redundant supervisor engines and redundant power supplies for critical user groups is an available option within the Cisco switch portfolio. Moreover, additional software features of Cisco switches offer access to default gateway redundancy using dual connections from access switches to redundant distribution layer switches that use first-hop redundancy protocols (FHRP) such as the hot standby routing protocol (HSRP). Of note, FHRP and HSRP features are supported only on Layer 3 switches; Layer 2 switches do not participate in HSRP and FHRP and forwarding respective frames.
- **Convergence:** Cisco switches deployed in an access layer optionally support inline Power over Ethernet (PoE) for IP telephony and wireless access points, enabling customers to converge voice onto their data network and providing roaming WLAN access for users.
- **Security:** Cisco switches used in an access layer optionally provide services for additional security against unauthorized access to the network through the use of tools such as port security, DHCP snooping, Dynamic Address Resolution Protocol (ARP) Inspection, and IP Source Guard. These features are discussed in later chapters of this book.

Figure 1-13 illustrates the use of access layer deploying redundant upstream connections to the distribution layer.

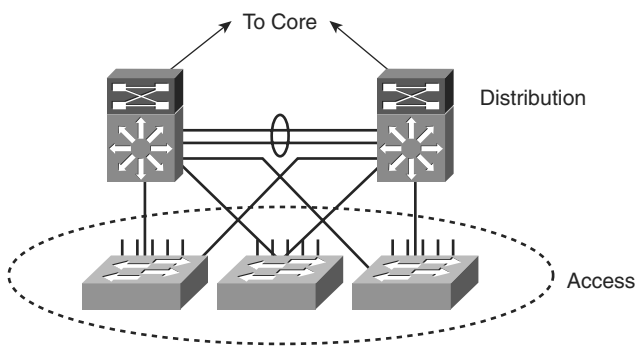


Figure 1-13 *Access Layer Depicting Two Upstream Connections*

Distribution Layer

Availability, fast path recovery, load balancing, and QoS are the important considerations at the distribution layer. High availability is typically provided through dual paths from the distribution layer to the core, and from the access layer to the distribution layer. Layer 3 equal-cost load sharing enables both uplinks from the distribution to the core layer to be utilized.

The distribution layer is the place where routing and packet manipulation are performed and can be a routing boundary between the access and core layers. The distribution layer represents a redistribution point between routing domains or the demarcation between static and dynamic routing protocols. The distribution layer performs tasks such as controlled-routing decision making and filtering to implement policy-based connectivity and QoS. To improve routing protocol performance further, the distribution layer summarizes routes from the access layer. For some networks, the distribution layer offers a default route to access layer routers and runs dynamic routing protocols when communicating with core routers.

The distribution layer uses a combination of Layer 2 and multilayer switching to segment workgroups and isolate network problems, preventing them from affecting the core layer. The distribution layer is commonly used to terminate VLANs from access layer switches. The distribution layer connects network services to the access layer and implements policies for QoS, security, traffic loading, and routing. The distribution layer provides default gateway redundancy by using an FHRP such as HSRP, Gateway Load Balancing Protocol (GLBP), or Virtual Router Redundancy Protocol (VRRP) to allow for the failure or removal of one of the distribution nodes without affecting endpoint connectivity to the default gateway.

In review, the distribution layer provides the following enhancements to the campus network design:

- Aggregates access layer switches
- Segments the access layer for simplicity
- Summarizes routing to access layer
- Always dual-connected to upstream core layer
- Optionally applies packet filtering, security features, and QoS features

Figure 1-14 illustrates the distribution layer interconnecting several access layer switches.

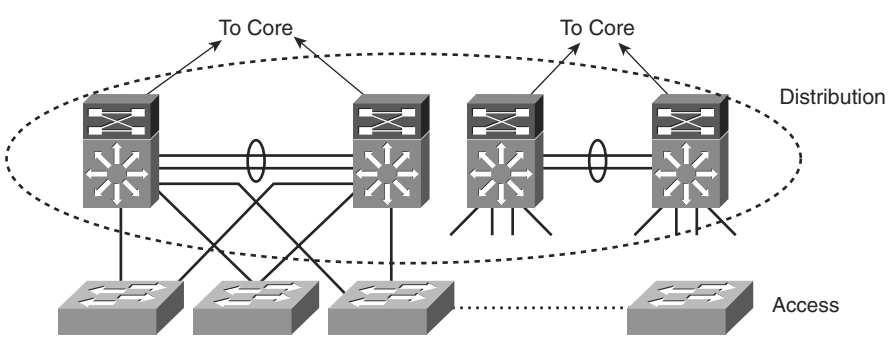


Figure 1-14 *Distribution Layer Interconnecting the Access Layer*

Core Layer

The core layer is the backbone for campus connectivity and is the aggregation point for the other layers and modules in the enterprise network. The core must provide a high level of redundancy and adapt to changes quickly. Core devices are most reliable when they can accommodate failures by rerouting traffic and can respond quickly to changes in the network topology. The core devices must be able to implement scalable protocols and technologies, alternative paths, and load balancing. The core layer helps in scalability during future growth.

The core should be a high-speed, Layer 3 switching environment utilizing hardware-accelerated services in terms of 10 Gigabit Ethernet. For fast convergence around a link or node failure, the core uses redundant point-to-point Layer 3 interconnections in the core because this design yields the fastest and most deterministic convergence results. The core layer should not perform any packet manipulation in software, such as checking access-lists and filtering, which would slow down the switching of packets. Catalyst and Nexus switches support access lists and filtering without effecting switching performance by supporting these features in the hardware switch path.

Figure 1-15 depicts the core layer aggregating multiple distribution layer switches and subsequently access layer switches.

In review, the core layer provides the following functions to the campus and enterprise network:

- Aggregates multiple distribution switches in the distribution layer with the remainder of the enterprise network
- Provides the aggregation points with redundancy through fast convergence and high availability
- Designed to scale as the distribution and consequently the access layer scale with future growth

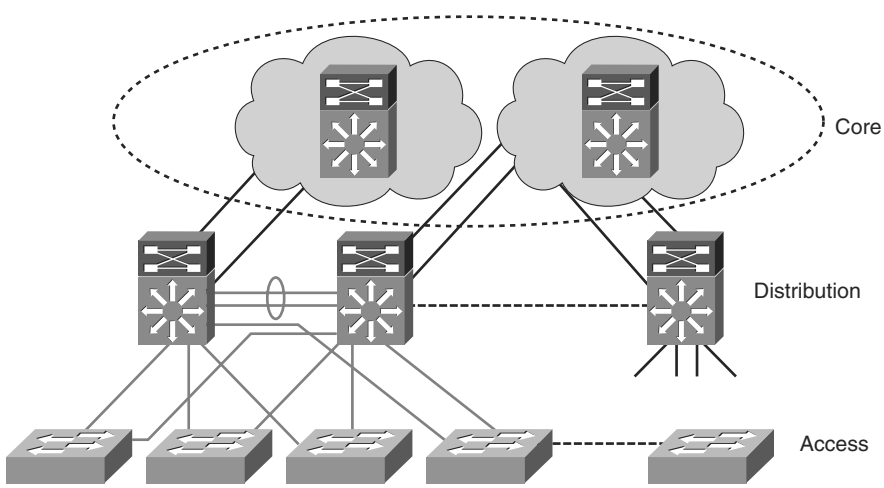


Figure 1-15 *Core Layer Aggregating Distribution and Access Layers*

The Need for a Core Layer

Without a core layer, the distribution layer switches need to be fully meshed. This design is difficult to scale and increases the cabling requirements because each new building distribution switch needs full-mesh connectivity to all the distribution switches. This full-mesh connectivity requires a significant amount of cabling for each distribution switch. The routing complexity of a full-mesh design also increases as you add new neighbors.

In Figure 1-16, the distribution module in the second building of two interconnected switches requires four additional links for full-mesh connectivity to the first module. A third distribution module to support the third building would require eight additional links to support connections to all the distribution switches, or a total of 12 links. A fourth module supporting the fourth building would require 12 new links for a total of 24 links between the distribution switches. Four distribution modules impose eight interior gateway protocol (IGP) neighbors on each distribution switch.

As a recommended practice, deploy a dedicated campus core layer to connect three or more physical segments, such as building in the enterprise campus or four or more pairs of building distribution switches in a large campus. The campus core helps make scaling the network easier when using Cisco switches with the following properties:

- 10-Gigabit and 1-Gigabit density to scale
- Seamless data, voice, and video integration
- LAN convergence optionally with additional WAN and MAN convergence

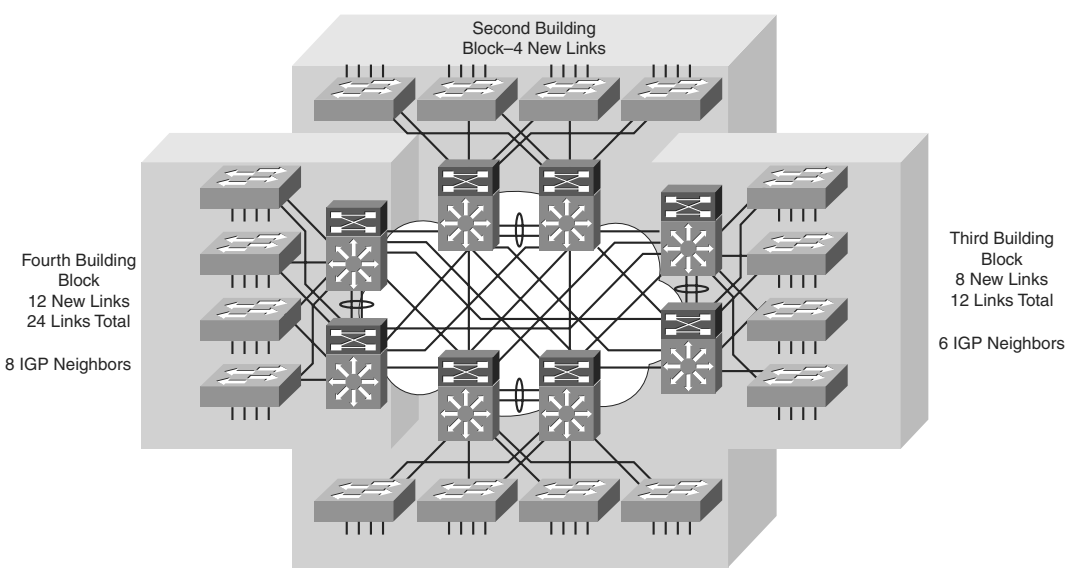


Figure 1-16 *Scaling Without Distribution Layer*

Campus Core Layer as the Enterprise Network Backbone

The core layer is the backbone for campus connectivity and optionally the aggregation point for the other layers and modules in the enterprise campus architecture. The core provides a high level of redundancy and can adapt to changes quickly. Core devices are most reliable when they can accommodate failures by rerouting traffic and can respond quickly to changes in the network topology. The core devices implement scalable protocols and technologies, alternative paths, and load balancing. The core layer helps in scalability during future growth. The core layer simplifies the organization of network device interconnections. This simplification also reduces the complexity of routing between physical segments such as floors and between buildings.

Figure 1-17 illustrates the core layer as a backbone interconnecting the data center and Internet edge portions of the enterprise network. Beyond its logical position in the enterprise network architecture, the core layer constituents and functions depend on the size and type of the network. Not all campus implementations require a campus core. Optionally, campus designs can combine the core and distribution layer functions at the distribution layer for a smaller topology. The next section discusses one such example.

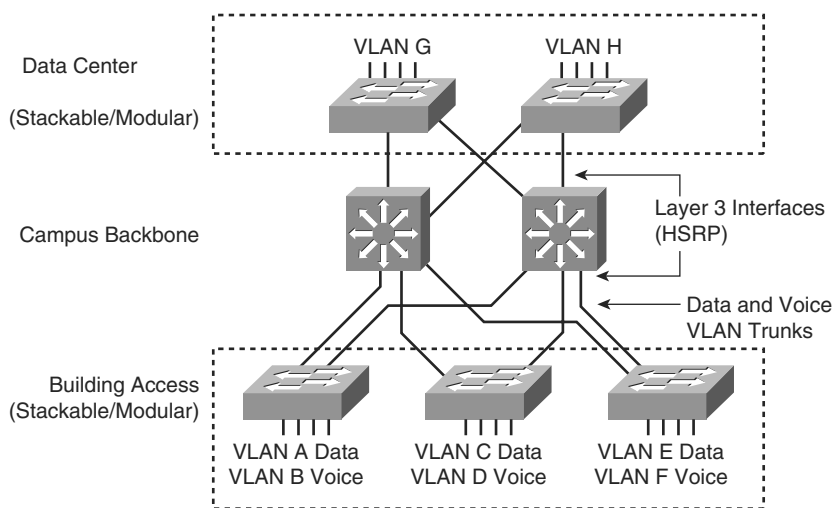


Figure 1-17 *Core Layer as Interconnect for Other Modules of Enterprise Network*

Small Campus Network Example

A small campus network or large branch network is defined as a network of fewer than 200 end devices, whereas the network servers and workstations might be physically connected to the same wiring closet. Switches in small campus network design might not require high-end switching performance or future scaling capability.

In many cases with a network of less than 200 end devices, the core and distribution layers can be combined into a single layer. This design limits scale to a few access layer switches for cost purposes. Low-end multilayer switches such as the Cisco Catalyst 3560E optionally provide routing services closer to the end user when there are multiple VLANs. For a small office, one low-end multilayer switch such as the Cisco Catalyst 2960G might support the Layer 2 LAN access requirements for the entire office, whereas a router such as the Cisco 1900 or 2900 might interconnect the office to the branch/WAN portion of a larger enterprise network.

Figure 1-17 depicts a sample small campus network with campus backbone that interconnects the data center. In this example, the backbone could be deployed with Catalyst 3560E switches, and the access layer and data center could utilize the Catalyst 2960G switches with limited future scalability and limited high availability.

Medium Campus Network Example

For a medium-sized campus with 200 to 1000 end devices, the network infrastructure is typically using access layer switches with uplinks to the distribution multilayer switches that can support the performance requirements of a medium-sized campus network. If redundancy is required, you can attach redundant multilayer switches to the building access switches to provide full link redundancy. In the medium-sized campus network, it is best practice to use at least a Catalyst 4500 series or Catalyst 6500 family of switches because they offer high availability, security, and performance characteristics not found in the Catalyst 3000 and 2000 family of switches.

Figure 1-18 shows a sample medium campus network topology. The example depicts physical distribution segments as buildings. However, physical distribution segments might be floors, racks, and so on.

Large Campus Network Design

Large campus networks are any installation of more than 2000 end users. Because there is no upper bound to the size of a large campus, the design might incorporate many scaling technologies throughout the enterprise. Specifically, in the campus network, the designs generally adhere to the access, distribution, and core layers discussed in earlier sections. Figure 1-17 illustrates a sample large campus network scaled for size in this publication.

Large campus networks strictly follow Cisco best practices for design. The best practices listed in this chapter, such as following the hierarchical model, deploying Layer 3 switches, and utilizing the Catalyst 6500 and Nexus 7000 switches in the design, scratch only the surface of features required to support such a scale. Many of these features are still used in small and medium-sized campus networks but not to the scale of large campus networks.

Moreover, because large campus networks require more persons to design, implement, and maintain the environment, the distribution of work is generally segmented. The sections of the enterprise network previously mentioned in this chapter, campus, data

center, branch/WAN and Internet edge, are the first-level division of work among network engineers in large campus networks. Later chapters discuss many of the features that might be optionally for smaller campuses that become requirements for larger networks. In addition, large campus networks require a sound design and implementation plans. Design and implementation plans are discussed in upcoming sections of this chapter.

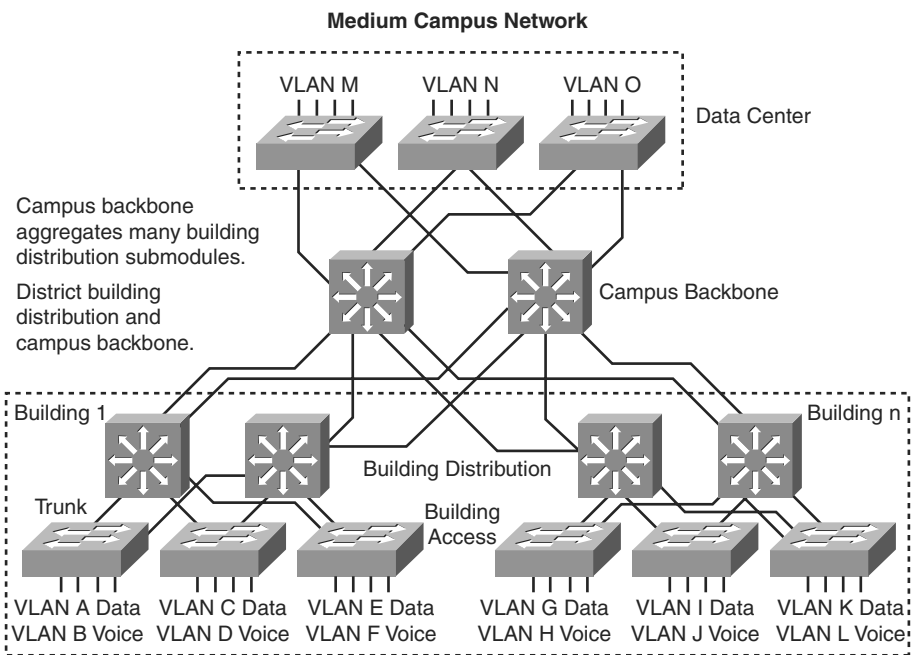


Figure 1-18 *Sample Medium Campus Network Topology*

Data Center Infrastructure

The data center design as part of the enterprise network is based on a layered approach to improve scalability, performance, flexibility, resiliency, and maintenance. There are three layers of the data center design:

- **Core layer:** Provides a high-speed packet switching backplane for all flows going in and out of the data center.
- **Aggregation layer:** Provides important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy.
- **Access layer:** Connects servers physically to the network.

Multitier HTTP-based applications supporting web, application, and database tiers of servers dominate the multitier data center model. The access layer network infrastructure can support both Layer 2 and Layer 3 topologies, and Layer 2 adjacency requirements fulfilling the various server broadcast domain or administrative requirements. Layer 2 in the access layer is more prevalent in the data center because some applications support low-latency via Layer 2 domains. Most servers in the data center consist of single and dual attached one rack unit (RU) servers, blade servers with integrated switches, blade servers with pass-through cabling, clustered servers, and mainframes with a mix of oversubscription requirements. Figure 1-19 illustrates a sample data center topology at a high level.

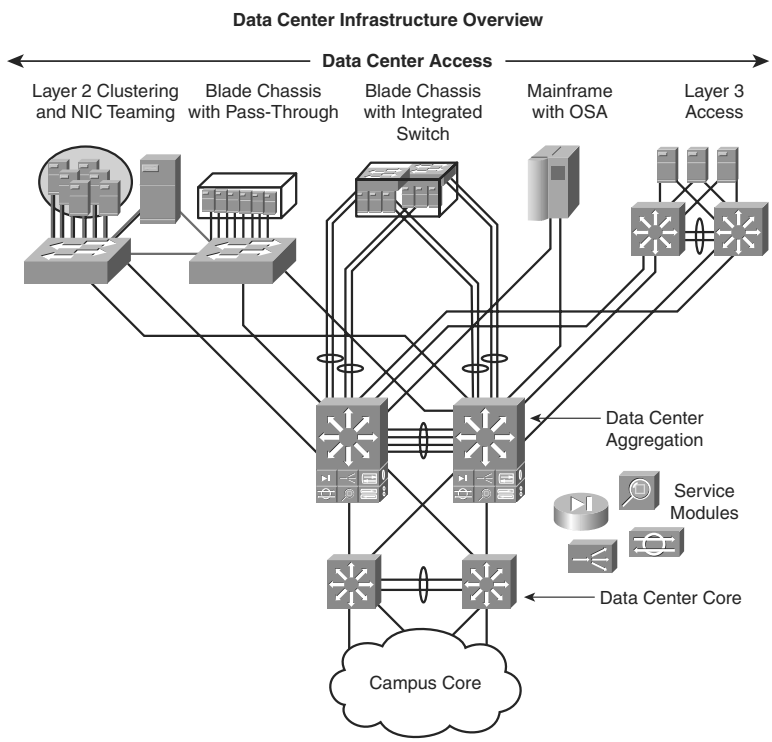


Figure 1-19 *Data Center Topology*

Multiple aggregation modules in the aggregation layer support connectivity scaling from the access layer. The aggregation layer supports integrated service modules providing services such as security, load balancing, content switching, firewall, SSL offload, intrusion detection, and network analysis.

As previously noted, this book focuses on the campus network design of the enterprise network exclusive to data center design. However, most of the topics present in this text overlap with topics applicable to data center design, such as the use of VLANs. Data center designs differ in approach and requirements. For the purpose of CCNP SWITCH, focus primarily on campus network design concepts.

The next section discusses a lifecycle approach to network design. This section does not cover specific campus or switching technologies but rather a best-practice approach to design. Some readers might opt to skip this section because of its lack of technical content; however, it is an important section for CCNP SWITCH and practical deployments.

PPDIOO Lifecycle Approach to Network Design and Implementation

PPDIOO stands for Prepare, Plan, Design, Implement, Operate, and Optimize. PPDIOO is a Cisco methodology that defines the continuous life-cycle of services required for a network.

PPDIOO Phases

The PPDIOO phases are as follows:

- **Prepare:** Involves establishing the organizational requirements, developing a network strategy, and proposing a high-level conceptual architecture identifying technologies that can best support the architecture. The prepare phase can establish a financial justification for network strategy by assessing the business case for the proposed architecture.
- **Plan:** Involves identifying initial network requirements based on goals, facilities, user needs, and so on. The plan phase involves characterizing sites and assessing any existing networks and performing a gap analysis to determine whether the existing system infrastructure, sites, and the operational environment can support the proposed system. A project plan is useful for helping manage the tasks, responsibilities, critical milestones, and resources required to implement changes to the network. The project plan should align with the scope, cost, and resource parameters established in the original business requirements.
- **Design:** The initial requirements that were derived in the planning phase drive the activities of the network design specialists. The network design specification is a comprehensive detailed design that meets current business and technical requirements, and incorporates specifications to support availability, reliability, security, scalability, and performance. The design specification is the basis for the implementation activities.
- **Implement:** The network is built or additional components are incorporated according to the design specifications, with the goal of integrating devices without disrupting the existing network or creating points of vulnerability.
- **Operate:** Operation is the final test of the appropriateness of the design. The operational phase involves maintaining network health through day-to-day operations, including maintaining high availability and reducing expenses. The fault detection, correction, and performance monitoring that occur in daily operations provide the initial data for the optimization phase.

- **Optimize:** Involves proactive management of the network. The goal of proactive management is to identify and resolve issues before they affect the organization. Reactive fault detection and correction (troubleshooting) is needed when proactive management cannot predict and mitigate failures. In the PPDIOO process, the optimization phase can prompt a network redesign if too many network problems and errors arise, if performance does not meet expectations, or if new applications are identified to support organizational and technical requirements.

Note Although design is listed as one of the six PPDIOO phases, some design elements can be present in all the other phases. Moreover, use the six PPDIOO phases as a model or framework; it is not necessary to use it exclusively as defined.

Benefits of a Lifecycle Approach

The network lifecycle approach provides several key benefits aside from keeping the design process organized. The main documented reasons for applying a lifecycle approach to campus design are as follows:

- Lowering the total cost of network ownership
- Increasing network availability
- Improving business agility
- Speeding access to applications and services

The total cost of network ownership is especially important into today's business climate. Lower costs associated with IT expenses are being aggressively assessed by enterprise executives. Nevertheless, a proper network lifecycle approach aids in lowering costs by these actions:

- Identifying and validating technology requirements
- Planning for infrastructure changes and resource requirements
- Developing a sound network design aligned with technical requirements and business goals
- Accelerating successful implementation
- Improving the efficiency of your network and of the staff supporting it
- Reducing operating expenses by improving the efficiency of operational processes and tools

Network availability has always been a top priority of enterprises. However, network downtime can result in a loss of revenue. Examples of where downtime could cause loss of revenue is with network outages that prevent market trading during a surprise interest rate cut or the inability to process credit card transactions on black Friday, the shopping day following Thanksgiving. The network lifecycle improves high availability of networks by these actions:

- Assessing the network's security state and its capability to support the proposed design
- Specifying the correct set of hardware and software releases, and keeping them operational and current
- Producing a sound operations design and validating network operations
- Staging and testing the proposed system before deployment
- Improving staff skills
- Proactively monitoring the system and assessing availability trends and alerts
- Proactively identifying security breaches and defining remediation plans

Enterprises need to react quickly to changes in the economy. Enterprises that execute quickly gain competitive advantages over other businesses. Nevertheless, the network lifecycle gains business agility by the following actions:

- Establishing business requirements and technology strategies
- Readying sites to support the system that you want to implement
- Integrating technical requirements and business goals into a detailed design and demonstrating that the network is functioning as specified
- Expertly installing, configuring, and integrating system components
- Continually enhancing performance

Accessibility to network applications and services is critical to a productive environment. As such, the network lifecycle accelerates access to network applications and services by the following actions:

- Assessing and improving operational preparedness to support current and planned network technologies and services
- Improving service-delivery efficiency and effectiveness by increasing availability, resource capacity, and performance
- Improving the availability, reliability, and stability of the network and the applications running on it
- Managing and resolving problems affecting your system and keeping software applications current

Note The content of this book focuses on the prepare phase, plan phase, and design phases of the PPDIOO process as applied to building an enterprise campus network.

Planning a Network Implementation

The more detailed the implementation plan documentation is, the more likely the implementation will be a success. Although complex implementation steps usually require the designer to carry out the implementation, other staff members can complete

well-documented detailed implementation steps without the direct involvement of the designer. In practical terms, most large enterprise design engineers rarely perform the hands-on steps of deploying the new design. Instead, network operations or implementation engineers are often the persons deploying a new design based on an implementation plan.

Moreover, when implementing a design, you must consider the possibility of a failure, even after a successful pilot or prototype network test. You need a well-defined, but simple, process test at every step and a procedure to revert to the original setup in case there is a problem.

Note It is best-practice to lay out implementation steps in a tabular form and review those steps with your peers

Implementation Components

Implementation of a network design consists of several phases (install hardware, configure systems, launch into production, and so on). Each phase consists of several steps, and each step should contain, but be not limited to, the following documentation:

- Description of the step
- Reference to design documents
- Detailed implementation guidelines
- Detailed roll-back guidelines in case of failure
- Estimated time needed for implementation

Summary Implementation Plan

Table 1-3 provides an example of an implementation plan for migrating users to new campus switches. Implementations can vary significantly between enterprises. The look and feel of your actual implementation plan can vary to meet the requirements of your organization.

Each step for each phase in the implementation phase is described briefly, with references to the detailed implementation plan for further details. The detailed implementation plan section should describe the precise steps necessary to complete the phase.

Table 1-3 *Sample Summary Implementation Plan*

Phase	Date, Time	Description	Implementation Details	Completed
Phase 3	12/26/2010 1:00 a.m. EST	Installs new campus switches	Section 6.2.3	Yes
Step 1		Installs new modules in campus backbone to support new campus switches	Section 6.2.3.1	Yes
Step 2		Interconnects new campus switches to new modules in campus backbone	Section 6.2.3.2	Yes
Step 3		Verifies cabling	Section 6.2.3.3	
Step 4		Verifies that interconnects have links on respective switches	Section 6.2.3.4	
Phase 4	12/27/2010 1:00 a.m. EST	Configures new campus switches and new modules in campus backbone	Section 6.2.4.1	
Step 1		Loads standard configuration file into switches for network management, switch access, and so on	Section 6.2.4.2	
Step 2		Configures Layer 3 interfaces for IP address and routing configuration on new modules in campus backbone	Section 6.2.4.3	
Step 3		Configures Layer 3 interfaces for IP address and routing info on new campus switches	Section 6.2.4.4	
Step 4		Configures Layer 2 features such as VLAN, STP, and QoS on new campus switches	Section 6.2.4.5	

continues

Table 1-3 *Sample Summary Implementation Plan (continued)*

Phase	Date, Time	Description	Implementation Details	Completed
Step 5		Tests access layer ports on new campus switches by piloting access for a few enterprise applications	Section 6.2.4.6	
Phase 5	12/28/2010 1:00 a.m. EST	Production implementation	Section 6.2.5	
Step 1		Migrate users to new campus switches	Section 6.2.5.1	
Step 2		Verifies migrated workstations can access enterprise applications	Section 6.2.5.2	

Detailed Implementation Plan

A detailed implementation plan describes the exact steps necessary to complete the implementation phase. It is necessary to includes steps to verify and check the work of the engineers implementing the plan. The following list illustrates a sample network implementation plan:

Section 6.2.4.6, "Configure Layer 2 features such as VLAN, STP, and QoS on new campus switches"

- Number of switches involved: 8
- Refer to Section 1.1 for physical port mapping to VLAN
- Use configuration template from Section 4.2.3 for VLAN configuration
- Refer to Section 1.2 for physical port mapping to spanning-tree configuration
- Use configuration template from Section 4.2.4 for spanning-tree configuration
- Refer to Section 1.3 for physical port mapping to QoS configuration
- Use configuration template from Section 4.2.5 for QoS configuration
- Estimate configuration time to be 30 minutes per switch
- Verify configuration preferable by another engineer

This section highlighted the key concepts around PPDIOO. Although this topic is not a technical one, the best practices highlighted will go a long way with any network design

and implementation plan. Poor plans will always yield poor results. Today's networks are too critical for business operations not to plan effectively. As such, reviewing and utilizing the Cisco Lifecycle will increase the likelihood of any network implementation.

Summary

Evolutionary changes are occurring within the campus network. One example is the migration from a traditional/Layer 2 access-switch design (with its requirement to span VLANs and subnets across multiple access switches) to a virtual switch-based design. Another is the movement from a design with subnets contained within a single access switch to the routed-access design. This evolvement requires careful planning and deployments. Hierarchical design requirements along with other best practices are detailed throughout the remainder of this book to ensure a successful network.

As the network evolves, new capabilities are added, such as virtualization of services or mobility. The motivations for introducing these capabilities to the campus design are many. The increase in security risks, the need for a more flexible infrastructure, and the change in application data flows have all driven the need for a more capable architecture. However, implementing the increasingly complex set of business-driven capabilities and services in the campus architecture can be challenging if done in a piece meal fashion. Any successful architecture must be based on a foundation of solid design theory and principles. For any enterprise business involved in the design and operation of a campus network, the adoption of an integrated approach based on solid systems design principles, is a key to success.

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers are found in Appendix A, "Answers to Chapter Review Questions."

1. The following statement describes which part of the enterprise network that is understood as the portion of the network infrastructure that provides access to services and resources to end users and devices that are spread over a single geographic location?

   a. Campus

   b. Data center

   c. Branch/WAN

   d. Internet Edge

2. The following statement describes which part of the enterprise network that is generally understood to be the facility used to house computing systems and associated components and was original referred to as the server farm?

   a. Campus

   b. Data center

   c. Branch/WAN

   d. Internet Edge

3. This area of the enterprise network was originally referred to as the server farm.

   a. Campus

   b. Data center

   c. Branch/WAN

   d. Internet Edge

4. Which of the following are characteristics of a properly designed campus network?

   a. Modular

   b. Flexible

   c. Scalable

   d. Highly available

5. Layer 2 networks were originally built to handle the performance requirements of LAN interconnectivity, whereas Layer 3 routers could not accommodate multiple interfaces running at near wire-rate speed. Today, Layer 3 campus LAN networks can achieve the same performance of Layer 2 campus LAN networks due to the following technology change:

   a. Layer 3 switches are now built using specialized components that enable similar performance for both Layer 2 and Layer 3 switching.

   b. Layer 3 switches can generally switch packets faster than Layer 2 switches.

   c. Layer 3 switches are now built using multiple virtual routers enabling higher speed interfaces.

6. Why are Layer 2 domains popular in data center designs?

   a. Data centers do not require the same scalability as the campus network.

   b. Data centers do not require fast convergence.

   c. Data centers place heavier emphasis on low-latency, whereas some applications operate at Layer 2 in an effort to reduce Layer 3 protocol overhead.

   d. Data centers switches such as the Nexus 7000 are Layer 2-only switches.

7. In the content of CCNP SWITCH and this book, what number of end devices or users quantifies as a small campus network?

   a. Up to 200 users

   b. Up to 2000 users

   c. Between 500 to 2500 users

   d. Between 1000 to 10,000 users

8. In the context of CCNP SWITCH and this book, what number of end devices or user quantifies a medium-sized campus network?

   a. A message digest encrypted with the sender's private key

   b. Up to 200 users

   c. Up to 2000 users

   d. Between 500 to 2500 users

   e. Between 1000 to 10,000 users

9. Why are hierarchical designs used with layers as an approach to network design?

   a. Simplification of large-scale designs.

   b. Reduce complexity of troubleshooting analysis.

   c. Reduce costs by 50 percent compared to flat network designs.

   d. Packets that move faster through layered networks reduce latency for applications.

10. Which of the following is not a Layer 2 switching feature? You might need to consult later chapters for guidance in answering this question; there might be more than one answer.

    a. Forwarding based upon the destination MAC address

    b. Optionally supports frame classification and quality of service

    c. IP routing

    d. Segmenting a network into multiple broadcast domains using VLANs

    e. Optionally applies network access security

11. Which of the following switches support(s) IP routing?

    a. Catalyst 6500

    b. Catalyst 4500

    c. Catalyst 3750, 3560E

    d. Catalyst 2960G

    e. Nexus 7000

    f. Nexus 5000

12. Which of the following switches support(s) highly available power via integrated redundant power?

- **a.** Catalyst 6500
- **b.** Catalyst 4500
- **c.** Catalyst 3750, 3560E
- **d.** Catalyst 2960G
- **e.** Nexus 7000
- **f.** Nexus 5000

13. Which of the following switches support(s) redundant supervisor/routing engines?

- **a.** Catalyst 6500
- **b.** Catalyst 4500
- **c.** Catalyst 3750, 3560E
- **d.** Catalyst 2960G
- **e.** Nexus 7000
- **f.** Nexus 5000

14. Which of the following switches use(s) a modular architecture for additional scalability and future growth?

- **a.** Catalyst 6500
- **b.** Catalyst 4500
- **c.** Catalyst 3750, 3560E
- **d.** Catalyst 2960G
- **e.** Nexus 7000
- **f.** Nexus 5000

15. Which of the following traffic generally utilizes more network bandwidth than other traffic types?

- **a.** IP telephony
- **b.** Web traffic
- **c.** Network Management
- **d.** Apple iPhone on Wi-Fi campus network
- **e.** IP multicast

16. Which of the following are examples of peer-to-peer applications?

- **a.** Video conferencing
- **b.** IP phone calls
- **c.** Workstation-to-workstation file sharing
- **d.** Web-based database application
- **e.** Inventory management tool

17. Which of the following are examples of client-server applications?

- **a.** Human resources user tool
- **b.** Company wiki
- **c.** Workstation-to-workstation file sharing
- **d.** Web-based database application
- **e.** Apple iTunes media sharing

18. A small-sized campus network might combine which two layers of the hierarchical model?

- **a.** Access and distribution
- **b.** Access and core
- **c.** Core and distribution

19. In a large-sized enterprise network, which defined layer usually interconnects the data center, campus, Internet edge, and branch/WAN sections.

- **a.** Specialized access layer
- **b.** Four fully meshed distribution layers
- **c.** Core backbone

20. Which layer of the campus network are Layer 2 switches most likely to be found in a medium-sized campus network if at all?

- **a.** Core layer
- **b.** Distribution layer
- **c.** Access layer

21. SONA is an architectural framework that guides the evolution of _____?

- **a.** Enterprise networks to integrated applications
- **b.** Enterprise networks to a more intelligent infrastructure
- **c.** Commercial networks to intelligent network services

d. Enterprise networks to intelligent network services

e. Commercial networks to a more intelligent infrastructure

22. SONA Which are the three layers of SONA?

a. Integrated applications layer

b. Application layer

c. Interactive services layer

d. Intelligent services layer

e. Networked infrastructure layer

f. Integrated transport layer

23. Which of the following best describe the core layer as applied to the campus network?

a. A fast, scalable, and high-available Layer 2 network that interconnects the different physical segments such as buildings of a campus

b. A point to multipoint link between the headquarters and the branches, usually based on a push technology

c. A fast, scalable, and high-available Layer 3 network that interconnects the different physical segments such as buildings of a campus

d. The physical connections between devices, also known as the physical layer

24. Which of the following best describes the relationship between the data center and the campus backbone?

a. The campus backbone interconnects the data center to the campus core layer.

b. The data center devices physically connect directly to the Enterprise Distribution Layer switches.

c. The data center devices physically connect to access switches.

d. The data center devices connection model is different from the Layer 3 model used for the rest of the enterprise network

25. List the phases of the Cisco Lifecycle approach in the correct order.

a. Propose

b. Implement

c. Plan

d. Optimize

e. Prepare

f. Inquire

g. Design

h. Document

i. Operate

26. Which three are considered to be technical goals of the Cisco Lifecycle approach?

a. Improving security

b. Simplifying network management

c. Increasing competitiveness

d. Improving reliability

e. Increasing revenue

f. Improving customer support

27. When implementing multiple complex components, which of the following is the most-efficient approach per the PPDIOO model?

a. Implement each component one after the other, test to verify at each step.

b. Implement all components simultaneously for efficiency reasons.

c. Implement all components on a per physical location approach.

This page intentionally left blank

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q

R

S

T

U

V

W-X-Y-Z