CCDA Official Exam Certification Guide

Third Edition

Anthony Bruno, CCIE No. 2738

Steve Jordan, CCIE No. 11293

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

CCDA Official Exam Certification Guide, Third Edition

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

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

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing June 2007

Library of Congress Cataloging-in-Publication Data

Bruno, A. Anthony.

CCDA official exam certification guide / Anthony Bruno, Steve Jordan. —3rd ed.

p. cm.

ISBN-13: 978-1-58720-177-6 (hardcover w/dvd) 1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. I. Jordan, Steve. II. Title.

QA76.3.B7847 2007

004.6076--dc22

2007015940

ISBN-10: 1-58720-177-1

ISBN-13: 978-1-58720-177-6

Warning and Disclaimer

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Corporate and Government Sales

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

For sales outside of the U.S. please contact: **International Sales** 1-317-581-3793 international@pearsontechgroup.com

Trademark Acknowledgments

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

Publisher: Paul Boger

Associate Publisher: David Dusthimer

Executive Editor: Brett Bartow

Cisco Representative: Anthony Wolfenden

Managing Editor: Patrick Kanouse

Cisco Press Program Manager: Jeff Brady

Development Editor: Andrew Cupp

Technical Editors: Mark Gallo, Steve Jordan, and Anthony Sequeira

Senior Project Editor: Tonya Simpson

Copy Editor: Gayle Johnson

Publishing Coordinator: Vanessa Evans

Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright

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

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

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

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

About the Authors

Anthony Bruno, CCIE No. 2738, is a senior principal consultant with British Telecom with more than 17 years of experience in the internetworking field. Previously, he worked for International Network Services. His other network certifications include CISSP, CCDP, CCVP, and CWNA. He has consulted for many enterprise and service-provider customers in the design, implementation, and optimization of large-scale data and IP telephony networks. He completed his MSEE at the University of Missouri–Rolla in 1994 and his BSEE at the University of Puerto Rico–Mayaguez in 1990. He is also a part-time instructor for the University of Phoenix–Online, teaching networking courses.

Steve Jordan, CCIE No. 11293, is a senior consultant with British Telecom with more than 11 years of experience in internetworking. Previously, he worked for International Network Services. His other network certifications include CCDP, CCSP, and CCVP. He specializes in security, internetworking, and voice technologies. He has extensive experience with large-scale data center environments and has designed and implemented various network solutions in the manufacturing, telecommunication, and transportation industries. Steve was also a technical reviewer for this book.

About the Technical Reviewers

Mark Gallo is a systems engineering manager at Cisco within the Channels organization. He has led several engineering groups responsible for positioning and delivering Cisco end-to-end systems, as well as designing and implementing enterprise LANs and international IP networks. He has a BS in electrical engineering from the University of Pittsburgh and holds CCNP and CCDP certifications. He resides in northern Virginia with his wife, Betsy, and son, Paul.

Anthony Sequeira, CCIE No. 15626, completed the CCIE in Routing and Switching in January 2006. He is currently pursuing the CCIE in Security. For the past ten years he has written and lectured to massive audiences about the latest in networking technologies. He currently is a senior technical instructor and certified Cisco instructor for Thomson NETg. He lives with his wife and daughter in Florida. When he is not reading about the latest Cisco innovations, he is training for the World Series of Poker or exploring the Florida skies in a Cessna.

Dedications

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

—Anthony Bruno

This book is dedicated to my wife of 13 years, Dorin, and to our sons, Blake, Lance, and Miles, for their support during the writing of this book. For Blake, Lance, and Miles, we can now go fishing and golfing much more! I would also like to dedicate this book to my loving family in Tampa, Florida and Jackson, Mississippi.

—Steve Jordan

Acknowledgments

This book would not have been possible without the efforts of many dedicated people. Thanks to Andrew Cupp, development editor, for his guidance and special attention to detail. Thanks to Tonya Simpson, senior project editor, for her accuracy. Thanks to Brett Bartow, executive editor, for his vision. Thanks to all other Cisco Press team members who worked behind the scenes to make this a better book.

A special thanks my coauthor, Steve Jordan, for stepping in and contributing four chapters in addition to performing the technical review of my chapters. And a special thanks to the other technical reviewers, Mark Gallo and Anthony Sequeira. Their technical advice and careful attention to detail made this book accurate. Also, thanks to DL—you are the best!

—Anthony Bruno

This book would not be possible without all the great people who have assisted me. I would first like to thank Anthony Bruno for inviting me to assist him in this endeavor. Thanks to Brett Bartow, executive editor, for his guidance and support during the project. Thanks to Andrew Cupp, development editor, for supporting my schedule delays and keeping me on track.

Special thanks to the technical reviewers, Mark Gallo and Anthony Sequeira, who helped with the accuracy of this book.

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

—Steve Jordan

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to http://www.ciscopress.com/safarienabled
- Complete the brief registration form
- Enter the coupon code DNEN-JAPD-QVWI-HCDJ-GFLT

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Contents at a Glance

Contents

Command Syntax Conventions

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

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Foreword

CCDA Official Exam Certification Guide, Third Edition, is an excellent self-study resource for the 640-863 DESGN exam. Passing the exam validates your knowledge of network design for Cisco converged networks based on SONA (the Cisco Service-Oriented Network Architecture). Passing the exam is required for the Cisco Certified Design Associate (CCDA) certification.

Gaining certification in Cisco technology is key to the continuing educational development of today's networking professional. Through certification programs, Cisco validates the skills and expertise required to effectively manage the modern enterprise network.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in your field of expertise, or to gain new skills. Whether used as a supplement to more traditional training or as a primary source of learning, these materials offer users the information and knowledge validation required to gain new understanding and proficiencies.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco. They offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit www.cisco.com/go/training.

I hope that you find these materials to be an enriching and useful part of your exam preparation.

Erik Ullanderson
Manager, Global Certifications
Learning@Cisco
March 2007

Introduction

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

Cisco Certified Design Associate (CCDA) is the entry-level certification that represents knowledge of the design of Cisco internetwork infrastructure.

The routing and switching path has various levels of certification. CCDA is the entry-level certification in the network design track. The next step, Cisco Certified Design Professional (CCDP), requires you to demonstrate advanced knowledge of network design. The Cisco Certified Internetwork Expert (CCIE) requires an expert level of knowledge about internetworking.

The test to obtain CCDA certification is called Designing for Cisco Internetwork Solutions (DESGN) Exam #640-863. It is a computer-based test that has 65 questions and a 90-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for course and exam updates at http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html.

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

The CCDA exam measures your ability to design networks that meet certain requirements for performance, security, capacity, and scalability. The exam focuses on small- to medium-sized networks. The candidate should have at least one year of experience in the design of small- to medium-sized networks using Cisco products. A CCDA candidate should understand internetworking technologies, including the Enterprise Composite Network Model, routing, switching, WAN technologies, LAN protocols, security, IP telephony, and network management.

Cisco suggests taking the DESGN course before you take the CCDA exam. For more information on the various levels of certification, career tracks, and Cisco exams, go to the Cisco Certifications page at http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html.

Strategies for Exam Preparation

The strategy you use for the CCDA test might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the DESGN course, you might take a different approach than someone who learned switching via on-the-job training.

Regardless of the strategy you use or your background, this book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about IP addressing and subnetting if you fully understand them already. However, many people like to make sure that they truly know a topic and thus read material they already know. This book's features will make you confident that you know some of the material already and also will help you figure out what topics you need to study more.

The following are some additional suggestions for using this book and preparing for the exam:

- Familiarize yourself with the exam topics in Table I-1, and thoroughly read the chapters on topics you are unfamiliar with. Use the assessment tools provided in this book to identify areas where you need additional study. The assessment tools include the "Do I Know This Already?" quizzes, the "Q&A" questions, and the sample exam questions on the CD-ROM.
- Take all quizzes in this book, and review the answers and their explanations. It is not enough to know the correct answer; you also need to understand why it is correct and why the other possible answers are incorrect. Retake the chapter quizzes until you pass with 100 percent.
- Take the CD-ROM test included with this book, and review the answers. Use your results to identify areas where you need additional preparation.
- Review other documents, RFCs, and the Cisco website for additional information. If this book references an outside source, it's a good idea to spend some time looking at it.
- Review the chapter questions and CD-ROM questions the day before your test. Review each chapter's "Foundation Summary" when you are making your final preparations.
- On the test date, arrive at least 20 minutes before your test time. This gives you time to register and glance through your notes before the test without feeling rushed or anxious.
- If you are unsure of the correct answer to a question, attempt to eliminate the incorrect answers.
- You might need to spend more time on some questions than others. Remember, you have a little over 1 minute to answer each question.

How This Book Is Organized

This book is divided into the following parts:

Part I: General Network Design (Chapters 1 and 2)
Part II: LAN and WAN Design (Chapters 3 through 6)
Part III: The Internet Protocol and Routing Protocols (Chapters 7 through 12)
Part IV: Security, Convergence, and Network Management (Chapters 13 through 16)
Part V: Comprehensive Scenarios (Chapter 17)
Part VI: Appendixes (Appendixes A and B)

The "CCDA Exam Topics" section describes the design topics that are covered on the CCDA exam. Before you begin studying for any exam, it is important that you know which topics might be covered. With the CCDA exam, knowing what is on the exam is seemingly straightforward, because Cisco publishes a list of CCDA exam topics. The topics, however, are open to interpretation.

Chapters 1 through 16 cover the Cisco CCDA exam design topics and provide detailed information on each topic. Each chapter begins with a quiz so that you can quickly determine your current level of readiness. Each chapter ends with a review summary and Q&A quiz. Chapter 17, "Comprehensive Scenarios," provides scenario-based questions for further comprehensive study. Some of the questions on the CCDA test might be based on a scenario design.

Finally, in the back of the book you will find an invaluable CD-ROM. The companion CD-ROM contains a powerful testing engine that allows you to focus on individual topic areas or take complete, timed exams. The assessment engine also tracks your performance and provides feedback on a topic-by-topic basis, presenting question-by-question remediation to the text. The practice exam has a database of more than 200 questions, so you can test yourself more than once. Questions can also be delivered in standard exam format or flash card format, and you can choose to randomly generate tests or focus on specific topic areas.

The following summarizes the chapters and appendixes in this book:

- **Chapter 1, "Network Design Methodology,"** discusses obtaining organization requirements, IIR, SONA, PPDIOO methodology, and the process of completing a network design.
- **Chapter 2, "Network Structure Models,"** discusses network hierarchical models and the Enterprise Converged Network Model.
- **Chapter 3, "Enterprise LAN Design,"** covers design models and technologies used in the campus local-area networks.
- **Chapter 4, "Wireless LAN Design,"** covers the technologies and design options for wireless LANs.

- **Chapter 5, "WAN Technologies,"** examines the use of wide-area network technologies for the enterprise edge.
- **Chapter 6, "WAN Design,"** covers WAN designs for the enterprise WAN and enterprise branch.
- **Chapter 7, "Internet Protocol Version 4,"** covers the header, addressing, and protocols used by IPv4.
- **Chapter 8, "Internet Protocol Version 6,"** covers the header, addressing, and protocols used by IPv6.
- **Chapter 9, "Routing Protocol Selection Criteria,"** covers routing protocol characteristics and metrics.
- **Chapter 10, "RIP and EIGRP Characteristics and Design,"** covers the distance vector routing protocols RIPv1, RIPv2, RIPng, EIGRP, and EIGRP for IPv6.
- **Chapter 11, "OSPF and IS-IS,"** covers the link-state routing protocols OSPFv2, OSPFv3, and IS-IS.
- **Chapter 12, "Border Gateway Protocol, Route Manipulation, and IP Multicast,"** covers Border Gateway Protocol, route summarization and redistribution, and multicast protocols.
- **Chapter 13, "Security Management,"** covers network security in terms of security management and policy.
- **Chapter 14, "Security Technologies and Design,"** covers Cisco's security technologies and security solutions for the enterprise edge.
- **Chapter 15, "Traditional Voice Architectures and IP Telephony Design,"** covers traditional TDM-based concepts and solutions, VoIP protocols, and Cisco's Unified IP telephony solutions.
- **Chapter 16, "Network Management Protocols,"** covers network management design, the FCAPS model, SNMP, RMON, and other network management protocols.
- **Chapter 17, "Comprehensive Scenarios,"** provides network case studies for further comprehensive study.
- **Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections,"** provides the answers to the various chapter quizzes.
- **Appendix B, "The OSI Reference Model, TCP/IP Architecture, and Numeric Conversion,"** reviews the Open Systems Interconnection (OSI) reference model to give you a better understanding of internetworking. It reviews the TCP/IP architecture and also reviews the techniques to convert between decimal, binary, and hexadecimal numbers. Although there might not be a specific question on the exam about converting a binary number to decimal, you need to know how to do so to do problems on the test.

Features of This Book

This book features the following:

- **"Do I Know This Already?" Quizzes**—Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter. If you follow the directions at the beginning of the chapter, the "Do I Know This Already?" quiz directs you to study all or particular parts of the chapter.
- **Foundation Topics**—These are the core sections of each chapter. They explain the protocols, concepts, and configuration of the topics in that chapter. If you need to learn about the topics in a chapter, read the "Foundation Topics" section.
- **Foundation Summaries**—Near the end of each chapter, a summary collects the most important information from the chapter. The "Foundation Summary" section is designed to help you review the key concepts in the chapter if you scored well on the "Do I Know This Already?" quiz. This section is an excellent tool for last-minute review.
- **Q&A**—Each chapter ends with a "Q&A" section that forces you to recall the facts and processes described in that chapter. The questions are generally similar than the actual exam. These questions are a great way to improve your recollection of the facts.
- **CD-ROM test questions**—Using the test engine on the CD-ROM, you can take simulated exams. You can also choose to be presented with several questions on a topic that you need more work on. This testing tool provides you with practice to make you more comfortable when you take the CCDA exam.

CCDA Exam Topics

Cisco lists the topics of the CCDA exam on its website at http://www.cisco.com/web/learning/le3/current_exams/640-863.html. The list provides key information about what the test covers. Table I-1 lists the CCDA exam topics and the corresponding parts in this book that cover those topics. Each part begins with a list of the topics covered. Use these references as a road map to find the exact materials you need to study to master the CCDA exam topics. Note, however, that all exam information is managed by Cisco Systems and is subject to change. Therefore, you should continually monitor the Cisco Systems site at www.cisco.com for course and exam updates.

Table I-1 *CCDA Topics and the Parts Where They Are Covered*

Topic	Part
Describe the Methodology Used to Design a Network	
Describe the Cisco Service-Oriented Network Architecture	I
Identify Network Requirements to Support the Organization	I
Characterize an Existing Network	I
Describe the Top Down Approach to Network Design	I
Describe Network Management Protocols and Features	IV
Describe Network Structure and Modularity	
Describe the Network Hierarchy	I
Describe the Modular Approach in Network Design	I
Describe the Cisco Enterprise Architecture	I
Design Basic Enterprise Campus Networks	
Describe Campus Design Considerations	II
Design the Enterprise Campus Network	II
Design the Enterprise Data Center	II
Design Enterprise Edge and Remote Network Modules	
Describe the Enterprise Edge, Branch, and Teleworker Design Characteristics	II
Describe the Functional Components of the Central Site Enterprise Edge	II
Describe WAN Connectivity Between Two Campuses	II
Design the Branch Office WAN Solutions	II
Describe Access Network Solutions for a Teleworker	II
Design the WAN to Support Selected Redundancy Methodology	II
Identify Design Considerations for a Remote Data Center	II
Design IP Addressing and Routing Protocols	
Describe IPv4 & IPv6 Addressing	III
Identify Routing Protocol Considerations in an Enterprise Network	III
Design a Routing Protocol Deployment	III
Design Security Services	
Describe the Security Lifecycle	IV
Identify Cisco Technologies to Mitigate Security Vulnerabilities	IV
Select Appropriate Cisco Security Solutions and Deployment Placement	IV

Table I-1 *CCDA Topics and the Parts Where They Are Covered (Continued)*

Topic	Part
Identify Voice Networking Considerations	
Describe Traditional Voice Architectures and Features	IV
Describe Cisco IP Telephony	IV
Identify the Design Considerations for Voice Services	IV
Identify Wireless Networking Considerations	
Describe Cisco Unified Wireless Network Architectures and Features	II
Design Wireless Network Using Controllers	II
Design Wireless Network Using Roaming	II

In addition, the comprehensive scenarios in Part V test your knowledge of an overall combination of the CCDA exam topics.

If your knowledge of a particular chapter's subject matter is strong, you might want to proceed directly to that chapter's Q&A to assess your true level of preparedness. If you have difficulty with those questions, be sure to read that chapter's "Foundation Topics." Also, be sure to test yourself by using the CD-ROM's test engine.

This part covers the following CCDA exam topics (to view the CCDA exam overview, visit http://www.cisco.com/web/learning/le3/current_exams/640-863.html):

- Describe the Cisco Service-Oriented Network Architecture
- Identify Network Requirements to Support the Organization
- Characterize an Existing Network
- Describe the Top Down Approach to Network Design
- Describe the Network Hierarchy
- Describe the Modular Approach in Network Design
- Describe the Cisco Enterprise Architecture

Part I: General Network Design

This chapter covers the following subjects:

- Intelligent Information Network and Service-Oriented Network Architecture
- Prepare, Plan, Design, Implement, Operate, and Optimize Phases
- Identifying Customer Requirements
- Characterizing the Existing Network
- Designing the Network Topology and Solutions

CHAPTER 1

Network Design Methodology

Networks can become complex and difficult to manage. Network architectures and design methodologies help you manage the complexities of networks. This chapter provides an overview of Cisco's Service-Oriented Network Architecture (SONA) as part of Cisco's vision of the Intelligent Information Network (IIN). This chapter also describes the six network life cycle phases and steps in design methodology.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

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

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

Foundation Topics Section	Questions Covered in This Section
Intelligent Information Network and Service-Oriented Network Architecture	1, 2, 3, 4
Prepare, Plan, Design, Implement, Operate, and Optimize Phases	5, 6
Identifying Customer Requirements	9, 10
Characterizing the Existing Network	7
Designing the Network Topology and Solutions	8

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. What are the three phases of IIN?
   a. Application, Interactive Services, Network Infrastructure
   b. Transport, Service, Application Integration
   c. Policy, System, Service Integration
   d. SONA, Enterprise Architecture, SONA framework
2. What are the three layers of SONA?
   a. Application, Interactive Services, Network Infrastructure
   b. Transport, Service, Application Integration
   c. Policy, System, Service Integration
   d. SONA, Enterprise Architecture, SONA framework
3. Virtualization occurs in which layer of the SONA framework?
   a. Application layer
   b. Virtual layer
   c. Interactive Service layer
   d. Infrastructure Service layer
4. Which of the following is a collaboration application?
   a. Supply chain
   b. IPCC
   c. Product Life Cycle
   d. Human Capital Management
5. Which of the following is the correct order of the six phases of PPDIOO?
   a. Prepare, Plan, Design, Implement, Operate, Optimize
   b. Plan, Prepare, Design, Implement, Operate, Optimize
   c. Prepare, Plan, Design, Implement, Optimize, Operate
   d. Plan, Prepare, Design, Implement, Optimize, Operate

6. The PPDIOO design methodology includes which steps? (Select all that apply.)
   a. Identify customer requirements
   b. Design the network topology
   c. Characterize the network
   d. Optimize the network
7. What are the three primary sources of information in a network audit?
   a. CIO, network manager, network engineer
   b. Network manager, management software, CDP
   c. Network discovery, CDP, SNMP
   d. Existing documentation, management software, new management tools
8. Which design solution states that a design must start from the application layer and finish in the physical layer?
   a. SONA
   b. PPDIOO
   c. IIN
   d. Top-down
9. Budget and personnel limitations are examples of what?
   a. Organization requirements
   b. Organization constraints
   c. Technical goals
   d. Technical constraints
10. Improving network response time and reliability are examples of what?
   a. Organization requirements
   b. Organization constraints
   c. Technical goals
   d. Technical constraints

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the Q&A section. Otherwise, move to the next chapter.

Foundation Topics

With the complexities of networks, it is necessary to use architectures and methodologies in network design to support business goals. Cisco's Intelligent Information Network (IIN) framework and Service-Oriented Network Architecture (SONA) make it possible to better align IT resources with business priorities. The Cisco Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) network life cycle defines a continuous cycle of phases in a network's life. Each phase includes key steps in successful network planning, design, implementation, and operation. The top-down design approach to network design adapts the network infrastructure to the network applications' needs.

Intelligent Information Network and Service-Oriented Network Architecture

Cisco has developed a strategy to address the increasing demands placed on today's networks. Beyond just basic connectivity, the network plays a crucial role because it touches many components of the infrastructure: end users, servers, middleware, and applications. As demands for networks grow, the network can become complex and difficult to scale and manage. Many applications are not visible to network managers on a limited scale, hampering capacity planning and service performance. Furthermore, the network must be able to respond quickly to denial-of-service (DoS) attacks, viruses, and other security-related events that hamper productivity. Drivers for new network architectures are summarized with

- Application growth
- IT evolution from basic connectivity to intelligent systems
- Increased business expectations from networks

The Cisco IIN framework and SONA make it possible to better align IT resources with business priorities.

IIN Framework

The IIN framework is a vision and architecture that adds intelligence to a network. It is implemented in a phased approach for integrating the network with applications, middleware, servers, and services. The idea is to have a single integrated system to extend intelligence across multiple layers to more closely link the network with the rest of the IT infrastructure. Adding intelligence to the network lets the network actively participate in the delivery of services and applications. IIN defines the evolving role of the network in facilitating the integration of the network with services and applications to better align IT resources with business priorities. It lets

organizations quickly adapt to the IT environment and respond to changing business requirements. An IIN's capabilities are as follows:

- **An integrated system**—The network is integrated with applications, middleware, and services.
- **Active participation**—Allows the network to manage, monitor, and optimize application and services delivery.
- **Policy enforcement**—The network enforces policies linking business processes to network rules.

IIN has an evolutionary approach that consists of three phases—Integrated Transport, Integrated Service, and Integrated Application. The goal is for the enterprise to migrate to an intelligent information network.

Integrated Transport involves the convergence of voice, data, and video into a single transport network. The use of Cisco's Unified communications platforms allows the deployment of new applications that enhance communications. Unified messaging is one example of an application where a user can check messages from the IP phone or via email in text or as a voice recording.

Integrated Service merges common elements such as storage and data center server capacity. Virtualization technologies allow the integration of servers, storage, and network elements. With the virtualization of systems with redundant resources, the network can provide services in the event of a local network failure, which enhances business continuity.

The Integrated Application phase allows the network to become application-aware. The network can optimize application performance by integrating application message handling, application optimization, and application security. Cisco calls this technology Application-Oriented Networking (AON).

SONA

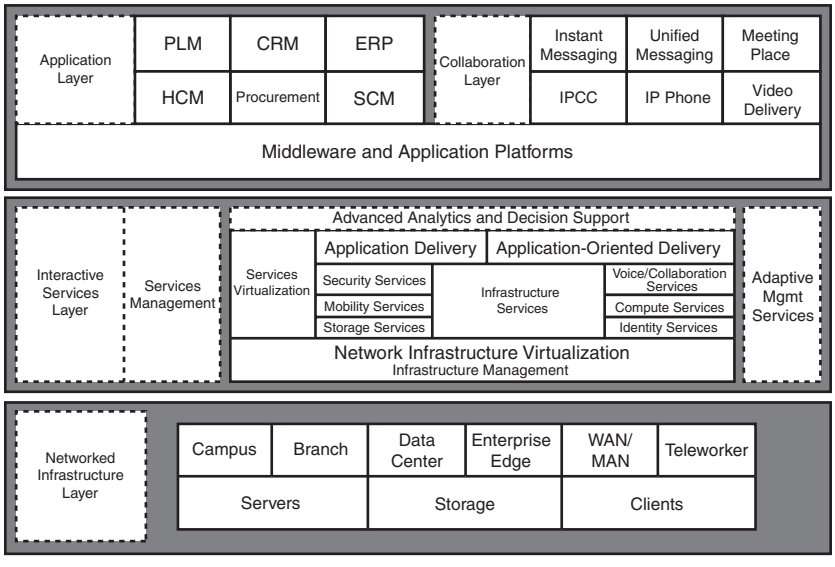
SONA is an architectural framework that guides the evolution of enterprise networks to IIN to support new IT strategies. With SONA, distributed applications and services are centrally managed over a common, unified platform. An integrated system allows access to networked applications and services from all locations with greater speed and service quality. Figure 1-1 shows the SONA framework and the offerings included at each layer. SONA networks are based on a three-layer design that incorporates the applications, services, and network. Offerings are contained within each layer:

- **Network Infrastructure layer** contains the Cisco Enterprise Architecture (campus, LAN, WAN, data center, branch) and facilitates the transport of services across the network. It also includes servers, storage, and clients.

- **Interactive Service layer** optimizes the communication between applications and services using intelligent network functions such as security, identity, voice, virtualization, and quality of service.
- **Application layer** contains the business and collaboration applications used by end users, such as enterprise resource planning, procurement, customer relationship, unified messaging, and conferencing.

Each layer in this framework is covered in the sections that follow.

Figure 1-1 *SONA Framework*



Network Infrastructure Layer

The Network Infrastructure layer contains the Enterprise Network Architecture, which includes the Enterprise Campus, Enterprise Branch, data center, Enterprise Edge, WAN and LAN, and teleworkers. The Cisco Enterprise Architecture is covered in Chapter 2, "Network Structure Models." Servers, storage networks, and end-user clients reside at this layer.

This layer contains switching and routing elements to enhance performance and capabilities, including reliability and security. The network infrastructure is built with redundancy to provide increased reliability. Security configurations are applied to the infrastructure to enforce security policies.

Interactive Service Layer

This layer supports essential applications and the Network Infrastructure layer. Standardized network foundation and virtualization are used to allow security and voice services to scale better. A standardized network architecture can be duplicated and further copied to scale a network. Services provided at this layer fall into two categories: Infrastructure Services and Application Networking Services.

Infrastructure Services

The six infrastructure services are essential in the operation and optimization of network services and applications:

- **Identity services** include authentication, authorization, and accounting (AAA); Network Admission Control (NAC); and Network-Based Application Recognition (NBAR).
- **Mobility services** allow network access regardless of the location. An example is VPN.
- **Storage services** improve storage of critical data. Critical data must be backed up and stored offsite to allow for business continuity and disaster recovery.
- **Compute services** improve computing resources enterprise-wide. High-end servers can be used for virtual machines to scale the amount of servers on the network.
- **Security services** deliver security for all network devices, servers, and users. These services include intrusion detection and prevention devices.
- **Voice and collaboration services** allow user collaboration through all network resources. Cisco's MeetingPlace is an example of a collaboration application.

Application Networking Services

This tier uses middleware applications and Cisco AON to optimize the delivery of applications. Application services deliver application information, optimize application delivery, manipulate application messages, and provide application security and application-level events. Virtualization technologies in this layer are used to maximize resource usage and provide greater flexibility. Servers with multiple virtual machines maximize the use of hardware resources.

Application Layer

The Application layer includes business applications and collaboration applications. Business applications include

- Product Lifecycle Management (PLM)
- Customer Relationship Management (CRM) applications

- Enterprise Resource Planning (ERP) applications
- Human Capital Management (HCM)
- Procurement applications
- Supply Chain Management (SCM)

Collaboration applications include

- Instant messaging (IM)
- Unified messaging (UM)
- IP Contact Center (IPCC)
- Meeting Place
- Video Delivery

Benefits of SONA

The benefits of SONA are as follows:

- **Functionality**—SONA supports the enterprise's operational requirements. The network's services meet the requirements of the business.
- **Scalability**—SONA separates functions into layers, allowing for the growth and expansion of organizational tasks. Modularity and hierarchy allows for network resources to be added to allow growth.
- **Availability**—SONA provides the services from any location in the enterprise and at any time. The network is built with redundancy and resiliency to prevent network downtime.
- **Performance**—SONA provides fast response times and throughput, with quality of service per application. The network is configured to maximize the throughput of critical applications.
- **Manageability**—SONA provides configuration management, performance monitoring, and fault detection. Network management tools are used to detect and correct network faults before applications are affected. Trending tools are used to determine when to add more infrastructure or services to support the increasing demands of applications.
- **Efficiency**—SONA provides the network services with reasonable operational costs and sensible capital investment. Maximum use of existing resources reduces cost and additional equipment is added only when the application demands increase.

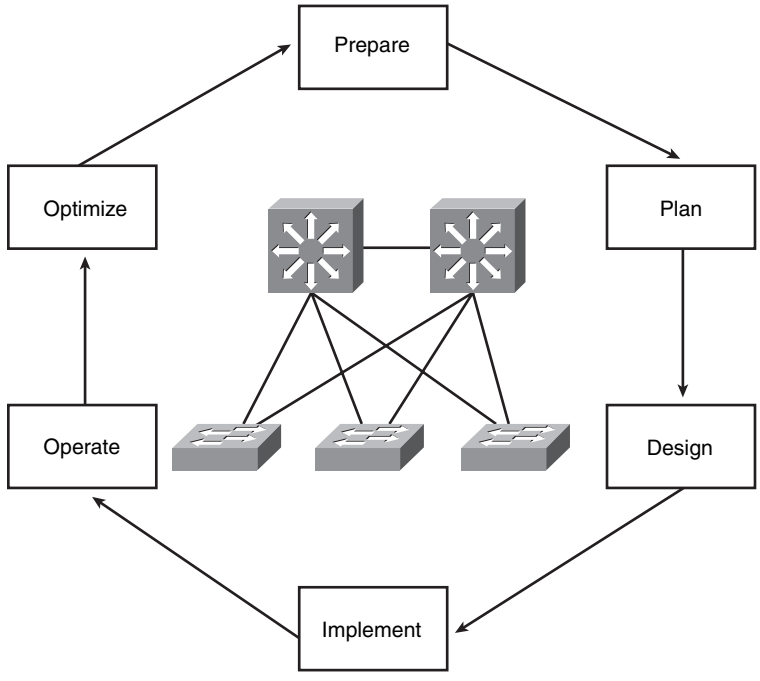
Prepare, Plan, Design, Implement, Operate, and Optimize Phases

Cisco has formalized a network's life cycle into six phases: Prepare, Plan, Design, Implement, Operate, and Optimize. These phases are collectively known as PPDIOO. The PPDIOO life cycle provides four main benefits:

- It lowers the total cost of ownership by validating technology requirements and planning for infrastructure changes and resource requirements.
- It increases network availability by producing a sound network design and validating the network operation.
- It improves business agility by establishing business requirements and technology strategies.
- It speeds access to applications and services by improving availability, reliability, security, scalability, and performance.

Figure 1-2 shows the PPDIOO network life cycle.

Figure 1-2 *Cisco PPDIOO Network Life Cycle*



The following sections discuss these phases in detail.

Prepare Phase

The Prepare phase establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture to support the strategy. Technologies that support the architecture are identified. This phase creates a business case to establish a financial justification for a network strategy.

Plan Phase

The Plan phase identifies the network requirements by characterizing and assessing the network, performing a gap analysis against best-practice architectures, and looking at the operational environment. A project plan is developed to manage the tasks, responsible parties, milestones, and resources to do the design and implementation. This project plan is followed during all phases of the cycle.

Design Phase

The network design is developed based on the technical and business requirements obtained from the previous phases. The network design provides high availability, reliability, security, scalability, and performance. The design includes network diagrams and an equipment list. The project plan is updated with more granular information for implementation. After the Design phase is approved, the Implement phase begins.

Implement Phase

New equipment is installed and configured in the Implement phase. New devices replace or augment the existing infrastructure. The project plan is followed during this phase. Planned network changes should be communicated in change control meetings, with necessary approvals to proceed. Each step in the implementation should includes a description, detailed implementation guidelines, estimated time to implement, rollback steps in case of a failure, and any additional reference information. As changes are implemented they are also tested before moving to the Operate phase.

Operate Phase

The Operate phase maintains the network's day-to-day operational health. Operations include managing and monitoring network components, routing maintenance, managing upgrades, managing performance, and identifying and correcting network faults. This phase is the design's final test. During operation, network management stations should monitor the network's general health and generate traps when certain thresholds are reached.

Optimize Phase

The Optimize phase involves proactive network management by identifying and resolving issues before they affect the network. The Optimize phase may create a modified network design if too many network problems arise, to improve performance issues, or to resolve application issues. The requirement for a modified network design leads to the network life cycle beginning.

Design Methodology Under PPDIOO

The following sections focus on a design methodology for the first three phases of the PPDIOO methodology. This design methodology has three steps:

Step 1 Identify network requirements.

Step 2 Characterize the existing network.

Step 3 Design the network topology and solutions.

In step 1, decision makers identify requirements, and a conceptual architecture is proposed. This step occurs in the PPDIOO Prepare phase.

In step 2, the network is assessed, and a gap analysis is performed to determine the infrastructure necessary to meet the requirements. The network is assessed on function, performance, and quality. This step occurs in the PPDIOO Plan phase.

In step 3, the network topology is designed to meet the requirements and close the network gaps identified in the previous steps. A detailed design document is prepared during this phase. Design solutions include network infrastructure, Voice over IP (VoIP), content networking, and intelligent network services. This set occurs in the PPDIOO Design phase.

Identifying Customer Requirements

To obtain customer requirements, you need to not only talk to network engineers, but also talk to business unit personnel and company managers. Networks are designed to support applications; you want to determine the network services that you need to support. The steps to identify customer requirements are as follows:

Step 1 Identify network applications and services.

Step 2 Define the organizational goals.

Step 3 Define the possible organizational constraints.

Step 4 Define the technical goals.

Step 5 Define the possible technical constraints.

You need to identify current and planned applications and determine the importance of each application. Is e-mail as important as customer support? Is IP telephony being deployed? High-availability and high-bandwidth applications need to be identified for the design to accommodate their network requirements.

For organizational goals, you should identify if the company's goal is to improve customer support, add new customer services, increase competitiveness, or reduce costs. It may be a combination of these goals, with some of them being more important than others.

Organizational constraints include budget, personnel, policy, and schedule. The company might limit you to a certain budget or timeframe. The organization may require the project to be completed in an unreasonable timeframe. It may have limited personnel to support the assessment and design efforts, or it might have policy limitations to use certain protocols.

Technical goals support the organization's objectives and the supported applications. Technical goals include the following:

- Improve the network's response time throughput
- Decrease network failures and downtime
- Simplify network management
- Improve network security
- Improve reliability of mission-critical applications
- Modernize outdated technologies (technology refresh)
- Improve the network's scalability

Network design may be constrained by parameters that limit the solution. Legacy applications may still exist that must be supported going forward, and these applications may require a legacy protocol that may limit a design. Technical constraints include

- Existing wiring does not support new technology
- Bandwidth may not support new applications
- Network must support exiting legacy equipment
- Legacy applications must be supported

Characterizing the Existing Network

Characterizing the network is step 2 of the design methodology. In this section you learn to identify a network's major features, tools to analyze existing network traffic, and tools for auditing and monitoring network traffic.

Steps in Gathering Information

When arriving at a site that has an existing network, you need to obtain all the existing documentation. Sometimes no documented information exists. You should be prepared to use tools to obtain information and/or get access to log into the network devices to obtain information. Here are the steps for gathering information:

Step 1 Identify all existing information and documentation.

Step 2 Perform a network audit.

Step 3 Use traffic analysis to augment information on applications and protocols used.

When gathering exiting documentation, you look for site information such as site names, site addresses, site contacts, site hours of operation, and building and room access. Network infrastructure information includes locations and types of servers and network devices, data center and closet locations, LAN wiring, WAN technologies and circuit speeds, and power used. Logical network information includes IP addressing, routing protocols, network management, and security access lists used. You need to find out if voice or video is being used on the network.

Network Audit Tools

When performing a network audit, you have three primary sources of information:

- Existing documentation
- Existing network management software
- New network management tools

After gathering the existing documentation, you must obtain access to the existing management software. The client may already have CiscoWorks tools from which you can obtain hardware models and components and software versions. You can also obtain the existing router and switch configurations.

The network audit should provide the following information:

- Network device list
- Hardware models

- Software versions
- Configurations
- Auditing tool output information
- Interface speeds
- Link, CPU, and memory utilization
- WAN technology types and carrier information

When performing manual auditing on network devices, you can use the following commands to obtain information:

- **show tech-support**
- **show processes cpu**
- **show version**
- **show processes memory**
- **show running-config**

Example 1-1 shows the output of a **show version** command. This command shows the operating system version, the router type, the amount of flash and RAM memory, the router uptime, and interface types.

Example 1-1 **show version** *Command*

```
R2>show version
Cisco IOS Software, 7200 Software (C7200-K91P-M), Version 12.2(25)S9, RELEASE SO
FTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright  1986-2006 by Cisco Systems, Inc.
Compiled Tue 28-Mar-06 23:12 by alnguyen

ROM: ROMMON Emulation Microcode
BOOTLDR: 7200 Software (C7200-K91P-M), Version 12.2(25)S9, RELEASE SOFTWARE (fc1
)

 R2 uptime is 5 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0
x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
```

Example 1-1 **show version** *Command (Continued)*

```
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 7206VXR (NPE400) processor (revision A) with 147456K/16384K bytes of memor
y.
Processor board ID 4294967295
R7000 CPU at 150Mhz, Implementation 39, Rev 2.1, 256KB L2 Cache
6 slot VXR midplane, Version 2.1

Last reset from power-on

PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 200 bandwidth points.
This configuration is within the PCI bus capacity and is supported.

PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 0 bandwidth points
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port
Adaptor Hardware Configuration Guidelines" on CCO <www.cisco.com>,
for c7200 bandwidth points oversubscription/usage guidelines.


1 FastEthernet interface
8 Serial interfaces
125K bytes of NVRAM.

65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
```

Here are some of the network management tools you can use to obtain network audit information:

- **CiscoWorks** is Cisco's configuration and auditing tool from which you can obtain device inventory and configuration information.
- **WhatsUP Gold/WhatsUP Professional** is IPSwitch's network monitoring tool. It can monitor router bandwidth and do trend analysis. The tool can also monitor servers performing network discovery.
- **Castle Rock SNMPc** monitors network devices, servers, and WAN links. Web reports can be generated.
- **Cacti** is resource monitoring software and a graphing tool.
- **Netcordia NetMRI** is a network analysis product that discovers the network, performs analysis, and makes configuration recommendations.
- **NetQoS NetVoyant** does device performance monitoring and reports on network infrastructure, devices, and services.
- **Other tools** include network protocol analyzers (sniffers) such as Network General Sniffer and WildPackets EtherPeek.

Network Analysis Tools

To obtain application-level information, the IP packet needs to be further inspected. Cisco devices or dedicated hardware or software analyzers capture packets or use SNMP to gather specific information. Network analysis tools include the following:

- **Network-Based Application Recognition (NBAR)** is a Cisco IOS tool used to identify well-known applications and protocols.
- **NetFlow** is IOS software that collects and measures data as it passes through router and switch interfaces.
- **CNS NetFlow Collector Engine** is Cisco hardware that gathers every flow in a network segment.
- **Third-party tools** include Sniffer, Ethernet, and SolarWinds Orion.

Network Checklist

The following is a network checklist that can be used to determine a network's health status:

- No shared Ethernet segments are saturated (no more than 40 percent sustained network utilization). New segments should use switched and not shared technology.

- No WAN links are saturated (no more than 70 percent sustained network utilization).
- The response time is generally less than 100ms (one-tenth of a second). More commonly less than 2ms in a LAN.
- No segments have more than 20 percent broadcasts or multicast traffic. Broadcasts are sent to all hosts in a network and should be limited. Multicast traffic is sent to a group of hosts but should also be controlled and limited to only those hosts registered to receive it.
- No segments have more than one cyclic redundancy check (CRC) error per million bytes of data.
- On the Ethernet segments, less than 0.1 percent of the packets result in collisions.
- A CPU utilization at or over 75 percent for a 5-minute interval likely suggests network problems. Normal CPU utilization should be much lower during normal periods.
- The number of output queue drops has not exceeded 100 in an hour on any Cisco router.
- The number of input queue drops has not exceeded 50 in an hour on any Cisco router.
- The number of buffer misses has not exceeded 25 in an hour on any Cisco router.
- The number of ignored packets has not exceeded 10 in an hour on any interface on a Cisco router.

Designing the Network Topology and Solutions

This section describes the top-down approach for network design, reviews pilot and prototype test networks, and describes the components of the design document. As part of the Design phase of the PPDIOO methodology, a top-down approach is used that begins with the organization's requirements before looking at technologies. Network designs are tested using a pilot or prototype network before moving into the Implement phase.

Top-Down Approach

Top-down design simply means starting your design from the top layer of the OSI model and working your way down. Top-down design adapts the network and physical infrastructure to the network application's needs. With a top-down approach, network devices and technologies are not selected until the applications' requirements are analyzed.

Figure 1-3 shows a top-down structure design process. The design process begins with the applications and moves down to the network. Notice that SONA's Network Infrastructure and Infrastructure Services are incorporated into the design process. Logical subdivisions are then incorporated with specifics.

Figure 1-3 *Top-Down Design Process*

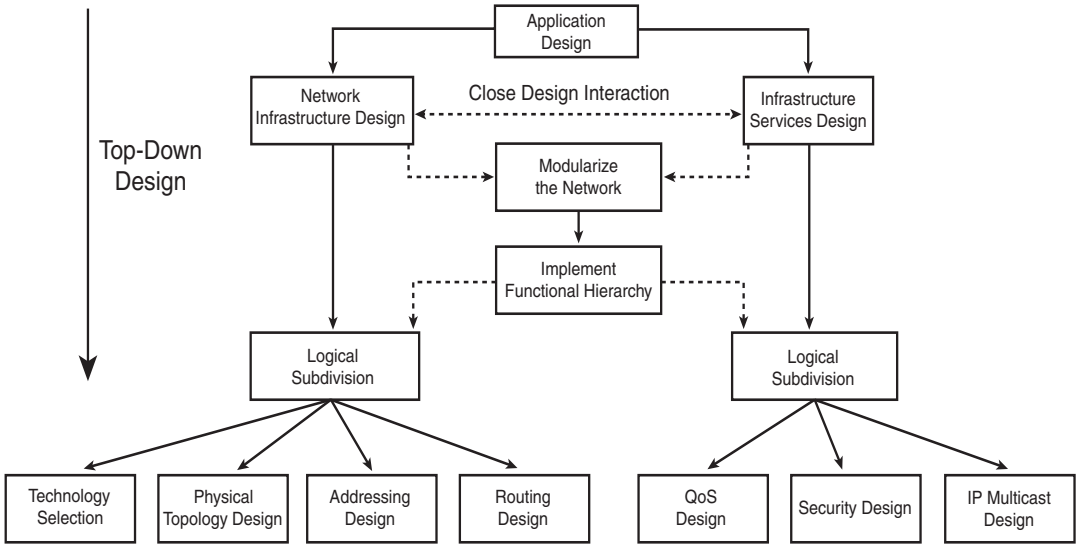


Table 1-2 compares the top-down approach to the bottom-up approach to network design.

Table 1-2 *Top-Down Design Compared to Bottom-Up Design*

Design Approach	Benefits	Disadvantages
Top-down	Incorporates the organization's requirements. Provides the big picture. The design meets current and future requirements.	More time-consuming.
Bottom-up	The design is based on previous experience and allows for a quick solution.	May result in inappropriate design. Organizational requirements are not included.

Pilot and Prototype Tests

As soon as the design is complete and before the full implementation, it is a best practice to test the new solution. This testing can be done in one of two ways: prototype or pilot.

A prototype network is a subset of the full design, tested in an isolated environment. The prototype does not connect to the existing network. The benefit of using a prototype is that it allows testing of the network design before it is deployed before affecting a production network.

A pilot site is an actual "live" location that serves as a test site before the solution is deployed to all locations in an enterprise. A pilot allows real-world problems to be discovered before deploying a network design solution to the rest of the internetwork.

With both a prototype and a pilot, successful testing leads to proving the design and moving forward with implementation. A failure leads to correcting the design and repeating the tests to correct any deficiencies.

Design Document

The design document describes the business requirements; old network architecture; network requirements; and design, plan, and configuration information for the new network. The network architects and analysts use it to document the new network changes, and it serves as documentation for the enterprise. The design document should include the following sections:

- **Introduction** describes the project's purpose and the reasons for the network design.
- **Design Requirements** lists the organization's requirements, constraints, and goals.
- **Existing Network Infrastructure** includes logical (Layer 3) topology diagrams; physical topology diagrams; audit results; routing protocols; a summary of applications; a list of network routers, switches, and other devices; configurations; and a description of issues.
- **Design** contains the specific design information, such as logical and physical topology, IP addressing, routing protocols, and security configurations.
- **Proof of Concept** results from live pilot or prototype testing.
- **Implementation Plan** includes the detailed steps for the network staff to implement the new installation and changes.
- **Appendixes** contains additional information and configurations.

References and Recommended Reading

"The Intelligent Information Network: Introduction," http://www.cisco.com/en/US/netsol/ns648/networking_solutions_intelligent_information_network_home.html

"Service-Oriented Network Architecture: Introduction," http://www.cisco.com/en/US/netsol/ns629/networking_solutions_market_segment_solutions_home.html

"Service-Oriented Network Architecture: What Is It?" http://www.cisco.com/en/US/netsol/ns629/networking_solutions_products_generic_content0900aecd8058763e.html

"What Is IIN?: Introduction," http://www.cisco.com/en/US/netsol/ns650/networking_solutions_market_segment_solution.html

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

Table 1-3 describes the IIN phases.

Table 1-3 *IIN Phases*

IIN Phase	Description
Integrated Transport	Convergence of voice, data, and video into a single transport network.
Integrated Service	Merges common elements such as storage, servers, and network elements. Virtualization of systems.
Integrated Application	Allows the network to become application-aware.

Table 1-4 describes the SONA layers.

Table 1-4 *SONA Layers*

SONA Layer	Description
Network Infrastructure layer	Contains the Cisco Enterprise Architecture, servers, storage, and clients.
Interactive Service layer	Optimization of the communication between applications and services using intelligent network functions such as security, identity, voice, virtualization, and quality of service.
Application layer	Contains business and collaboration applications.

Table 1-5 summarizes the SONA infrastructure services.

Table 1-5 *SONA Infrastructure Services*

Infrastructure Service	Description
Identity Services	Includes AAA, NAC, and NBAR
Mobility Services	Access regardless of location

Table 1-5 *SONA Infrastructure Services (Continued)*

Infrastructure Service	Description
Storage Services	Storage of critical data.
Compute Services	Improves compute resources.
Security Services	Security for all resources.
Voice and Collaboration Services	Allows collaboration of users.

Table 1-6 summarizes the phases of the PPDIOO network life cycle.

Table 1-6 *PPDIOO Network Life Cycle Phases*

PPDIOO Phase	Description
Prepare	Establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture.
Plan	Identifies the network requirements by characterizing and assessing the network, performing a gap analysis.
Design	Provides high availability, reliability, security, scalability, and performance.
Implement	Installation and configuration of new equipment.
Operate	Day-to-day network operations.
Optimize	Proactive network management. Modifications to the design.

Table 1-7 summarizes areas in characterizing the network.

Table 1-7 *Characterizing the Network*

	Description
Steps in gathering information	Step 1: Obtain existing information and documentation Step 2: Network audit Step 3: Traffic analysis
Primary sources of network audit information	Existing documentation Existing network management software New network management tools

Table 1-8 compares the top-down design approach to the bottom-up design approach.

Table 1-8 *Top-Down Design Compared to Bottom-Up Design*

Design Approach	Benefits	Disadvantages
Top-down	Incorporates the organization's requirements. Provides the big picture. The design meets current and future requirements.	More time-consuming.
Bottom-up	The design is based on previous experience and allows for a quick solution.	May result in inappropriate design. Organizational requirements are not included.

Table 1-9 summarizes the sections of the design document.

Table 1-9 *Sections of the Design Document*

Section	Description
Introduction	Purpose and goals of the network design.
Design Requirements	Organization requirements and constraints.
Existing Network Infrastructure	Contains diagrams, hardware and software versions, and existing configurations.
Design	New logical topology, design, and IP addressing.
Proof of Concept	Results from pilot or prototype.
Implementation Plan	Detailed steps for implementation.
Appendixes	Supporting information.

Q&A

As mentioned in the introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. List the three layers of SONA.
2. List the three phases of IIN.
3. List the six infrastructure services.
4. List the drivers for IIN.
5. What name is given to the network's ability to optimize application performance by integrating application message handling and security?
6. List the PPDIOO phases in order.
7. Match each SONA layer with its description.

   i. Network Infrastructure

   ii. Interactive Service

   iii. Application

   a. Virtualization

   b. Contains servers, storage, and switches

   c. Customer relationship and unified messaging
8. SONA guides the evolution of what?
   a. Enterprise networks to integrated network services
   b. Organizations to application service providers
   c. Enterprise networks to intelligent information networks
   d. Enterprise networks to integrated information networks
   e. Cisco Enterprise Architecture to SONA

9. Match each PPDIOO phase with its description.

   i. Implement

   ii. Optimize

   iii. Design

   iv. Prepare

   v. Operate

   vi. Plan

   a. Establish requirements

   b. Gap analysis

   c. Provides high-availability design

   d. Installation and configuration

   c. Day to day

   e. Proactive management

10. Match each infrastructure service with its description.

    i. Identity

    ii. Mobility

    iii. Storage

    iv. Compute

    v. Security

    vi. Voice/collaboration

    a. Access from a remote location

    b. Improved computational resources

    c. Unified messaging

    d. AAA, NAC

    e. Storage of critical data

    f. Secure communications

11. A company location is used to test a new VoIP solution. What is this type of test called?

    a. Prototype

    b. Pilot

    c. Implementation

    d. New

12. An isolated network is created to test a new design. What is this type of test called?
    a. Prototype
    b. Pilot
    c. Implementation
    d. New
13. NBAR, NetFlow, and EtherPeek are examples of what?
    a. Network audit tools
    b. Network analysis tools
    c. SNMP tools
    d. Trending tools
14. Monitoring commands, CiscoWorks, and WhatsUP are examples of what?
    a. Network audit tools
    b. Network analysis tools
    c. SNMP tools
    d. Trending tools
15. Which of the following are technical constraints? (Select all that apply.)
    a. Existing wiring
    b. Existing network circuit bandwidth
    c. Improving the LAN's scalability
    d. Adding redundancy
16. Which of the following are technical goals? (Select all that apply.)
    a. Existing wiring
    b. Existing network circuit bandwidth
    c. Improving the LAN's scalability
    d. Adding redundancy
17. Which of the following are organizational goals? (Select all that apply.)
    a. Improving customer support
    b. Budget has been established
    c. Increasing competitiveness
    d. Completion in three months
    e. Reducing operational costs
    f. Network personnel are busy

18. Which of the following are organizational constraints? (Select all that apply.)

- **a.** Improving customer support
- **b.** Budget has been established
- **c.** Increasing competitiveness
- **d.** Completion in three months
- **e.** Reducing operational costs
- **f.** Network personnel are busy

19. What components are included in the design document? (Select four.)

- **a.** IP addressing scheme
- **b.** Implementation plan
- **c.** List of Layer 2 devices
- **d.** Design requirements
- **e.** Selected routing protocols
- **f.** List of Layer 1 devices

20. Match each design document section with its description.

i. Introduction

ii. Design Requirements

iii. Existing Network Infrastructure

iv. Design

v. Proof of Concept

vi. Implementation Plan

vii. Appendix

a. Detailed steps

b. Current diagram and configuration

c. Organizational requirements

d. Goals

e. Pilot

f. New logical topology

g. Supporting information

21. The network health analysis is based on what information?

    a. The number of users accessing the Internet

    b. The statements made by the CIO

    c. Statistics from the existing network

    d. The IP addressing scheme

22. When performing a network audit, you encounter a shared network hub. Collisions exist at 10 percent. What do you recommend?

    a. Replace the 10-Mbps hub with a Fast Ethernet hub.

    b. Replace the hub with a Fast Ethernet switch.

    c. Increase the hub amplification to reduce the number of collisions.

    d. There is no problem with 10 percent collisions in a shared hub.

23. While performing a network audit, you encounter a Frame Relay WAN segment running at a sustained rate of 75 percent from 9 a.m. to 5 p.m. What do you recommend?

    a. Nothing. The daily 24-hour average rate is still 45 percent.

    b. Change from Frame Relay to MPLS.

    c. Increase the provisioned WAN bandwidth.

    d. Deny VoIP calls from 9 a.m. to 5 a.m.

24. What information is included in the network audit report? (Select all that apply.)

    a. Network device list

    b. IOS versions

    c. Router models

    d. Interface speeds

    e. WAN utilization

25. What are the phases of IIN? (Select all that apply.)

    a. Intelligent Transport

    b. Intelligent Application

    c. Integrated Transport

    d. Intelligent Service

    e. Integrated Service

    f. Integrated Application

This chapter covers the following subjects:

- Hierarchical Network Models
- Cisco Enterprise Architecture Model
- Network Availability

CHAPTER 2

Network Structure Models

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

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The eight-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. Table 2-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

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

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

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. In the hierarchical network model, which layer is responsible for fast transport?
   a. Network
   b. Core
   c. Distribution
   d. Access
2. Which Enterprise Architecture model component interfaces with the service provider (SP)?
   a. Campus infrastructure
   b. Access layer
   c. Enterprise Edge
   d. Edge distribution
3. In the hierarchical network model, at which layer do security filtering, address aggregation, and media translation occur?
   a. Network
   b. Core
   c. Distribution
   d. Access
4. Which of the following is/are method(s) of workstation-to-router redundancy in the access layer?
   a. AppleTalk Address Resolution Protocol (AARP)
   b. Hot Standby Router Protocol (HSRP)
   c. Routing Information Protocol (RIP)
   d. Answers B and C
   e. Answers A, B, and C
5. The network-management module has tie-ins to which component(s)?
   a. Campus infrastructure
   b. Server farm
   c. Enterprise Edge
   d. SP Edge
   e. Answers A and B
   f. Answers A, B, and C
   g. Answers A, B, C, and D

6. Which of the following is an SP Edge module in the Cisco Enterprise Architecture model?
   a. Public Switched Telephone Network (PSTN) service
   b. Edge distribution
   c. Server farm
   d. Core layer
7. In which module would you place Cisco CallManager?
   a. Campus core
   b. E-commerce
   c. Server farm
   d. Edge distribution farm
8. High availability, port security, and rate limiting are functions of which hierarchical layer?
   a. Network
   b. Core
   c. Distribution
   d. Access

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

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

The Cisco Enterprise Architecture is a model that provides a functional modular approach to network design. In addition to a hierarchy, modules are used to organize server farms, network management, campus networks, WANs, and the Internet.

Hierarchical Network Models

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

Benefits of the Hierarchical Model

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

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

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

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

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

Structuring the network into small, easy-to-understand elements improves fault isolation. Network managers can easily understand the transition points in the network, which helps identify failure points.

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

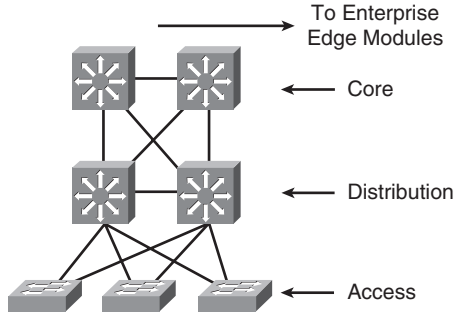
Hierarchical network design facilitates route summarization. EIGRP and all other routing protocols benefit greatly from route summarization. Route summarization reduces routing-protocol overhead on links in the network and reduces routing-protocol processing within the routers.

Hierarchical Network Design

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

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

Figure 2-1 *Hierarchical Network Design Has Three Layers: Core, Distribution, and Access*



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

Core Layer

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

- Fast transport
- High reliability
- Redundancy
- Fault tolerance
- Low latency and good manageability
- Avoidance of slow packet manipulation caused by filters or other processes
- Limited and consistent diameter
- Quality of service (QoS)

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

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

Distribution Layer

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

- Policy (for example, ensuring that traffic sent from a particular network is forwarded out one interface while all other traffic is forwarded out another interface)

- Redundancy and load balancing
- QoS
- Security filtering
- Address or area aggregation or summarization
- Departmental or workgroup access
- Broadcast or multicast domain definition
- Routing between virtual LANs (VLAN)
- Media translations (for example, between Ethernet and Token Ring)
- Redistribution between routing domains (for example, between two different routing protocols)
- Demarcation between static and dynamic routing protocols

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

- Filtering by source or destination address
- Filtering on input or output ports
- Hiding internal network numbers by route filtering
- Static routing
- QoS mechanisms (for example, ensuring that all devices along a path can accommodate the requested parameters)

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

Access Layer

The access layer provides user access to local segments on the network. The access layer is characterized by switched and shared-bandwidth LAN segments in a campus environment. Microsegmentation using LAN switches provides high bandwidth to workgroups by reducing collision domains on Ethernet segments. Some functions of the access layer include the following:

- High availability
- Port security
- Broadcast suppression
- QoS
- Rate limiting

- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACL)
- Spanning tree
- Trust classification
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP
- Auxiliary VLANs

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

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

For small office/home office (SOHO) environments, the entire hierarchy collapses to interfaces on a single device. Remote access to the central corporate network is through traditional WAN technologies such as ISDN, Frame Relay, and leased lines. You can implement features such as dial-on-demand routing (DDR) and static routing to control costs. Remote access can include virtual private network (VPN) technology.

Hierarchical Model Examples

You can implement the hierarchical model by using either routers or switches. Figure 2-2 is an example of a switched hierarchical design in the enterprise campus. In this design, the core provides high-speed transport between the distribution layers. The building-distribution layer provides redundancy and allows policies to be applied to the building-access layer. Layer 3 links between the core and distribution switches are recommended to allow the routing protocol to take care of load balancing and fast route redundancy in the event of a link failure. The server-distribution layer provides redundancy and allows access to the servers to be filtered. For example, Cisco Unified CallManager servers are placed in the server farm, and the server distribution is used to control access to the IP Telephony servers.

Figure 2-3 shows examples of a routed hierarchical design. In this design, the enterprise network connects to the WAN core. WAN distribution routers provide site redundancy to the remote sites. The selected routing protocol (EIGRP or OSPF) provides Layer 3 load balancing from the remote sites to the core.

Figure 2-2 *Switched Hierarchical Design*

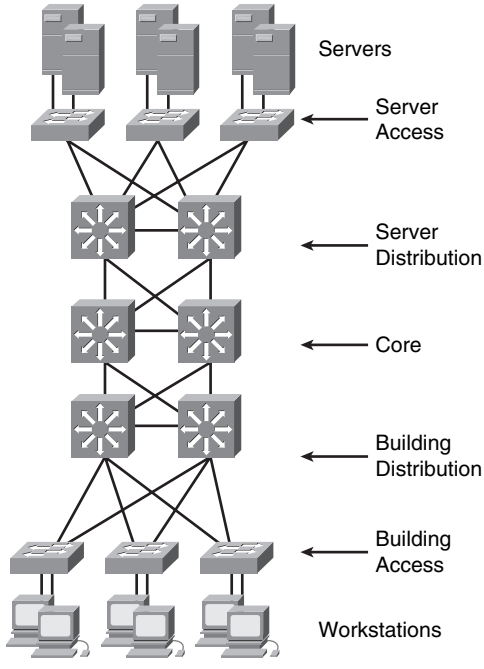
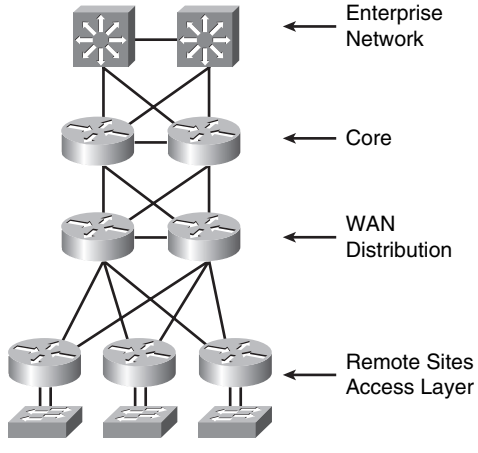


Figure 2-3 *Routed Hierarchical Design*



Cisco Enterprise Architecture Model

The Cisco Enterprise Architecture model facilitates the design of larger, more scalable networks. It represents the focused views of the Cisco Service-Oriented Network Architecture (SONA), which concentrates on each area of the network. SONA is covered in Chapter 1, "Network Design Methodology."

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

- Enterprise Campus module
- Enterprise Edge module
- Enterprise WAN module
- Enterprise Data Center module
- Enterprise Branch module
- Enterprise Teleworker module

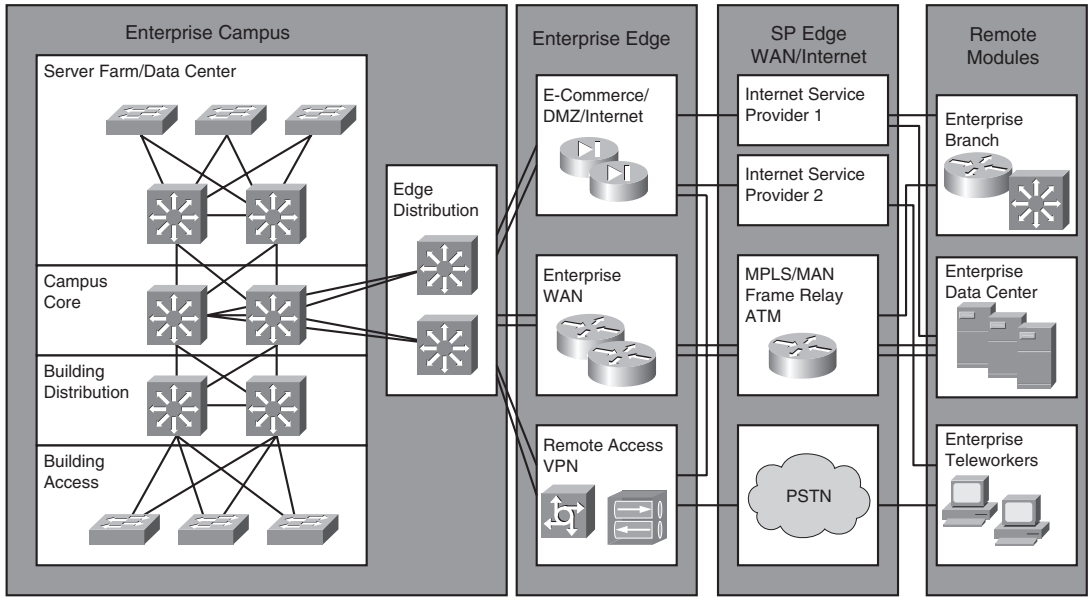
The Cisco Enterprise Architecture maintains the concept of distribution and access components connecting users, WAN services, and server farms through a high-speed campus backbone. The modular approach in design should be a guide to the network architect. In smaller networks, the layers can collapse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

Figure 2-4 shows the Cisco Enterprise Architecture model. The Enterprise Campus module contains a campus infrastructure that consists of core, building distribution, and building access layers, with a server farm/data center and edge distribution. Edge distribution provides distribution functions from the campus infrastructure to the Enterprise Edge. The Enterprise Edge module consists of the Internet, e-commerce, VPN, and WAN functions that connect the enterprise to the service provider's facilities. The SP Edge provides Internet, PSTN, and WAN services.

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

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

Figure 2-4 *Cisco Enterprise Architecture Model*



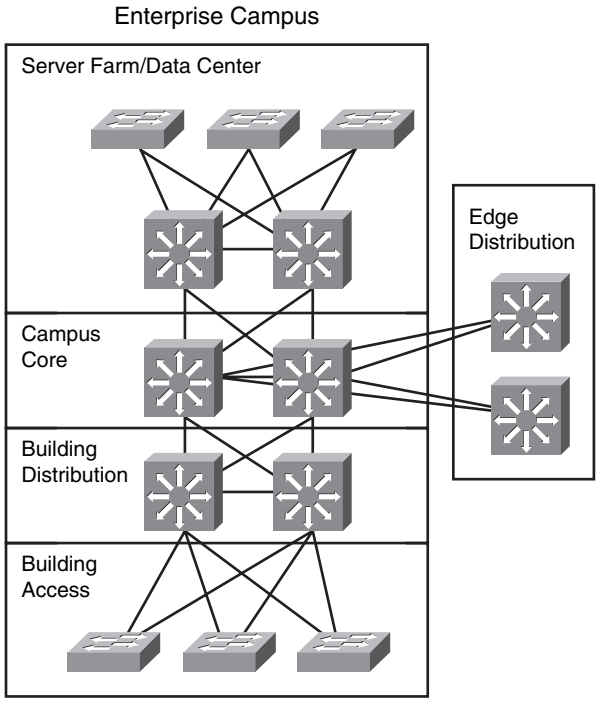
Enterprise Campus Module

The Enterprise Campus consists of the following submodules:

- Campus core
- Building distribution
- Building access
- Edge distribution
- Server farm/data center

Figure 2-5 shows the Enterprise Campus model. The campus infrastructure consists of the campus core, building-distribution, and building-access layers. The campus core provides a high-speed switched backbone between buildings, to the server farm and to the enterprise distribution. This segment consists of redundant and fast convergence connectivity. The building-distribution layer aggregates all the closet access switches and performs access control, QoS, route redundancy, and load balancing. The building-access switches provide VLAN access, PoE for IP phones and wireless access points, broadcast suppression, and spanning tree.

Figure 2-5 *Enterprise Campus Model*



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

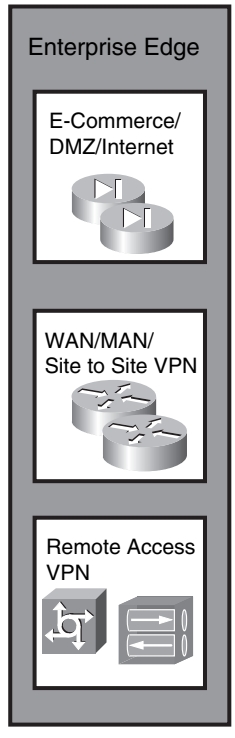
An enterprise campus infrastructure can apply to small, medium, and large locations. In most instances, large campus locations have a three-tier design with a wiring-closet component (building-access layer), a building-distribution layer, and a campus core layer. Small campus locations likely have a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

Enterprise Edge Module

As shown in Figure 2-6, the Enterprise Edge consists of the following submodules:

- E-commerce networks and servers
- Internet connectivity and DMZ
- VPN and remote access
- Enterprise WAN

Figure 2-6 *Enterprise Edge Module*



E-Commerce

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

- Web and application servers
- Database servers

- Firewalls
- Network and server intrusion detection systems (IDS)

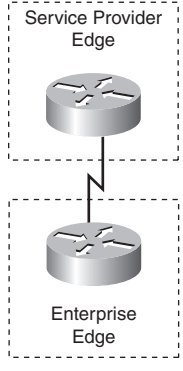
Internet Edge

The Internet submodule provides services such as public servers, e-mail, and DNS. Connectivity to one or several Internet service providers (ISP) is also provided. Components of this submodule include

- Firewalls
- Internet routers
- FTP and HTTP servers
- SMTP mail servers
- DNS servers

Several models connect the enterprise to the Internet. The simplest form is to have a single circuit between the enterprise and the SP, as shown in Figure 2-7. The drawback is that you have no redundancy or failover if the circuit fails.

Figure 2-7 *Simple Internet Connection*

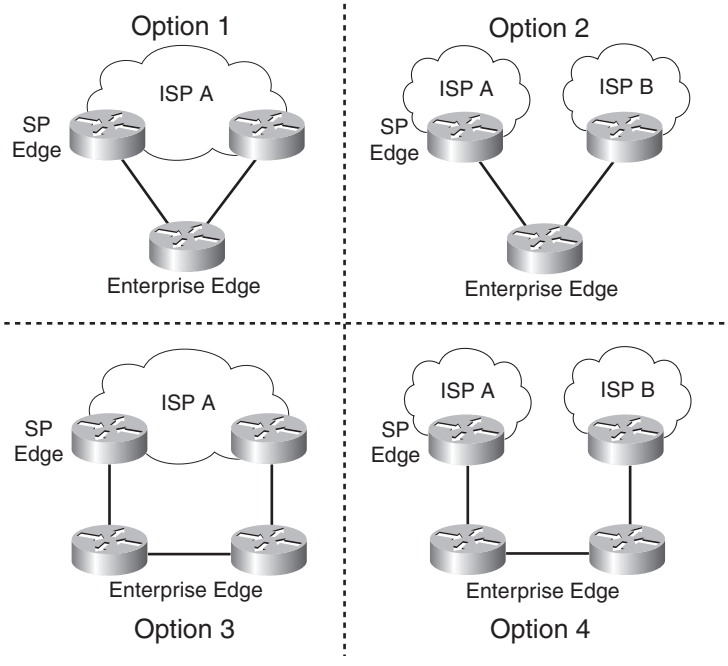


You can use multihoming solutions to provide redundancy or failover for Internet service. Figure 2-8 shows four Internet multihoming options:

- **Option 1**—Single router, dual links to one ISP
- **Option 2**—Single router, dual links to two ISPs

- **Option 3**—Dual routers, dual links to one ISP
- **Option 4**—Dual routers, dual links to two ISPs

Figure 2-8 *Internet Multihoming Options*



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

VPN/Remote Access

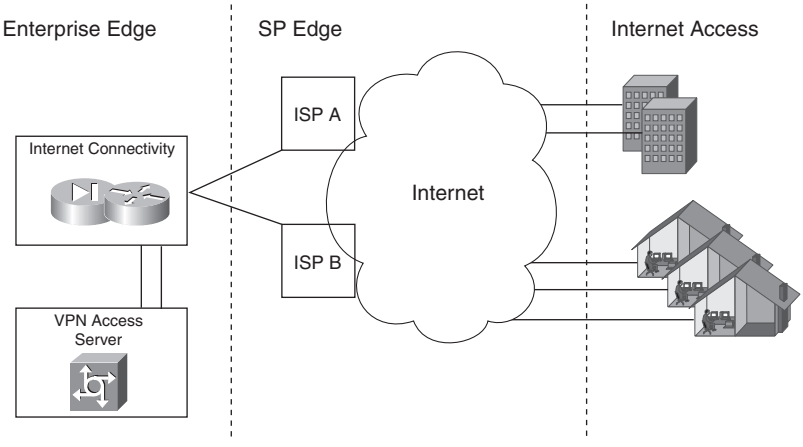
The VPN/remote access submodule provides remote-access termination services, including authentication for remote users and sites. Components of this submodule include

- Firewalls
- VPN concentrators
- Dial-in access concentrators
- Adaptive Security Appliances (ASA)
- Network intrusion detection system (IDS) appliances

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

Figure 2-9 shows a VPN design. Branch offices obtain local Internet access from an ISP. Teleworkers also obtain local Internet access. VPN software creates secured VPN tunnels to the VPN server that is located in the VPN submodule of the Enterprise Edge.

Figure 2-9 *VPN Architecture*



Enterprise WAN

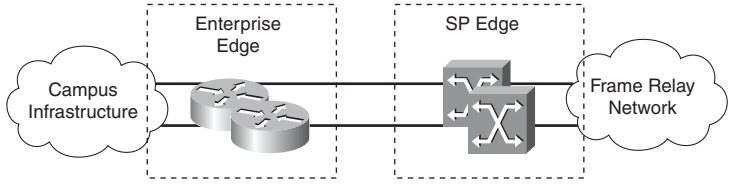
The Enterprise Edge includes access to WANs. WAN technologies include the following:

- MPLS
- Metro Ethernet
- Leased lines
- Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)
- PPP
- Frame Relay
- ATM

- Cable
- Digital subscriber line (DSL)
- Wireless

Chapters 5 and 6 cover these WAN technologies. Routers in the Enterprise WAN provide WAN access, QoS, routing, redundancy, and access control to the WAN. For MPLS networks, the WAN routers prioritize IP packets based on configured DSCP values to use one of several MPLS QoS levels. Figure 2-10 shows the WAN module connecting to the Frame Relay SP Edge. The Enterprise Edge routers in the WAN module connect to the SP's Frame Relay switches.

Figure 2-10 *WAN Module*



Service Provider (SP) Edge Module

The SP Edge module, shown in Figure 2-11, consists of SP edge services such as the following:

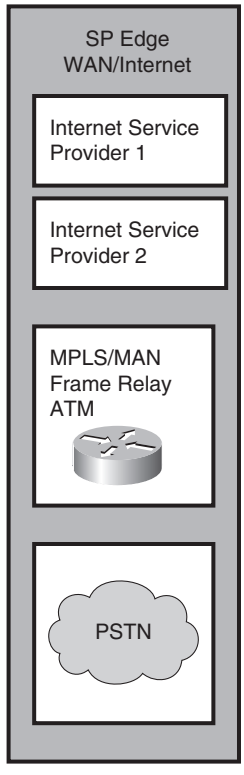
- Internet services
- PSTN services
- WAN services

Enterprises use SPs to acquire network services. ISPs offer enterprises access to the Internet. ISPs can route the enterprise's networks to their network and to upstream and peer Internet providers. Some ISPs can provide Internet services with DSL access. Connectivity with multiple ISPs was described in the "Internet Edge" section.

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

WAN SPs offer MPLS, Frame Relay, ATM, and other WAN services for Enterprise site-to-site connectivity with permanent connections. These and other WAN technologies are described in Chapter 5, "WAN Technologies."

Figure 2-11 *WAN/Internet SP Edge Module*



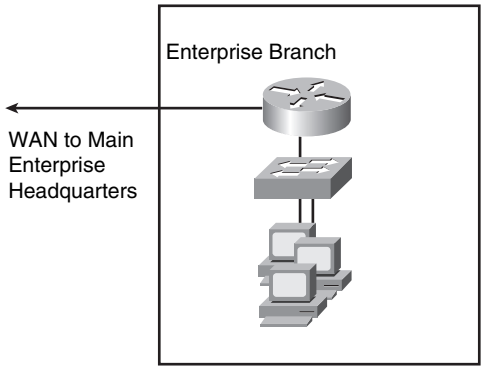
Remote Modules

The remote modules of the Cisco Enterprise Architecture model are the Enterprise Branch, Enterprise Data Center, and Enterprise Teleworker modules.

Enterprise Branch Module

The Enterprise Branch normally consists of remote offices or sales offices. These branch offices rely on the WAN to use the services and applications provided in the main campus. Infrastructure at the remote site usually consists of a WAN router and a small LAN switch, as shown in Figure 2-12. Instead of MPLS or Frame Relay, it is common to use site-to-site VPN technologies to connect to the main campus.

Figure 2-12 *Enterprise Branch Module*



Enterprise Data Center Module

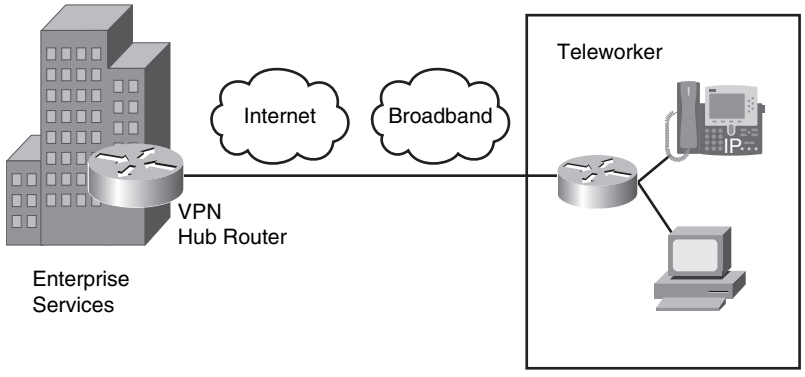
The Enterprise Data Center uses the network to enhance the server, storage, and application servers. The offsite data center provides disaster recovery and business continuance services for the enterprise. Highly available WAN services are used to connect the enterprise campus to the remote Enterprise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

- **Network devices**—Routers and high-speed switches
- **High-speed LAN technologies**—Gigabit and 10 Gigabit Ethernet, InfiniBand, optical switching
- **Interactive services**—Computer infrastructure services, storage services, security, application optimization
- **DC management**—Fault and trend management and Cisco VFrame for server and service management

Enterprise Teleworker Module

The Enterprise Teleworker module consists of a small office or a mobile user who needs to access services of the enterprise campus. As shown in Figure 2-13, mobile users connect from their homes, hotels, or other locations using dialup or Internet access lines. VPN clients are used to allow mobile users to securely access enterprise applications. The Cisco Teleworker solution provides a solution for teleworkers that is centrally managed using small integrated service routers (ISR) in the VPN solution. IP phone capabilities are also provided in the Cisco Teleworker solution, providing corporate voice services for mobile users.

Figure 2-13 *Enterprise Teleworker Solution*



Network Availability

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

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

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

The following sections discuss each type of redundancy.

Workstation-to-Router Redundancy

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

- ARP
- Explicit configuration
- ICMP Router Discovery Protocol (RDP)
- RIP

- HSRP
- Global Load Balancing Protocol (GLBP)

The following sections cover each of these methods.

ARP

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

Explicit Configuration

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

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

RDP

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

RIP

An IP workstation can run RIP to learn about routers. You should use RIP in passive mode rather than active mode. (Active mode means that the station sends RIP frames every 30 seconds.) Usually in these implementations, the workstation is a UNIX system running the **routed** or **gated** UNIX process.

HSRP

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

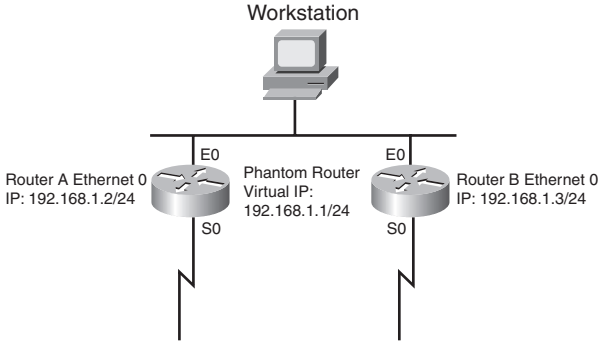
HSRP routers on a LAN communicate among themselves to designate two routers as *active* and *standby*. The active router sends periodic hello messages. The other HSRP routers listen for the hello messages. If the active router fails and the other HSRP routers stop receiving hello messages,

the standby router takes over and becomes the active router. Because the new active router assumes both the phantom's IP and MAC addresses, end nodes see no change. They continue to send packets to the phantom router's MAC address, and the new active router delivers those packets.

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

Figure 2-14 shows a sample implementation of HSRP.

Figure 2-14 *HSRP: The Phantom Router Represents the Real Routers*



In Figure 2-14, the following sequence occurs:

1. The workstation is configured to use the phantom router (192.168.1.1) as its default router.
2. Upon booting, the routers elect Router A as the HSRP active router. The active router does the work for the HSRP phantom. Router B is the HSRP standby router.
3. When the workstation sends an ARP frame to find its default router, Router A responds with the phantom router's MAC address.
4. If Router A goes offline, Router B takes over as the active router, continuing the delivery of the workstation's packets. The change is transparent to the workstation.

GLBP

GLBP protects data traffic from a failed router or circuit, such as Hot Standby Router Protocol (HSRP), while allowing packet load sharing between a group of redundant routers. The difference in GLBP from HSRP is that it provides for load balancing between the redundant routers. It load balances by using a single virtual IP address and multiple virtual MAC addresses. Each host is

configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every three seconds to the multicast address 224.0.0.102, User Datagram Protocol (UDP) port 3222.

Server Redundancy

Some environments need fully redundant (mirrored) file and application servers. For example, in a brokerage firm where traders must access data to buy and sell stocks, two or more redundant servers can replicate the data. Also, you can deploy CallManager servers in clusters for redundancy. The servers should be on different networks and use redundant power supplies.

Route Redundancy

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

Load Balancing

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

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

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

Increasing Availability

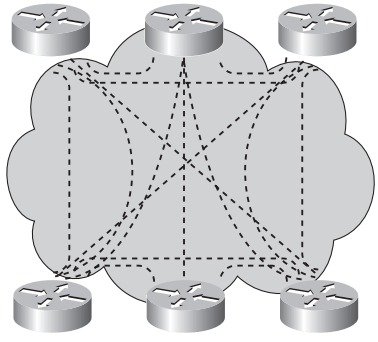
In addition to facilitating load balancing, redundant routes increase network availability.

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

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

You can design redundant network links to provide a full mesh or a well-connected partial mesh. In a full-mesh network, every router has a link to every other router, as shown in Figure 2-15. A full-mesh network provides complete redundancy and also provides good performance because there is just a single-hop delay between any two sites. The number of links in a full mesh is $n(n–1)/2$, where n is the number of routers. Each router is connected to every other router. A well-connected partial-mesh network provides every router with links to at least two other routing devices in the network.

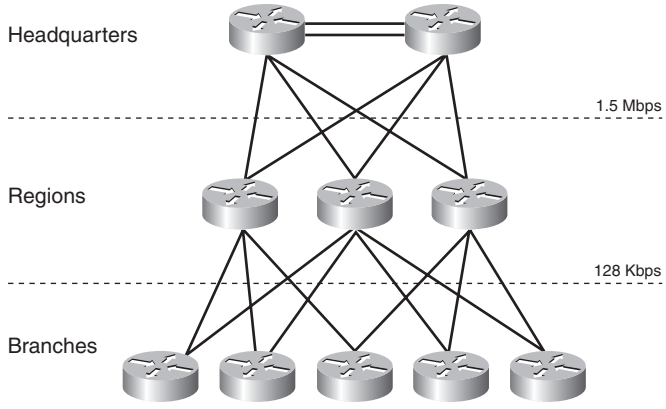
Figure 2-15 *Full-Mesh Network: Every Router Has a Link to Every Other Router in the Network*



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

A suggested guideline is to keep broadcast traffic at less than 20 percent of the bandwidth of each link; this amount limits the number of peer routers that can exchange routing tables or service advertisements. When planning redundancy, follow guidelines for simple, hierarchical design. Figure 2-16 illustrates a classic hierarchical and redundant enterprise design that uses a partial-mesh rather than a full-mesh topology. For LAN designs, links between the access and distribution layer can be Fast Ethernet, with links to the core at Gigabit Ethernet speeds.

Figure 2-16 *Partial-Mesh Design with Redundancy*



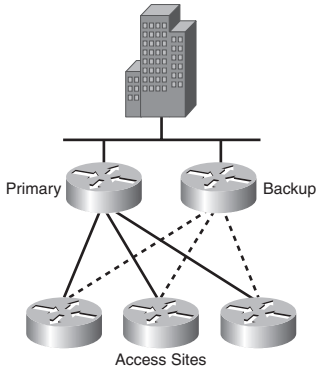
Media Redundancy

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

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

Because WAN links are often critical pieces of the internetwork, WAN environments often deploy redundant media. As shown in Figure 2-17, you can provision backup links so that they become active when a primary link goes down or becomes congested.

Figure 2-17 *Backup Links Can Provide Redundancy*



Often, backup links use a different technology. For example, a leased line can be in parallel with a backup dialup line or ISDN circuit. By using *floating static routes*, you can specify that the backup route have a higher administrative distance (used by Cisco routers to select routing information) so that it is not normally used unless the primary route goes down. This design is less available than the partial mesh presented previously. Typically, on-demand backup links reduce WAN charges.

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

You can combine backup links with load balancing and *channel aggregation*. Channel aggregation means that a router can bring up multiple channels (for example, ISDN B channels) as bandwidth requirements increase.

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

References and Recommended Reading

Cisco Enterprise Teleworker Solution, http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/networking_solutions_packages_list.html

Cisco Systems, Inc., “Enterprise Architectures,” http://www.cisco.com/en/US/netsol/ns517/networking_solutions_market_segment_solutions_home.html

Cisco Systems, Inc., “Service-Oriented Network Architecture,” http://www.cisco.com/en/US/netsol/ns629/networking_solutions_market_segment_solutions_home.html

RFC 3758, Virtual Router Redundancy Protocol (VRRP). Ed Hinden, April 2004

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you understand the three layers of a hierarchical network design:

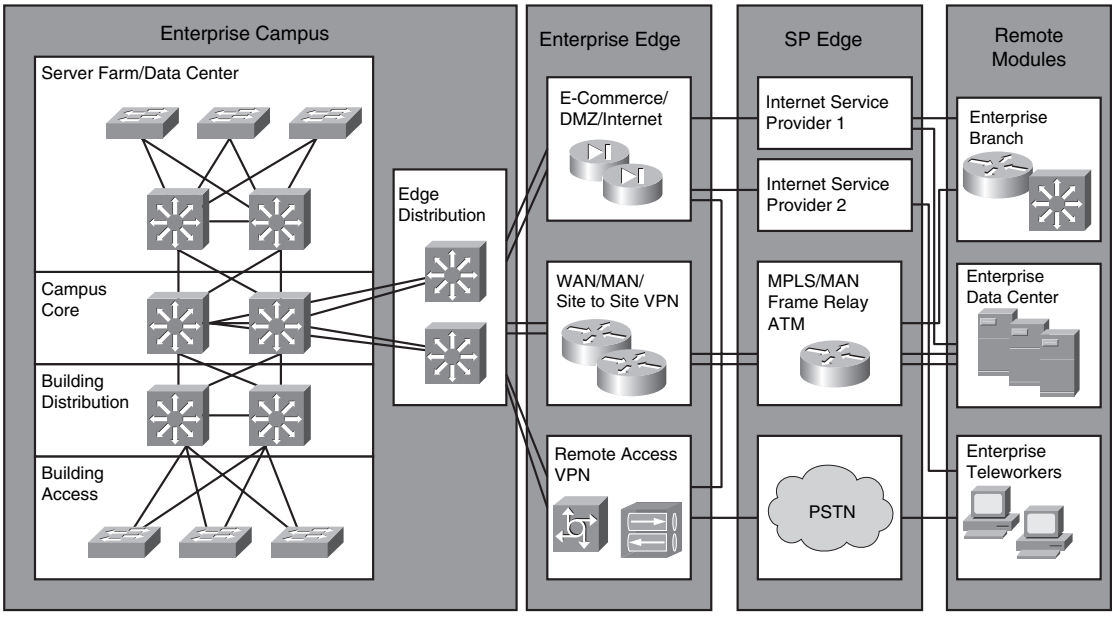
- The core layer and campus-backbone component provide fast transport within sites.
- The distribution layer and building-distribution component provide policy-based connectivity.
- The access layer and building-access component provide workgroup and user access to the network.

The Cisco Enterprise Architecture divides the network into six major modules:

- **Enterprise Campus (campus infrastructure, edge distribution, server farm, network management)**—The Enterprise Campus module includes the building-access and building-distribution components and the shared campus backbone component or campus core. Edge distribution provides connectivity to the Enterprise Edge. High availability is implemented in the server farm, and network management monitors the Enterprise Campus and Enterprise Edge.
- **Enterprise Edge (e-commerce, Internet, VPN/remote access, WAN)**—The e-commerce submodule provides high availability for business servers and connects to the Internet submodule.
- **Enterprise WAN**—This module provides Frame Relay or other WAN technology. The VPN submodule provides secure site-to-site remote access over the Internet.
- **Enterprise Branch**—The Enterprise Branch normally consists of remote offices, small offices, or sales offices. These branch offices rely on the WAN to use the services and applications provided in the main campus.
- **Enterprise Data Center**—The Enterprise Data Center consists of using the network to enhance the server, storage, and application servers. The offsite data center provides disaster recovery and business continuance services for the enterprise.
- **Enterprise Teleworker**—The Enterprise Teleworker supports a small office, mobile users, or home users providing access to corporate systems via VPN tunnels.

Figure 2-18 shows an Enterprise composite network model, as described here.

Figure 2-18 *Cisco Enterprise Architecture*



Network availability comes from design capacity, technologies, and device features that implement the following:

- Workstation-to-router redundancy in the building-access module
- Server redundancy in the server-farm module
- Route redundancy within and between network components
- Media redundancy in the access and distribution modules

Q&A

As mentioned in the introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: The core layer of the hierarchical model does security filtering and media translation.
2. True or false: The access layer provides high availability and port security.
3. You add CallManager to the network as part of a Voice over IP (VoIP) solution. In which submodule of the Enterprise Architecture should you place CallManager?
4. True or false: HSRP provides router redundancy.
5. Which Enterprise Edge submodule connects to an ISP?
6. List the six modules of the Cisco Enterprise Architecture for network design.
7. True or false: In the Cisco Enterprise Architecture, the network management submodule does not manage the SP Edge.
8. True or false: You can implement a full-mesh network to increase redundancy and reduce a WAN's costs.
9. How many links are required for a full mesh of six sites?
10. List and describe four options for multihoming to the SP between the Enterprise Edge and the SP Edge. Which option provides the most redundancy?
11. To what Enterprise Edge submodule does the SP Edge Internet submodule connect?
12. What are four benefits of hierarchical network design?
13. In an IP telephony network, in which submodule or layer are the IP phones and CallManagers located?

14. Match the redundant model with its description:

    i. Workstation-router redundancy

    ii. Server redundancy

    iii. Route redundancy

    iv. Media redundancy

    a. Cheap when implemented in the LAN and critical for the WAN

    b. Provides load balancing

    c. Host has multiple gateways

    d. Data is replicated

15. True or false: Small to medium campus networks must always implement three layers of hierarchical design.

16. How many full-mesh links do you need for a network with ten routers?

17. Which layer provides routing between VLANs and security filtering?

    a. Access layer
    b. Distribution layer
    c. Enterprise edge
    d. WAN submodule

18. List the four submodules of the Enterprise Edge.

19. List the three submodules of the SP Edge.

20. List the components of the Internet Edge.

21. Which submodule contains firewalls, VPN concentrators, and ASAs?

    a. WAN
    b. VPN/Remote Access
    c. Internet
    d. Server Farm

22. Which of the following describe the access layer? (Select two.)

    a. High-speed data transport
    b. Applies network policies
    c. Performs network aggregation
    d. Concentrates user access
    e. Provides PoE
    f. Avoids data manipulation

23. Which of the following describe the distribution layer? (Select two.)

    a. High-speed data transport
    b. Applies network policies
    c. Performs network aggregation
    d. Concentrates user access
    e. Provides PoE
    f. Avoids data manipulation

24. Which of the following describe the core layer? (Select two.)

    a. High-speed data transport
    b. Applies network policies
    c. Performs network aggregation
    d. Concentrates user access
    e. Provides PoE
    f. Avoids data manipulation

25. Assuming that there is no Enterprise distribution, which campus submodule connects to the Enterprise Edge module?

    a. SP Edge
    b. WAN submodule
    c. Building Distribution
    d. Campus Core
    e. Enterprise Branch
    f. Enterprise Data Center

26. Which remote module connects to the enterprise via the Internet or WAN submodules and contains a small LAN switch for users?

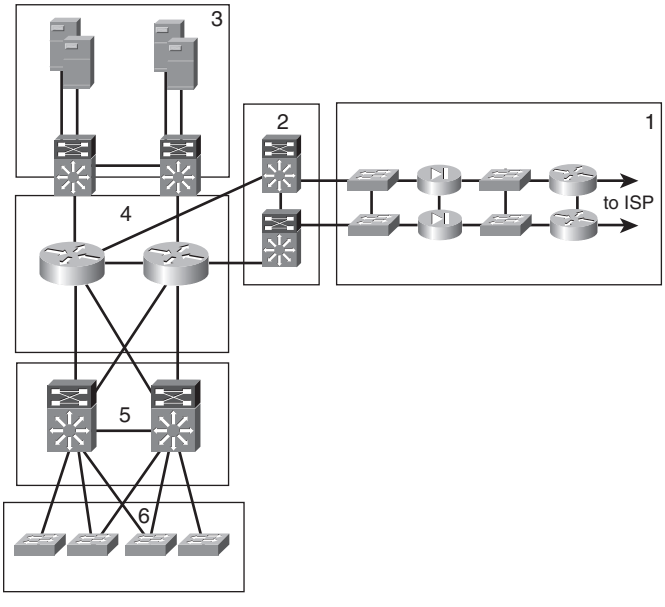
- **a.** SP Edge
- **b.** WAN submodule
- **c.** Building Distribution
- **d.** Campus Core
- **e.** Enterprise Branch
- **f.** Enterprise Data Center

27. Which three types of servers are placed in the e-commerce submodule?

- **a.** Web
- **b.** Application
- **c.** Database
- **d.** Intranet
- **e.** Internet
- **f.** Public share

Use Figure 2-19 to answer the following questions.

Figure 2-19 *Scenario*



28. Which is the campus core layer?
29. Which is the Enterprise Edge?
30. Which is the campus access layer?
31. Which is the Enterprise Edge distribution?
32. Which is the campus distribution layer?
33. Which is the campus data center?

This part covers the following CCDA exam topics (to view the CCDA exam overview, visit http://www.cisco.com/web/learning/le3/current_exams/640-863.html):

- Describe Campus Design Considerations
- Design the Enterprise Campus Network
- Design the Enterprise Data Center
- Describe the Enterprise Edge, Branch, and Teleworker Design Characteristics
- Describe the Functional Components of The Central Site Enterprise Edge
- Describe WAN Connectivity Between Two Campuses
- Design the Branch Office WAN Solutions
- Describe Access Network solutions for a Teleworker
- Design the WAN to Support Selected Redundancy Methodology
- Identify Design Considerations for a Remote Data Center
- Describe Cisco Unified Wireless Network Architectures and Features
- Design Wireless Network Using Controllers
- Design Wireless Network Using Roaming

Part II: LAN and WAN Design

This chapter covers the following subjects:

- LAN Media
- LAN Hardware
- LAN Design Types and Models

CHAPTER 3

Enterprise LAN Design

This chapter covers the design of campus local-area networks (LAN). It reviews LAN media, components, and design models. The section "LAN Media" reviews the design characteristics of different Ethernet media technologies.

This chapter covers how you apply Layer 2 switches, Layer 3 switches, and routers in the design of LANs. It reviews several design models for large building, campus, and remote LANs.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 3-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 3-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
LAN Media	2
LAN Hardware	1, 3, 8
LAN Design Types and Models	4, 5, 6, 7

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. What device filters broadcasts?
   a. Layer 2 switch
   b. Hub
   c. Layer 3 switch
   d. Router
   e. Answers A and C
   f. Answers C and D
   g. Answers A, C, and D
2. What is the maximum segment distance for Fast Ethernet over unshielded twisted-pair (UTP)?
   a. 100 feet
   b. 500 feet
   c. 100 meters
   d. 285 feet
3. What device limits the collision domain?
   a. Layer 2 switch
   b. Hub
   c. Layer 3 switch
   d. Router
   e. Answers A and C
   f. Answers C and D
   g. Answers A, C, and D
4. The summarization of routes is a best practice at which layer?
   a. Access layer
   b. Distribution layer
   c. Core layer
   d. WAN layer
5. What type of LAN switches are preferred in the campus backbone of an enterprise network?
   a. Layer 2 switches
   b. Layer 3 switches
   c. Layer 3 hubs
   d. Hubs

6. What Cisco-proprietary protocol can you use in LAN switches to control multicast traffic at the data link layer within a LAN switch?

   a. IGMP

   b. Cisco Group Management Protocol (CGMP)

   c. MAC filters

   d. Cisco Discovery Protocol (CDP)

7. Marking is also known as what?

   a. Classifying

   b. Pinging

   c. Coloring

   d. Tracing

8. Why is switching preferred on shared segments?

   a. Shared segments provide a collision domain for each host.

   b. Switched segments provide a collision domain for each host.

   c. Shared segments provide a broadcast domain for each host.

   d. Switched segments provide a broadcast domain for each host.

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

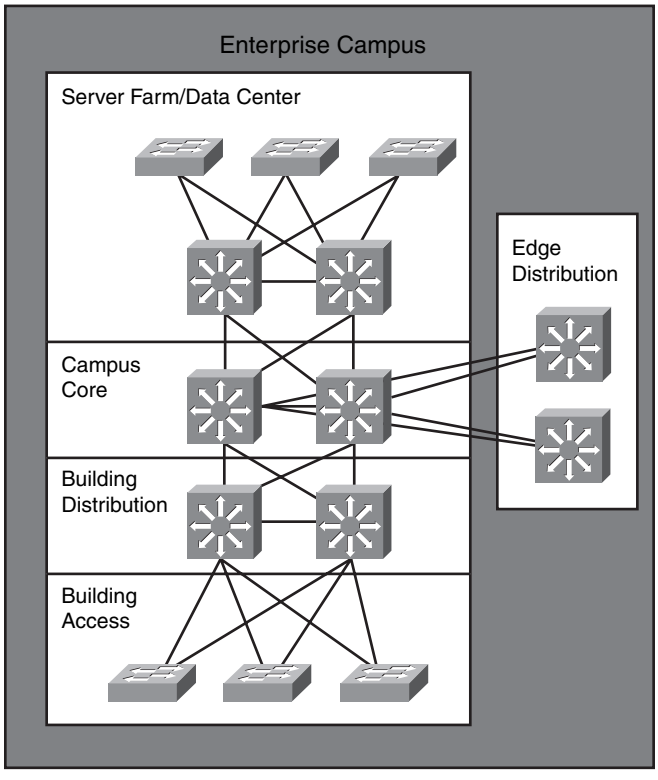
- **6 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers the design of LANs. It reviews LAN media, components, and design models. Figure 3-1 shows the Enterprise Campus section of the Enterprise Composite Network model. Enterprise LANs have a campus backbone and one or more instances of building-distribution and building-access layers, with server farms and an Enterprise Edge to the WAN or Internet.

Figure 3-1 *Enterprise Campus*



LAN Media

This section identifies some of the constraints you should consider when provisioning various LAN media types. It covers the physical specifications of Ethernet, Fast Ethernet, and Gigabit Ethernet. It also covers the specifications for Token Ring, because you may find this technology on existing networks.

You must also understand the design constraints of wireless LANs in the campus network. Specifications for wireless LANs are covered in Chapter 4, "Wireless LAN Design."

Ethernet Design Rules

Ethernet is the underlying basis for the technologies most widely used in LANs. In the 1980s and early 1990s, most networks used 10-Mbps Ethernet, defined initially by Digital, Intel, and Xerox (DIX Ethernet Version II) and later by the IEEE 802.3 working group. The IEEE 802.3-2002 standard contains physical specifications for Ethernet technologies through 10 Gbps.

Table 3-2 describes the physical Ethernet specifications up to 100 Mbps. It provides scalability information that you can use when provisioning IEEE 802.3 networks. Of these specifications, 10BASE5 and 10BASE2 are no longer used but are included for completeness.

Table 3-2 *Scalability Constraints for IEEE 802.3*

Specification	10BASE5	10BASE2	10BASE-T	100BASE-T
Physical Topology	Bus	Bus	Star	Star
Maximum Segment Length (in Meters)	500	185	100 from hub to station	100 from hub to station
Maximum Number of Attachments Per Segment	100	30	2 (hub and station or hub-hub)	2 (hub and station or hub-hub)
Maximum Collision Domain	2500 meters (m) of five segments and four repeaters; only three segments can be populated	2500 m of five segments and four repeaters; only three segments can be populated	2500 m of five segments and four repeaters; only three segments can be populated	See the details in the section "100-Mbps Fast Ethernet Design Rules" later in this chapter

The most significant design rule for Ethernet is that the round-trip propagation delay in one collision domain must not exceed 512-bit times. This is a requirement for collision detection to work correctly. This rule means that the maximum round-trip delay for a 10-Mbps Ethernet network is 51.2 microseconds. The maximum round-trip delay for a 100-Mbps Ethernet network is only 5.12 microseconds because the bit time on a 100-Mbps Ethernet network is 0.01 microseconds, as opposed to 0.1 microseconds on a 10-Mbps Ethernet network.

10-Mbps Fiber Ethernet Design Rules

Table 3-3 provides some guidelines for fiber-based 10-Mbps Ethernet media for network designs. These specifications are not part of the CCDA test but are included for reference. The 10BASE-FP standard uses a passive-star topology. The 10BASE-FB standard is for a backbone or repeater-based system. The 10BASE-FL standard provides specifications on fiber links.

Table 3-3 *Scalability Constraints for 10-Mbps Fiber Ethernet*

Specification	10BASE-FP	10BASE-FB	10BASE-FL
Topology	Passive star	Backbone or repeater-fiber system	Link
Maximum Segment Length	1000 m	2000 m	2000 m
Allows Cascaded Repeaters?	No	Yes	No
Maximum Collision Domain	2500 m	2500 m	2500 m

100-Mbps Fast Ethernet Design Rules

IEEE introduced the IEEE 802.3u-1995 standard to provide Ethernet speeds of 100 Mbps over UTP and fiber cabling. The 100BASE-T standard is similar to 10-Mbps Ethernet in that it uses carrier sense multiple access collision detect (CSMA/CD); runs on Category (CAT) 3, 4, and 5 UTP cable; and preserves the frame formats. Connectivity still uses hubs, repeaters, and bridges.

100-Mbps Ethernet, or Fast Ethernet, topologies present some distinct constraints on the network design because of their speed. The combined latency due to cable lengths and repeaters must conform to the specifications for the network to work properly. This section discusses these issues and provides sample calculations.

The overriding design rule for 100-Mbps Ethernet networks is that the round-trip collision delay must not exceed 512-bit times. However, the bit time on a 100-Mbps Ethernet network is 0.01 microseconds, as opposed to 0.1 microseconds on a 10-Mbps Ethernet network. Therefore, the maximum round-trip delay for a 100-Mbps Ethernet network is 5.12 microseconds, as opposed to the more lenient 51.2 microseconds in a 10-Mbps Ethernet network.

The following are specifications for Fast Ethernet, each of which is described in the following sections:

- 100BASE-TX
- 100BASE-T4
- 100BASE-FX

100BASE-TX Fast Ethernet

The 100BASE-TX specification uses CAT 5 UTP wiring. Like 10BASE-T, Fast Ethernet uses only two pairs of the four-pair UTP wiring. If CAT 5 cabling is already in place, upgrading to Fast Ethernet requires only a hub or switch and network interface card (NIC) upgrades. Because of the low cost, most of today's installations use switches. The specifications are as follows:

- Transmission over CAT 5 UTP wire.
- RJ-45 connector (the same as in 10BASE-T).
- Punchdown blocks in the wiring closet must be CAT 5 certified.
- 4B5B coding.

100BASE-T4 Fast Ethernet

The 100BASE-T4 specification was developed to support UTP wiring at the CAT 3 level. This specification takes advantage of higher-speed Ethernet without recabling to CAT 5 UTP. This implementation is not widely deployed. The specifications are as follows:

- Transmission over CAT 3, 4, or 5 UTP wiring.
- Three pairs are used for transmission, and the fourth pair is used for collision detection.
- No separate transmit and receive pairs are present, so full-duplex operation is not possible.
- 8B6T coding.

100BASE-FX Fast Ethernet

The 100BASE-FX specification for fiber is as follows:

- It operates over two strands of multimode or single-mode fiber cabling.
- It can transmit over greater distances than copper media.
- It uses media interface connector (MIC), Stab and Twist (ST), or Stab and Click (SC) fiber connectors defined for FDDI and 10BASE-FX networks.
- 4B5B coding.

100BASE-T Repeaters

To make 100-Mbps Ethernet work, distance limitations are much more severe than those required for 10-Mbps Ethernet. Repeater networks have no five-hub rule; Fast Ethernet is limited to two repeaters. The general rule is that 100-Mbps Ethernet has a maximum diameter of 205 meters (m)

with UTP cabling, whereas 10-Mbps Ethernet has a maximum diameter of 500 m with 10BASE-T and 2500 m with 10BASE5. Most networks today use switches instead of repeaters, which limits the length of 10BASE-T and 100BASE-TX to 100 m between the switch and host.

The distance limitation imposed depends on the type of repeater.

The IEEE 100BASE-T specification defines two types of repeaters: Class I and Class II. Class I repeaters have a latency (delay) of 0.7 microseconds or less. Only one repeater hop is allowed. Class II repeaters have a latency of 0.46 microseconds or less. One or two repeater hops are allowed.

Table 3-4 shows the maximum size of collision domains, depending on the type of repeater.

Table 3-4 *Maximum Size of Collision Domains for 100BASE-T*

Repeater Type	Copper	Mixed Copper and Multimode Fiber	Multimode Fiber
DTE-DTE (or Switch-Switch)	100 m	Not applicable	412 m (2000 if full duplex)
One Class I Repeater	200 m	260 m	272 m
One Class II Repeater	200 m	308 m	320 m
Two Class II Repeaters	205 m	216 m	228 m

Again, for switched networks, the maximum distance between the switch and the host is 100 m.

Gigabit Ethernet Design Rules

Gigabit Ethernet was first specified by two standards: IEEE 802.3z-1998 and 802.3ab-1999. The IEEE 802.3z standard specifies the operation of Gigabit Ethernet over fiber and coaxial cable and introduces the Gigabit Media-Independent Interface (GMII). These standards are superseded by the latest revision of all the 802.3 standards included in IEEE 802.3-2002.

The IEEE 802.3ab standard specified the operation of Gigabit Ethernet over CAT 5 UTP. Gigabit Ethernet still retains the frame formats and frame sizes, and it still uses CSMA/CD. As with Ethernet and Fast Ethernet, full-duplex operation is possible. Differences appear in the encoding; Gigabit Ethernet uses 8B10B coding with simple nonreturn to zero (NRZ). Because of the 20 percent overhead, pulses run at 1250 MHz to achieve a 1000 Mbps throughput.

Table 3-5 gives an overview of Gigabit Ethernet scalability constraints.

Table 3-5 *Gigabit Ethernet Scalability Constraints*

Type	Speed	Maximum Segment Length	Encoding	Media
1000BASE-T	1000 Mbps	100 m	Five-level	CAT 5 UTP
1000BASE-LX (long wavelength)	1000 Mbps	550 m	8B10B	Single-mode/ multimode fiber
1000BASE-SX (short wavelength)	1000 Mbps	62.5 micrometers: 220 m 50 micrometers: 500 m	8B10B	Multimode fiber
1000BASE-CX	1000 Mbps	25 m	8B10B	Shielded balanced copper

The following are the physical specifications for Gigabit Ethernet, each of which is described in the following sections:

- 1000BASE-LX
- 1000BASE-SX
- 1000BASE-CX
- 1000BASE-T

1000BASE-LX Long-Wavelength Gigabit Ethernet

IEEE 1000BASE-LX uses long-wavelength optics over a pair of fiber strands. The specifications are as follows:

- Uses long wave (1300 nanometers [nm])
- Use on multimode or single-mode fiber
- Maximum lengths for multimode fiber are
  - 62.5-micrometer fiber: 440 m
  - 50-micrometer fiber: 550 m
- Maximum length for single-mode fiber (9 micrometers) is 5 km
- Uses 8B10B encoding with simple NRZ

1000BASE-SX Short-Wavelength Gigabit Ethernet

IEEE 1000BASE-SX uses short-wavelength optics over a pair of multimode fiber stands. The specifications are as follows:

- Uses short wave (850 nm)
- Use on multimode fiber
- Maximum lengths:
  - 62.5-micrometer fiber: 260 m
  - 50-micrometer fiber: 550 m
- Uses 8B10B encoding with simple NRZ

1000BASE-CX Gigabit Ethernet over Coaxial Cable

IEEE 1000BASE-CX standard is for short copper runs between servers. The specification is as follows:

- Used on short-run copper
- Runs over a pair of 150-ohm balanced coaxial cables (twinax)
- Maximum length is 25 m
- Mainly for server connections
- Uses 8B10B encoding with simple NRZ

1000BASE-T Gigabit Ethernet over UTP

The IEEE standard for 1000-Mbps Ethernet over CAT 5 UTP was IEEE 802.3ab; it was approved in June 1999. It is now included in IEEE 802.3-2002. This standard uses the four pairs in the cable. (100BASE-TX and 10BASE-T Ethernet use only two pairs.) The specifications are as follows:

- CAT 5, four-pair UTP
- Maximum length is 100 m
- Encoding defined is a five-level coding scheme
- 1 byte is sent over the four pairs at 1250 MHz

10 Gigabit Ethernet (10GE) Design Rules

The IEEE 802.3ae supplement to the 802.3 standard, published in August 2002, specifies the standard for 10 Gigabit Ethernet. It is defined only for full-duplex operation over optical media. Hubs or repeaters cannot be used because they operate in half-duplex mode. It allows the use of Ethernet frames over distances typically encountered in metropolitan-area networks (MAN) and WANs. Other uses include data centers, corporate backbones, and server farms.

10GE Media Types

10GE has seven physical media specifications based on different fiber types and encoding. Multimode fiber (MMF) and single-mode fiber (SMF) are used. Table 3-6 describes the different 10GE media types.

Table 3-6 *10GE Media Types*

10GE Media Type	Wavelength/Fiber (Short or Long)	Distance	Other Description
10GBASE-SR	Short wavelength MMF	To 300 m	Uses 66B encoding
10GBASE-SW	Short wavelength MMF	To 300 m	Uses the WAN interface sublayer (WIS)
10GBASE-LR	Long wavelength SMF	To 10 km	Uses 66B encoding for dark fiber use
10GBASE-LW	Long wavelength SMF	To 10 km	Uses WIS
10GBASE-ER	Extra-long wavelength SMF	To 40 km	Uses 66B encoding for dark fiber use
10GBASE-EW	Extra-long wavelength SNMP	To 40 km	Uses WIS
10GBASE-LX4	Uses division multiplexing for both MMF and SMF	To 10 km	Uses 8B/10B encoding

Short-wavelength multimode fiber is 850 nm. Long-wavelength is 1310 nm, and extra-long-wavelength is 1550 nm. The WIS is used to interoperate with Synchronous Optical Network (SONET) STS-192c transmission format.

Fast EtherChannel

The Cisco EtherChannel implementations provide a method to increase the bandwidth between two systems by bundling Fast Ethernet or Gigabit Ethernet links. When bundling Fast Ethernet links, use Fast EtherChannel. EtherChannel port bundles allow you to group multiple ports into a single logical transmission path between the switch and a router, host, or another switch. EtherChannels provide increased bandwidth, load sharing, and redundancy. If a link fails in the

bundle, the other links take on the traffic load. You can configure EtherChannel bundles as trunk links.

Depending on your hardware, you can form an EtherChannel with up to eight compatibly configured ports on the switch. The participating ports must have the same speed and duplex mode and belong to the same VLAN.

Token Ring Design Rules

Token Ring is not a CCDA test subject but this section is included for reference because you might find Token Ring on existing networks. IBM developed Token Ring in the 1970s. In the 1980s, Token Ring and Ethernet competed as the preferred medium for LANs. The IEEE developed the IEEE 802.5 specification based on the IBM Token Ring specifications. The 802.5 working group is now inactive. The most recent specification is IEEE 802.5-1998. You can find more information at http://www.8025.org.

Table 3-7 lists some media characteristics for designing Token Ring segments.

Table 3-7 *Scalability Constraints for Token Ring*

Specification	IBM Token Ring	IEEE 802.5
Physical Topology	Star	Not specified
Maximum Segment Length	Depends on the type of cable, number of media attachment units (MAU), and so on	Depends on the type of cable, number of MAUs, and so on
Maximum Number of Attachments Per Segment	260 for STP, 72 for UTP	250
Maximum Network Diameter	Depends on the type of cable, number of MAUs, and so on	Depends on the type of cable, number of MAUs, and so on

LAN Hardware

This section covers the hardware devices and how to apply them to LAN design. You place devices in the LAN depending on their roles and capabilities. LAN devices are categorized based on how they operate in the OSI model. This section covers the following devices:

- Repeaters
- Hubs
- Bridges

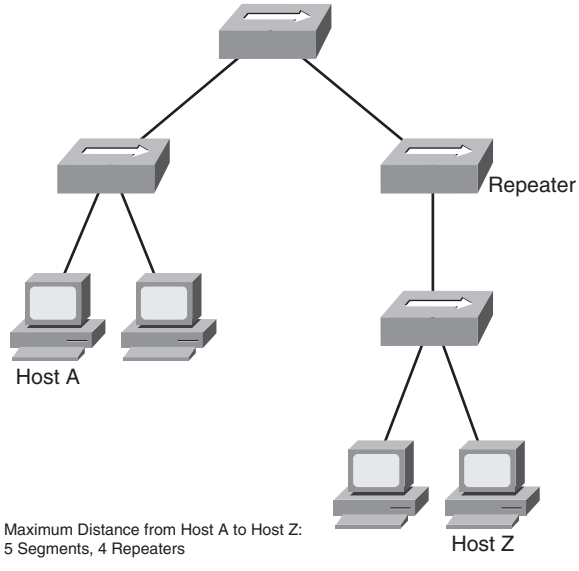
- Switches
- Routers
- Layer 3 switches

Repeaters

Repeaters are the basic unit in networks that connect separate segments. Repeaters take incoming frames, regenerate the preamble, amplify the signals, and send the frame out all other interfaces. Repeaters operate at the physical layer of the OSI model. Because repeaters are unaware of packets or frame formats, they do not control broadcasts or collision domains. Repeaters are said to be protocol-transparent because they are unaware of upper-layer protocols such as IP, Internetwork Packet Exchange (IPX), and so on.

One basic rule of using Ethernet repeaters is the 5-4-3 Rule, shown in Figure 3-2. The maximum path between two stations on the network should not be more than five segments, with four repeaters between those segments, and no more than three populated segments. Repeaters introduce a small amount of latency, or delay, when propagating the frames. A transmitting device must be able to detect a collision with another device within the specified time after the delay introduced by the cable segments and repeaters is factored in. The 512-bit time specification also governs segment lengths.

Figure 3-2 *Repeater 5-4-3 Rule*



Hubs

With the increasing density of LANs in the late 1980s and early 1990s, *hubs* were introduced to concentrate Thinnet and 10BASE-T networks in the wiring closet. Traditional hubs operate on the physical layer of the OSI model and perform the same functions as basic repeaters. The difference is that hubs have more ports than basic repeaters.

Bridges

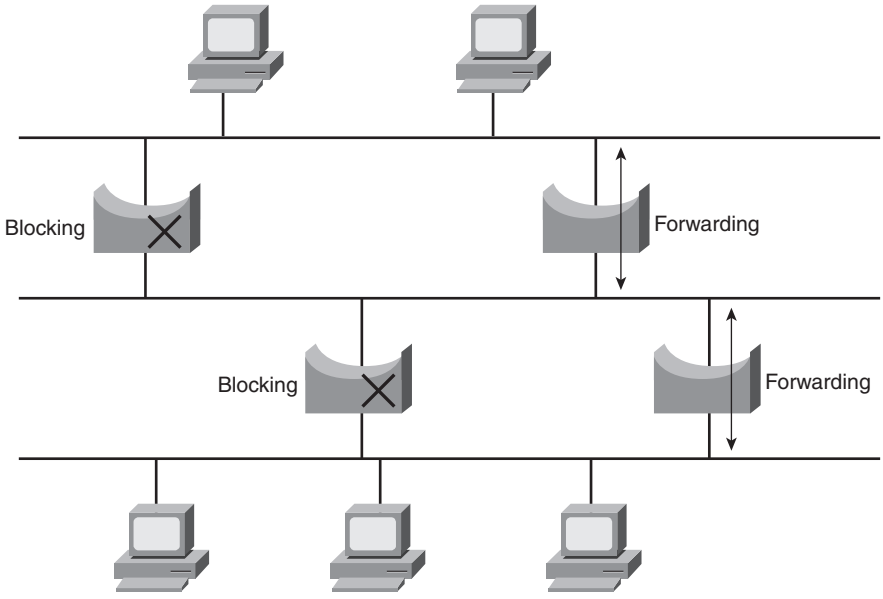
Bridges connect separate segments of a network. They differ from repeaters in that bridges are intelligent devices that operate in the data link layer of the OSI model. Bridges control the collision domains on the network. Bridges also learn the MAC layer addresses of each node on each segment and on which interface they are located. For any incoming frame, bridges forward the frame only if the destination MAC address is on another port or if the bridge is unaware of its location. The latter is called *flooding*. Bridges filter any incoming frames with destination MAC addresses that are on the same segment from where the frame arrives; they do not forward these frames.

Bridges are store-and-forward devices. They store the entire frame and verify the cyclic redundancy check (CRC) before forwarding. If the bridges detect a CRC error, they discard the frame. Bridges are protocol-transparent; they are unaware of the upper-layer protocols such as IP, IPX, and AppleTalk. Bridges are designed to flood all unknown and broadcast traffic.

Bridges implement Spanning Tree Protocol (STP) to build a loop-free network topology. Bridges communicate with each other, exchanging information such as priority and bridge interface MAC addresses. They select a root bridge and then implement STP. Some interfaces are in a blocking state, whereas other bridges have interfaces in forwarding mode. Figure 3-3 shows a network with bridges. STP has no load sharing or dual paths, as there is in routing. STP provides recovery of bridge failure by changing blocked interfaces to a forwarding state if a primary link fails. Although DEC and IBM versions are available, the IEEE 802.1d standard is the STP most commonly used.

STP elects a *root bridge* as the tree's root. It places all ports that are not needed to reach the root bridge in blocking mode. The selection of the root bridge is based on the lowest numerical bridge priority. The bridge priority ranges from 0 to 65,535. If all bridges have the same bridge priority, the bridge with the lowest MAC address becomes the root. The concatenation of the bridge priority and the MAC address is the bridge identification (BID). Physical changes to the network force spanning-tree recalculation.

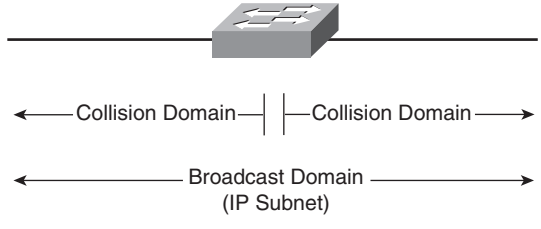
Figure 3-3 *Spanning Tree Protocol*



Switches

Switches use specialized integrated circuits to reduce the latency common to regular bridges. Switches are the evolution of bridges. Some switches can run in cut-through mode, where the switch does not wait for the entire frame to enter its buffer; instead, it begins to forward the frame as soon as it finishes reading the destination MAC address. Cut-through operation increases the probability that frames with errors are propagated on the network, because it forwards the frame before the entire frame is buffered and checked for errors. Because of these problems, most switches today perform store-and-forward operation as bridges do. As shown in Figure 3-4, switches are exactly the same as bridges with respect to collision-domain and broadcast-domain characteristics. Each port on a switch is a separate collision domain. By default, all ports in a switch are in the same broadcast domain. Assignment to different VLANs changes that behavior.

Figure 3-4 *Switches Control Collision Domains*



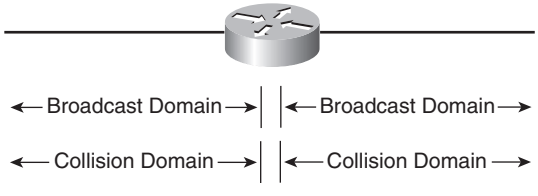
Switches have characteristics similar to bridges; however, they have more ports and run faster. Switches keep a table of MAC addresses per port, and they implement STP. Switches are data link layer devices. They are transparent to protocols operating at the network layer and above. Each port on a switch is a separate collision domain but is part of the same broadcast domain. Switches do not control broadcasts on the network.

The use of LAN switches instead of bridges or hubs is nearly universal. Switches are preferred over shared technology because they provide full bandwidth in each direction when configured in duplex mode. All the devices on a hub share the bandwidth in a single collision domain. Switches can also use VLANs to provide more segmentation. The "LAN Design Types and Models" section in this chapter discusses VLANs.

Routers

Routers make forwarding decisions based on network layer addresses. When an Ethernet frame enters the router, the layer 2 header is removed, the router forwards based on the layer 3 IP address and adds a new layer 2 address at the egress interface. In addition to controlling collision domains, routers bound data link layer broadcast domains. Each interface of a router is a separate broadcast domain. Routers do not forward data link layer broadcasts. IP defines network layer broadcast domains with a subnet and mask. Routers are aware of the network protocol, which means they can forward packets of routed protocols, such as IP and IPX. Figure 3-5 shows a router; each interface is a broadcast and a collision domain.

Figure 3-5 *Routers Control Broadcast and Collision Domains*



Routers exchange information about destination networks using one of several routing protocols. Routers use routing protocols to build a list of destination networks and to identify the best routes to reach those destinations. The following are examples of routing protocols:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Routing Information Protocol (RIP)
- Intermediate System-to-Intermediate System (IS-IS)

Chapter 9, "Routing Protocol Selection Criteria," discusses routing protocols in further detail. Routers translate data link protocols. They are the preferred method of forwarding packets between networks of differing media, such as Ethernet to Token Ring or Ethernet to serial. They also provide methods to filter traffic based on the network layer address, route redundancy, load balancing, hierarchical addressing, and multicast routing.

Layer 3 Switches

LAN switches that can run routing protocols are *Layer 3 switches*. These switches can run routing protocols and communicate with neighboring routers. Layer 3 switches have LAN technology interfaces that perform network layer packet forwarding. The use of switching technologies at the network layer greatly accelerates packet forwarding between connected LANs, including VLANs. You can use the router capacity you save to implement other features, such as security filtering and intrusion detection.

Layer 3 switches perform the functions of both data link layer switches and network layer routers. Each port is a collision domain. You can group ports into network layer broadcast domains (subnets). As with routers, a routing protocol provides network information to other network layer devices (subnets), and a routing protocol provides network information to other Layer 3 switches and routers.

LAN Design Types and Models

LANs can be classified as large-building LANs, campus LANs, or small and remote LANs. The large-building LAN typically contains a major data center with high-speed access and floor communications closets; the large-building LAN is usually the headquarters in larger companies. Campus LANs provide connectivity between buildings on a campus. Redundancy is usually a requirement in large-building and campus LAN deployments. Small and remote LANs provide connectivity to remote offices with a relatively small number of nodes.

Campus design factors include the following categories:

- Network application characteristics
- Infrastructure device characteristics
- Environmental characteristics

Applications are defined by the business, and the network must be able to support them. Applications may require high bandwidth or be time-sensitive. The infrastructure devices influence the design. Decisions on switched or routed architectures and port limitations influence the design. The actual physical distances affect the design. The selection of copper or fiber media

may be influenced by the environmental or distance requirements. The following sections show some sample LAN types. Table 3-8 summarizes the different application types.

Table 3-8 *Application Types*

Application Type	Description
Peer-to-peer	Includes instant messaging, file sharing, IP phone calls, and videoconferencing.
Client-local servers	Servers are located in the same segment as the clients or close by.
Client/server farms	Mail, server, file, and database servers. Access is reliable and controlled.
Client-Enterprise Edge servers	External servers such as SMTP, web, public servers, and e-commerce.

Best Practices for Hierarchical Layers

Each layer of the hierarchical architecture contains special considerations. The following sections describe best practices for each of the three layers of the hierarchical architecture: access, distribution, and core.

Access Layer Best Practices

When designing the building access layer, you must take into consideration the number of users or ports required to size up the LAN switch. Connectivity speed for each host should be considered. Hosts might be connected using various technologies such as Fast Ethernet, Gigabit Ethernet, or port channels. The planned VLANs enter into the design.

Performance in the access layer is also important. Redundancy and QoS features should be considered.

The following are recommended best practices for the building access layer:

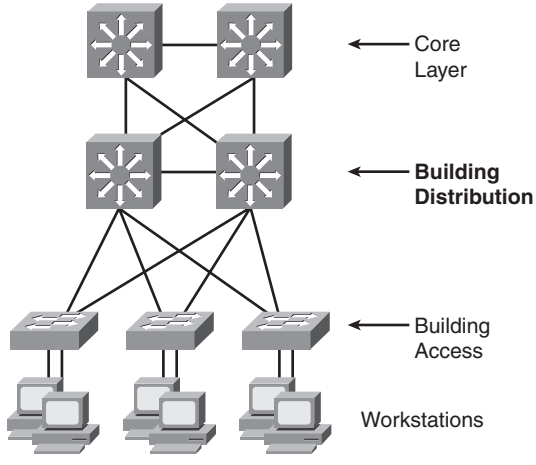
- Limit VLANs to a single closet when possible to provide the most deterministic and highly available topology.
- Use RPVST+ if STP is required. It provides the best convergence.
- Set VLAN Dynamic Trunking Protocol (DTP) to desirable/desirable with negotiation on.
- Manually prune unused VLANs to avoid broadcast propagation.
- Use VTP transparent mode, because there is little need for a common VLAN database in hierarchical networks.

- Disable trunking on host ports, because it is not necessary. Doing so provides more security and speeds up PortFast.
- Consider implementing routing in the access layer to provide fast convergence and Layer 3 load balancing.
- Use the **switchport host** commands on server and end-user ports to enable PortFast and disable channeling on these ports.

Distribution Layer Best Practices

As shown in Figure 3-6, the distribution layer aggregates all closet switches and connects to the core layer. Design considerations for the distribution layer include providing wire-speed performance on all ports, link redundancy, and infrastructure services.

Figure 3-6 *Distribution Layer*



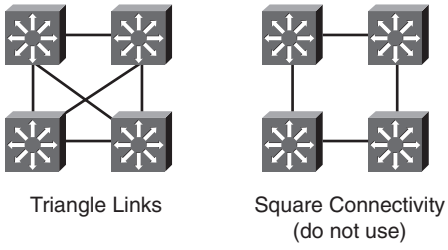
The distribution layer should not be limited on performance. Links to the core must be able to support the bandwidth used by the aggregate access layer switches. Redundant links from the access switches to the distribution layer and from the distribution layer to the core layer allow for high availability in the event of a link failure. Infrastructure services include QoS configuration, security, and policy enforcement. Access lists are configured in the distribution layer.

The following are recommended best practices at the distribution layer:

- Use first-hop redundancy protocols. Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) should be used if you implement Layer 2 links between the Layer 2 access switches and the distribution layer.

- Use Layer 3 links between the distribution and core switches to allow for fast convergence and load balancing.
- Build Layer 3 triangles, not squares as shown in Figure 3-7.

Figure 3-7 *Layer 3 Triangles*



- Use the distribution switches to connect Layer 2 VLANs that span multiple access layer switches.
- Summarize routes from the distribution to the core of the network to reduce routing overhead.

Core Layer Best Practices

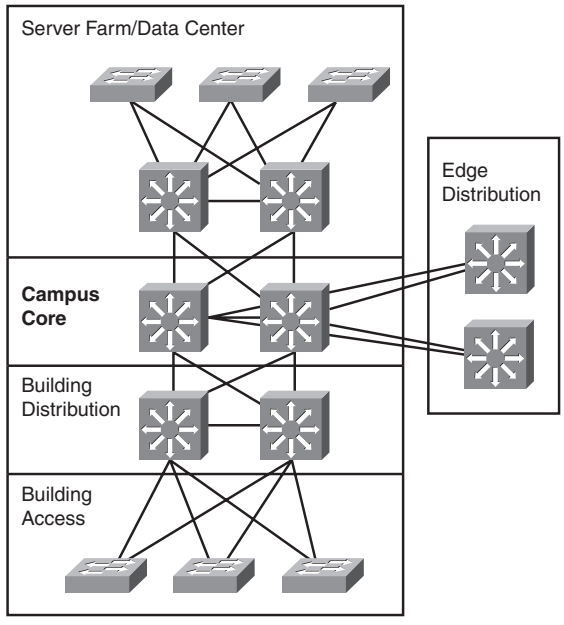
Depending on the network's size, a core layer may or may not be needed. For larger networks, building distribution switches are aggregated to the core. This provides high-speed connectivity to the server farm/data center and to the Enterprise Edge (to the WAN and the Internet).

Figure 3-8 shows the criticality of the core switches. The core must provide high-speed switching with redundant paths for high availability to all the distribution points. The core must support gigabit speeds and data and voice integration.

The following are best practices for the campus core:

- Reduce the switch peering by using redundant triangle connections between switches.
- Use routing that provides a topology with no Layer 2 loops which are seen in Layer 2 links using spanning tree protocol.
- Use Layer 3 switches on the core that provide intelligent services that Layer 2 switches do not support.

Figure 3-8 *Core Switches*

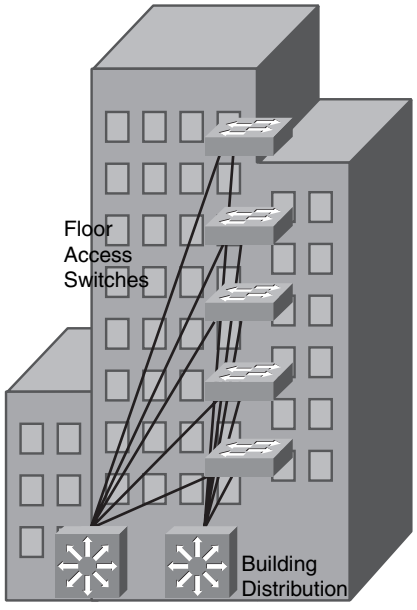


Large-Building LANs

Large-building LANs are segmented by floors or departments. The building-access component serves one or more departments or floors. The building-distribution component serves one or more building-access components. Campus and building backbone devices connect the data center, building-distribution components, and the Enterprise Edge-distribution component. The access layer typically uses Layer 2 switches to contain costs, with more expensive Layer 3 switches in the distribution layer to provide policy enforcement. Current best practice is to also deploy Layer 3 switches in the campus and building backbone. Figure 3-9 shows a typical large-building design.

Each floor can have more than 200 users. Following a hierarchical model of building access, building distribution, and core, Fast Ethernet nodes can connect to the Layer 2 switches in the communications closet. Fast Ethernet or Gigabit Ethernet uplink ports from closet switches connect back to one or two (for redundancy) distribution switches. Distribution switches can provide connectivity to server farms that provide business applications, DHCP, DNS, intranet, and other services.

Figure 3-9 *Large-Building LAN Design*

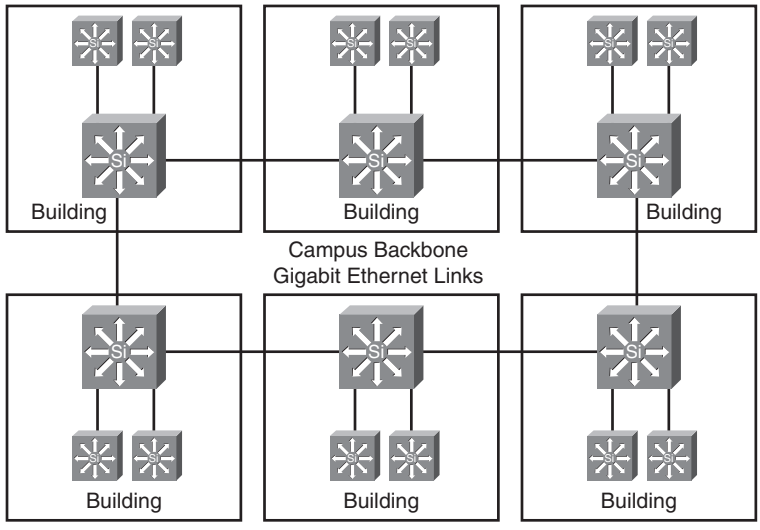


Enterprise Campus LANs

A campus LAN connects two or more buildings within a local geographic area using a high-bandwidth LAN media backbone. Usually the enterprise owns the medium (copper or fiber). High-speed switching devices minimize latency. In today's networks, Gigabit Ethernet campus backbones are the standard for new installations. In Figure 3-10, Layer 3 switches with Gigabit Ethernet media connect campus buildings.

Ensure that you implement a hierarchical composite design on the campus LAN and that you assign network layer addressing to control broadcasts on the networks. Each building should have addressing assigned in such a way as to maximize address summarization. Apply contiguous subnets to buildings at the bit boundary to apply summarization and ease the design. Campus networks can support high-bandwidth applications such as videoconferencing. Remember to use Layer 3 switches with high-switching capabilities in the campus-backbone design. In smaller installations, it might be desirable to collapse the building-distribution component into the campus backbone. An increasingly viable alternative is to provide building access and distribution on a single device selected from among the smaller Layer 3 switches now available.

Figure 3-10 *Campus LAN*



Edge Distribution

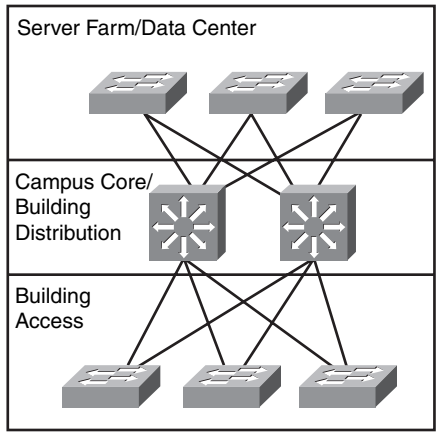
For large campus LANs, the Edge Distribution module provides additional security between the campus LAN and the Enterprise Edge (WAN, Internet, and VPNs). The edge distribution protects the campus from the following threats:

- **IP spoofing**—The edge distribution switches protect the core from spoofing of IP addresses.
- **Unauthorized access**—Controls access to the network core.
- **Network reconnaissance**—Filtering of network discovery packets to prevent discovery from external networks.
- **Packet sniffers**—The edge distribution separates the edge's broadcast domains from the campus, preventing possible network packet captures.

Medium Site LANs

Medium-sized LANs contain 200 to 1000 devices. Usually the distribution and core layers are collapsed in the medium-sized network. Access switches are still connected to both distribution/core switches to provide redundancy. Figure 3-11 shows the medium campus LAN.

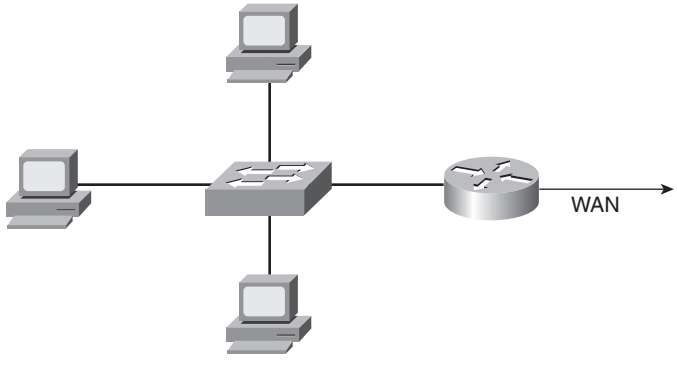
Figure 3-11 *Medium Campus LAN*



Small and Remote Site LANs

Small and remote sites usually connect to the corporate network via a small router. The LAN service is provided by a small LAN switch. The router filters broadcast to the WAN circuit and forward packets that require services from the corporate network. You can place a server at the small or remote site to provide DHCP and other local applications such as a backup domain controller and DNS; if not, you must configure the router to forward DHCP broadcasts and other types of services. As the site grows, you will need the structure provided by the Enterprise Composite Network model. Figure 3-12 shows a typical architecture of a remote LAN.

Figure 3-12 *Remote Office LAN*

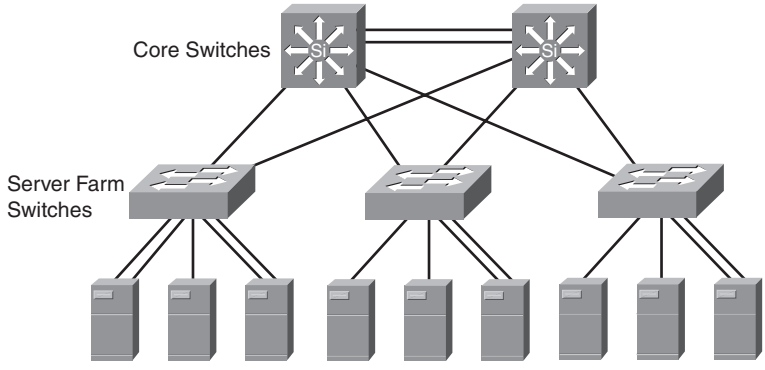


Server-Farm Module

The server-farm or data-center module provides high-speed access to servers for the campus networks. You can attach servers to switches via Gigabit Ethernet or 10 Gigabit Ethernet. Some campus deployments might need EtherChannel technology to meet traffic requirements. Figure

3-13 shows an example of a server-farm module for a small network. Servers are connected via Fast Ethernet or Fast EtherChannel.

Figure 3-13 *Server Farm*



The server-farm switches connect via redundant uplink ports to the core switches. The largest deployments might find it useful to hierarchically construct service to the data center using access and distribution network devices.

Server distribution switches are used in larger networks. Access control lists and QoS features are implemented on the server distribution switches to protect the servers and services and to enforce network policies.

Server Connectivity Options

Servers can be connected in three primary options:

- Single NIC
- Dual NIC EtherChannel
- Content switching

Single NIC connected servers contain Fast or Gigabit Ethernet full-duplex speeds with no redundancy. Servers requiring redundancy can be connected with dual NICs using switch EtherChannel.

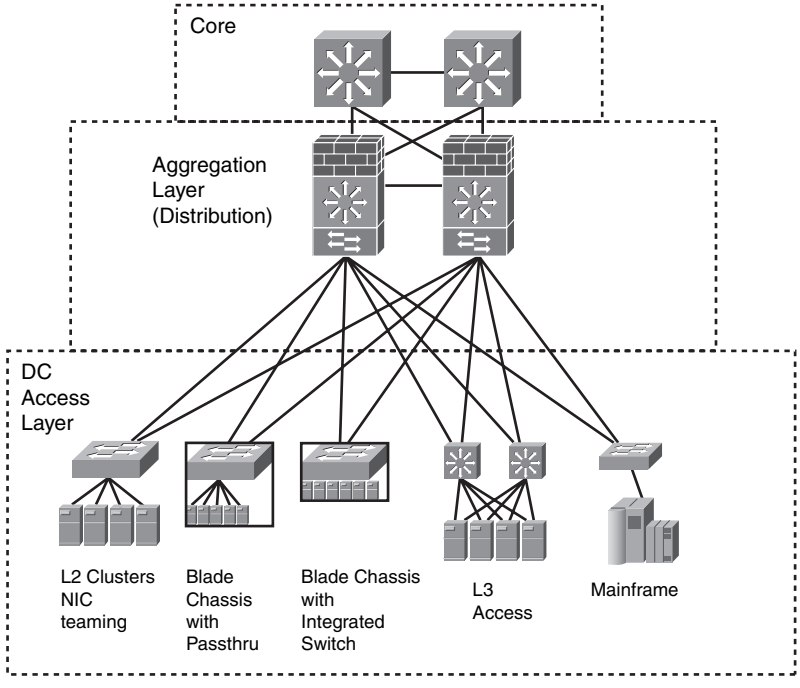
Advanced redundancy solutions use content switches that front end multiple servers. This provides redundancy and load balancing per user request.

Enterprise Data Center Infrastructure

Data centers (DC) contain different types of server technologies, including standalone servers, blade servers, mainframes, clustered servers, and virtual servers.

Figure 3-14 shows the Enterprise DC. The DC access layer must provide the port density to support the servers, provide high-performance/low-latency Layer 2 switching, and support dual and single connected servers. The preferred design is to contain Layer 2 to the access layer and Layer 3 on the distribution. Some solutions push Layer 3 links to the access layer. Blade chassis with integrated switches have become a popular solution. Each blade switch houses 16 Intel platforms, each logically connected within the chassis to two access switches.

Figure 3-14 *Enterprise Data Center*



The DC aggregation layer (distribution layer) aggregates traffic to the core. Deployed on the aggregation layer are

- **Load balancers** to provide load balancing to multiple servers
- **SSL offloading devices** to terminate SSL sessions
- **Firewalls** to control and filter access
- **Intrusion detection devices** to detect network attacks

Campus LAN Quality of Service Considerations

For the access layer of the campus LAN, you can classify and mark frames or packets to apply quality of service (QoS) policies in the distribution or at the Enterprise Edge. Classification is a fundamental building block of QoS and involves recognizing and distinguishing between different traffic streams. For example, you distinguish between HTTP/HTTPS, FTP, and VoIP traffic. Without classification, all traffic would be treated the same.

Marking sets certain bits in a packet or frame that has been classified. Marking is also called coloring or tagging. Layer 2 has two methods to mark frames for CoS:

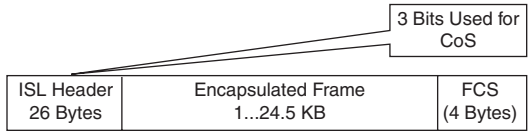
- Inter-Switch Link (ISL)
- IEEE 802.1p/802.1Q

The IEEE 802.1D-1998 standard describes IEEE 802.1p traffic class expediting.

Both methods provide 3 bits for marking frames. The Cisco ISL is a proprietary trunk-encapsulation method for carrying VLANs over Fast Ethernet or Gigabit Ethernet interfaces.

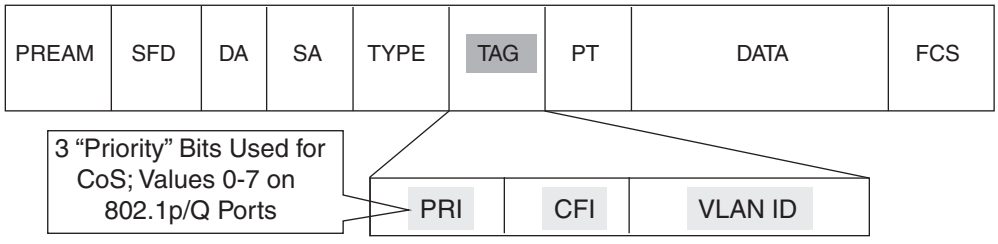
ISL appends tags to each frame to identify the VLAN it belongs to. As shown in Figure 3-15, the tag is a 30-byte header and CRC trailer that are added around the Fast Ethernet frame. This includes a 26-byte header and 4-byte CRC. The header includes a 15-bit VLAN ID that identifies each VLAN. The user field in the header also includes 3 bits for the CoS.

Figure 3-15 *ISL Frame*



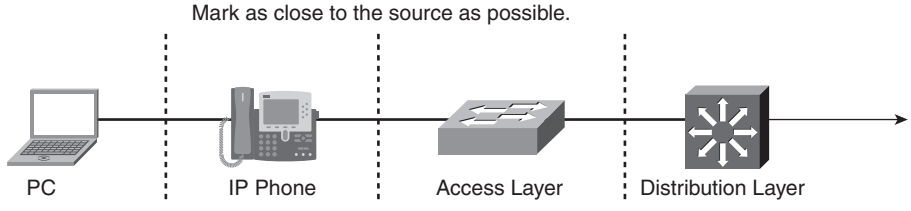
The IEEE 802.1Q standard trunks VLANs over Fast Ethernet and Gigabit Ethernet interfaces, and you can use it in a multivendor environment. IEEE 802.1q uses one instance of STP for each VLAN allowed in the trunk. Like ISL, IEEE 802.1Q uses a tag on each frame with a VLAN identifier. Figure 3-16 shows the IEEE 802.1Q frame. Unlike ISL, 802.1Q uses an internal tag. IEEE 802.1Q also supports the IEEE 802.1p priority standard, which is included in the 802.1D-1998 specification. A 3-bit priority field is included in the 802.1Q frame for CoS.

Figure 3-16 *IEEE 802.1Q Frame*



The preferred location to mark traffic is as close as possible to the source. Figure 3-17 shows a segment of a network with IP phones. Most workstations send packets with CoS or IP precedence bits (ToS) set to 0. If the workstation supports IEEE 802.1Q/p, it can mark packets. The IP phone can reclassify traffic from the workstation to 0. VoIP traffic from the phone is sent with a Layer 2 CoS set to 5 or Layer 3 ToS set to 5. The phone also reclassifies data from the PC to a CoS/ToS of 0. With Differentiated Services Code Point (DSCP), VoIP traffic is set to Expedited Forwarding (EF), binary value 101110 (hexadecimal 2E).

Figure 3-17 *Marking of Frames or Packets*



As shown in Figure 3-17, switches' capabilities vary in the access layer. If the switches in this layer are capable, configure them to accept the markings or remap them. The advanced switches in the distribution layer can mark traffic, accept the CoS/ToS markings, or remap the CoS/ToS values to different markings.

Multicast Traffic Considerations

Internet Group Management Protocol (IGMP) is the protocol between end workstations and the local Layer 3 switch. IGMP is the protocol used in multicast implementations between the end hosts and the local router. RFC 2236 describes IGMP version 2 (IGMPv2). RFC 1112 describes the first version of IGMP. IP hosts use IGMP to report their multicast group memberships to routers. IGMP messages use IP protocol number 2. IGMP messages are limited to the local interface and are not routed.

RFC 3376 describes IGMP Version 3 (IGMPv3) IGMPv3 provides the extensions required to support source-specific multicast (SSM). It is designed to be backward-compatible with both prior versions of IGMP. All versions of IGMP are covered in Chapter 12, "Border Gateway Protocol, Route Manipulation, and IP Multicast."

When campus LANs use multicast media, end hosts that do not participate in multicast groups might get flooded with unwanted traffic. Two solutions are

- CGMP
- IGMP snooping

CGMP

Cisco Group Management Protocol (CGMP) is a Cisco-proprietary protocol implemented to control multicast traffic at Layer 2. Because a Layer 2 switch is unaware of Layer 3 IGMP messages, it cannot keep multicast packets from being sent to all ports.

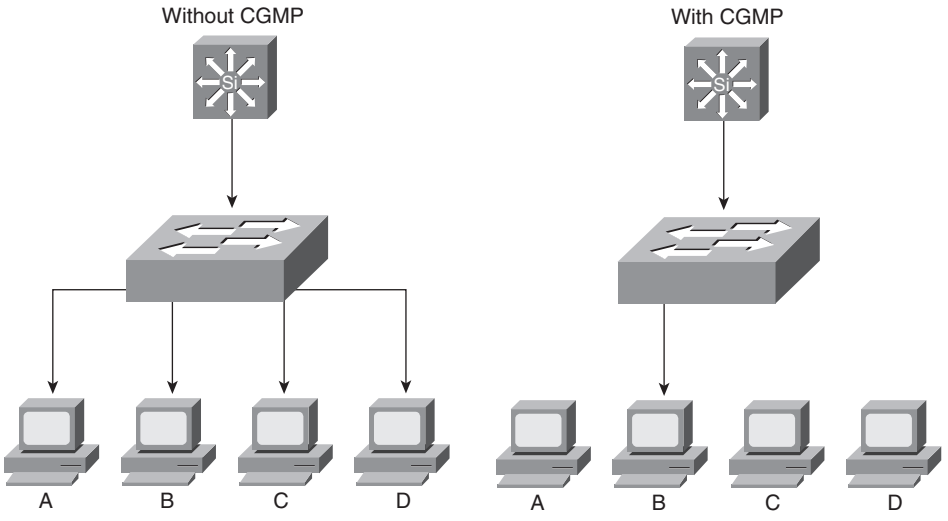
As shown in Figure 3-18, with CGMP, the LAN switch can speak with the IGMP router to find out the MAC addresses of the hosts that want to receive the multicast packets. You must also enable the router to speak CGMP with the LAN switches. With CGMP, switches distribute multicast sessions to the switch ports that have group members.

When a CGMP-enabled router receives an IGMP report, it processes the report and then sends a CGMP message to the switch. The switch can then forward the multicast messages to the port with the host receiving multicast traffic. CGMP Fast-Leave processing allows the switch to detect IGMP Version 2 leave messages sent by hosts on any of the supervisor engine module ports. When the IGMPv2 leave message is sent, the switch can then disable multicast for the port.

IGMP Snooping

IGMP snooping is another way for switches to control multicast traffic at Layer 2. It can be used instead of CGMP. With IGMP snooping, switches listen to IGMP messages between the hosts and routers. If a host sends an IGMP query message to the router, the switch adds the host to the multicast group and permits that port to receive multicast traffic. The port is removed from multicast traffic if an IGMP leave message is sent from the host to the router. The disadvantage of IGMP snooping is that it must listen to every IGMP control message, which can impact the switch's CPU utilization.

Figure 3-18 *CGMP*



References and Recommended Readings

10Gigabit Alliance, http://www.10gea.org

"Cisco Data Center Network Architecture and Solutions Overview," http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c643/cdccont_0900aecd802c9a4f.pdf?pcontent=dc_us&pagename=Data%20Center%20Solutions%20Overview

"CSMA/CD Access Method, IEEE 802.3-2005." New York, NY: Institute of Electrical and Electronics Engineers, 2005

IEEE P802.3ae 10Gb/s Ethernet Task Force, http://grouper.ieee.org/groups/802/3/ae/index.html

"Token-Ring Access Method, IEEE 802.5-1998." Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 1998

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires you to be familiar with the following topics that were addressed in this chapter:

- **LAN media**—Ethernet, Token Ring, and Gigabit LAN media
- **LAN hardware**—Components used in LAN networks
- **LAN design types and models**—Building and campus LAN types and LAN design models

Tables 3-9 through 3-15 provide an overview of the following items that will also assist you in preparing for the CCDA exam:

- Application types
- Overview and comparison of LAN devices
- Summary of LAN types and their characteristics
- Description of the components of the enterprise campus model
- Summary of the modules on the campus infrastructure

Table 3-9 *Application Types*

Application Type	Description
Peer-to-peer	Includes instant messaging, file sharing, IP phone calls, and videoconferencing.
Client-local servers	Servers are located in the same segment as the clients or close by.
Client/server farms	Mail, server, file, and database servers. Access is reliable and controlled.
Client-Enterprise Edge servers	External servers such as SMTP, web, public servers, and e-commerce.

Table 3-10 *Comparison of Transmission Media*

Media	Bandwidth	Distance	Price
Twisted pair	Up to 1 Gbps	100 m	Inexpensive
Multimode fiber	Up to 1 Gbps	2 km (FE) 550 m (GE)	Moderate
Single-mode fiber	10 Gbps	90 km (FE) 40 km (GE)	Moderate to expensive
Wireless	54 Mbps (27 Mbps effective)	500 m at 1 Mbps	Moderate

Table 3-11 *LAN Device Comparison*

Device	OSI Layer	Is Domain Protocol-Transparent or Protocol-Aware?	Boundary	What It Understands
Repeater	Layer 1: physical	Transparent	Amplify signal	Bits
Hub	Layer 1: physical	Transparent	Amplify signal	Bits
Bridge	Layer 2: data link	Transparent	Collision domain	Frames
Switch	Layer 2: data link	Transparent	Collision domain	Frames
Router	Layer 3: network	Aware	Broadcast domain	Packets
Layer 3 switch	Layer 3: network	Aware	Broadcast domain	Packets

Table 3-12 *Campus Layer Design Best Practices*

Campus Layer	Best Practices
Access layer	Limit VLANs to a single closet when possible to provide the most deterministic and highly available topology. Use RPVST+ if STP is required. It provides the best convergence. Set VLAN Dynamic Trunking Protocol (DTP) to desirable/desirable with negotiation on. Manually prune unused VLANs to avoid broadcast propagation. Use VTP transparent mode, because there is little need for a common VLAN database in hierarchical networks. Disable trunking on host ports, because it is not necessary. Doing so provides more security and speeds up PortFast. Consider implementing routing in the access layer to provide fast convergence and Layer 3 load balancing.
Distribution layer	Use first-hop redundancy protocols. Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) should be used if you implement Layer 2 links between the access and distribution. Use Layer 3 links between the distribution and core switches to allow for fast convergence and load balancing. Build Layer 3 triangles, not squares. Use the distribution switches to connect Layer 2 VLANs that span multiple access layer switches. Summarize routes from the distribution to the core of the network to reduce routing overhead.
Core layer	Reduce the switch peering by using redundant triangle connections between switches. Use routing that provides a topology with no spanning-tree loops. Use Layer 3 switches on the core that provide intelligent services that Layer 2 switches do not support.

Table 3-13 *LAN Types*

LAN Type	Characteristics
Large-building network	Large number of users, data center, floor closet switches, multiple LANs within the building, high-speed backbone switching between distribution devices
Campus network	High-speed backbone switching between multiple buildings in a geographic area
Small or remote LAN	Small number of users, small switches

Table 3-14 *Enterprise Campus Model Components*

Component	Description
Campus infrastructure	Core, building distribution, and building access
Server farm	Connects to the campus backbone; has enterprise servers
Edge distribution	Connects the campus backbone to the Enterprise Edge

Table 3-15 *Campus Infrastructure Modules*

Component	Description
Core or campus backbone	High-end Layer 3 switches
Building distribution	Layer 3 or Layer 2 switches providing redundant distribution to the access layer
Building access	Layer 2 access switches

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: Layer 2 switches control network broadcasts.
2. What technology can you use to limit multicasts at Layer 2?
3. True or false: Packet marking is also called coloring.
4. True or false: Usually the distribution and core layers are collapsed in medium-sized networks.
5. What are two methods to mark frames to provide CoS?
6. Which of the following is an example of a peer-to-peer application?
   a. IP phone call
   b. Client accessing file server
   c. Web access
   d. Using a local server on the same segment
7. What primary design factors affect the design of a campus network? (Select three.)
   a. Environmental characteristics
   b. Number of file servers
   c. Infrastructure devices
   d. Fiber and UTP characteristics
   e. Network applications
   f. Windows, Linux, and mainframe operating systems
8. You need to connect a building access switch to the distribution switch. The cable distance is 135 m. What type of cable do you recommend?
   a. UTP
   b. Coaxial cable
   c. Multimode fiber
   d. Single-mode fiber

9. Which layer of the campus network corresponds to the data center aggregation layer?
   a. Core layer
   b. Distribution layer
   c. Access layer
   d. Server farm
10. Which of the following is an access layer best practice?
   a. Reduce switch peering and routing
   b. Use HSRP and summarize routes
   c. Disable trunking and use RPVST+
   d. Offload SSL sessions and use load balancers
11. Which of the following is a distribution layer best practice?
   a. Reduce switch peering and routing
   b. Use HSRP and summarize routes
   c. Disable trunking and use RPVST+
   d. Offload SSL sessions and use load balancers
12. Which of the following is a core layer best practice?
   a. Reduce switch peering and routing
   b. Use HSRP and summarize routes
   c. Disable trunking and use RPVST+
   d. Offload SSL sessions and use load balancers
13. Which of the following is a DC aggregation layer best practice?
   a. Reduce switch peering and routing
   b. Use HSRP and summarize routes
   c. Disable trunking and use RPVST+
   d. Offload SSL sessions and use load balancers
14. Which of the following are threats to the edge distribution?
   a. IP spoofing
   b. Network discovery
   c. Packet-capture devices
   d. All of the above

15. An enterprise network has grown to multiple buildings supporting multiple departments. Clients access servers that are in local and other buildings. The company security assessment has identified policies that need to be applied. What would you recommend?

    a. Move all departments to a single building to prevent unauthorized access.

    b. Move all servers to one of the LAN client segments.

    c. Move all servers to a server farm segment that is separate from client LANs.

    d. Move all servers to the building distribution switches.

16. Link redundancy and infrastructure services are design considerations for which layer(s)?

    a. Core layer

    b. Distribution layer

    c. Access layer

    d. All of the above

17. Which of the following are server connectivity methods in the server farm?

    a. Single NIC

    b. EtherChannel

    c. Content switch

    d. All of the above

18. What is the recommended method to connect the distribution switches to the core?

    a. Redundant triangle links

    b. Redundant cross-connect links

    c. Redundant Layer 3 squares

    d. Redundant Layer 2 links

19. A campus network of four buildings is experiencing performance problems. Each building contains 400 to 600 devices, all in one IP subnet. The buildings are connected in a hub-and-spoke configuration back to building 1 using Gigabit Ethernet with multimode fiber. All servers are located in building 1. What would you recommend to improve performance?

    a. Connect all buildings in a ring topology

    b. Implement multiple VLANs in each building

    c. Move servers to the buildings

    d. Use single-mode fiber to make the Gigabit Ethernet links faster

20. What of the following is true about data link layer broadcasts?
    a. Not controlled by routers
    b. Not forwarded by routers
    c. Not forwarded by switches
    d. Not controlled by VLANs
21. Match each LAN medium with its original physical specification:

    i. Fast Ethernet

    ii. Gigabit Ethernet

    iii. WLAN

    iv. Token Ring

    v. 10Gigabit Ethernet

    a. IEEE 802.3ab

    b. IEEE 802.11b

    c. IEEE 802.3u

    d. IEEE 802.3ae

    e. IEEE 802.5
22. True or false: Layer 3 switches bound Layer 2 collision and broadcast domains.
23. Match each Enterprise Campus component with its description:

    i. Campus infrastructure

    ii. Server farm

    iii. Edge distribution

    a. Consists of backbone, building-distribution, and building-access modules

    b. Connects the campus backbone to the Enterprise Edge

    c. Provides redundancy access to the servers
24. Match each LAN device type with its description:

    i. Hub

    ii. Bridge

    iii. Switch

    iv. Layer 3 switch

    v. Router

a. Legacy device that connects two data link layer segments

b. Network layer device that forwards packets to serial interfaces connected to the WAN

c. High-speed device that forwards frames between two or more data link layer segments

d. High-speed device that bounds data link layer broadcast domains

e. Device that amplifies the signal between connected segments

25. Match each application type with its description:

i. Peer-to-peer

ii. Client-local server

iii. Client/server farm

iv. Client-Enterprise Edge

a. Server on the same segment

b. IM

c. Web access

d. Client accesses database server

26. Match each transmission medium with its upper-limit distance:

i. UTP

ii. Wireless

iii. Single-mode fiber

iv. Multimode fiber

a. 2 km

b. 100 m

c. 90 km

d. 500 m

27. True or false: IP phones and LAN switches can reassign a frame's CoS bits.

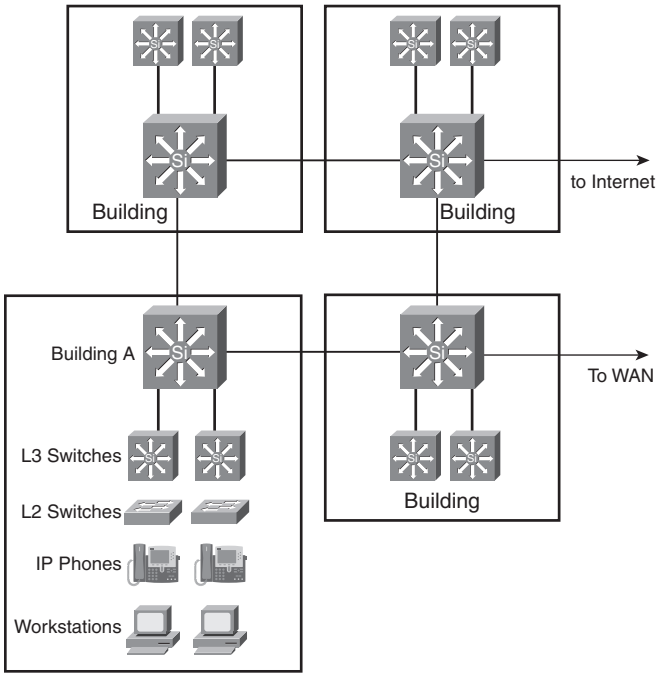
28. Name two ways to reduce multicast traffic in the access layer.

29. What are two VLAN methods you can use to carry marking CoS on frames?

30. True or false: You can configure CGMP in mixed Cisco switch and non-Cisco router environments.

Use Figure 3-19 to answer the following questions.

Figure 3-19 *Enterprise Campus Diagram*



31. What medium would you recommend for the campus LAN backbone?
32. The workstations send frames with the CoS set to 5. What should the IP phones do so that the network gives preference to VoIP traffic over data traffic?
33. If the Layer 2 switches in Building A cannot look at CoS and ToS fields, where should these fields be inspected for acceptance or reclassification: in the building Layer 3 switches or in the backbone Layer 3 switches?
34. Does the network have redundant access to the WAN?
35. Does the network have redundant access to the Internet?
36. Does Figure 3-19 use recommended devices for networks designed using the Enterprise Architecture model?

This chapter covers the following subjects:

- Wireless LAN Technologies
- Cisco Unified Wireless Network
- Wireless LAN Design

CHAPTER 4

Wireless LAN Design

Wireless LANs allow users to connect to network resources and services without using cables. With wireless LANs, users connect to the network in common areas, away from their desk, and in areas that do not easily accommodate the installation of wired cabling, such as outdoors and in designated historical sites. This chapter describes wireless LAN technologies, design, and Cisco solutions.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

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

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

Foundation Topics Section	Questions Covered in This Section
Wireless LAN Technologies	1, 2
Cisco Unified Wireless Network	3, 4, 5
Wireless LAN Design	6, 7, 8

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you with false sense of security.

1. What technology provides 54 Mbps of bandwidth using UNII frequencies?
   a. IEEE 802.11b
   b. IEEE 802.11g
   c. IEEE 802.11a
   d. Bluetooth
2. What frequency allotment provides 11 channels for unlicensed use for wireless LANs in North America?
   a. UNII
   b. ISM
   c. Bluetooth
   d. FM
3. What standard is used for control messaging between access points and controllers?
   a. IEEE 802.11
   b. CSMA/CA
   c. IEEE 802.1X
   d. LWAPP
4. Which WLAN controller interface is used for out-of-band management?
   a. Management interface
   b. Service-port interface
   c. AP manager interface
   d. Virtual interface
5. How many access points are supported by a Cisco Catalyst 3750 with an integrated controller?
   a. 6
   b. 50
   c. 100
   d. 300
6. Which WLAN controller redundancy scheme uses a backup WLC configured as the tertiary WLC in the APs?
   a. N+1
   b. N+N
   c. N+N+1
   d. N+N+B

7. What is the recommended maximum number of data devices associated to a WLAN?

   a. 8

   b. 20

   c. 50

   d. 100

8. Which device of Cisco's Wireless Mesh Networking communicates with the rooftop AP?

   a. WLC

   b. WCS

   c. RAP

   d. MAP

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

Cisco has developed a strategy to address the increasing wireless demands placed on today's networks. The Cisco Unified Wireless Network (UWN) architecture combines elements of wireless and wired networks to deliver scalable, manageable, and secure WLANs. Lightweight Access Point Protocol (LWAPP) allows the placement of lightweight access points that are remotely configured and easily deployable. Cisco provides solutions for client roaming, radio frequency management, and controller designs that make wireless networks scalable. This chapter covers the Cisco UWN architecture as well as general WLAN technologies and design.

Wireless LAN Technologies

This section reviews the Institute of Electronics and Electrical Engineers (IEEE) 802.11 wireless LAN standards, wireless LAN frequencies, access methods, security, and authentication.

Wireless LAN Standards

Wireless LAN (WLAN) applications include inside-building access, LAN extension, outside building-to-building communications, public access, and small office/home office (SOHO) communications. The first standard for wireless LANs is IEEE 802.11, approved by the IEEE in 1997. The current specification is IEEE 802.11-1999, with many amendments thereafter.

IEEE 802.11 implemented wireless LANs at speeds of 1 Mbps and 2 Mbps using Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) at the physical layer of the Open System Interconnection (OSI) model. DSSS divides data into separate sections; each section travels over different frequencies at the same time. FHSS uses a frequency-hopping sequence to send data in bursts. With FHSS, some data transmits at Frequency 1, and then the system hops to Frequency 2 to send more data, and so on, returning to transmit more data at Frequency 1.

In 1999, the 802.11b amendment was introduced, providing an 11-Mbps data rate. It provides speeds of 11, 5.5, 2, and 1 Mbps and uses 11 channels of the Industrial, Scientific, and Medical (ISM) frequencies. The interoperability certification for IEEE 802.11b WLANs is wireless fidelity (Wi-Fi). The Wireless Ethernet Compatibility Alliance (WECA) governs the Wi-Fi certification. IEEE 802.11b uses DSSS and is backward-compatible with 802.11 systems that use DSSS.

The IEEE approved a second standard in 1999. IEEE 802.11a provides a maximum 54-Mbps data rate but is incompatible with 802.11b. It provides speeds of 54, 48, 36, 24, 18, 12, 9, and 6 Mbps. IEEE 802.11a uses 13 channels of the Unlicensed National Information Infrastructure (UNII) frequencies and is incompatible with 802.11b and 802.11g. IEEE 802.11a is also known as Wi-Fi5.

In 2003, the IEEE 802.11g standard was approved, providing a 54-Mbps data rate using the ISM frequencies. The advantage of 802.11g over 802.11a is that it is backward-compatible with 802.11b.

The IEEE 802.11n standard is expected to be ratified in 2007; this will provide a maximum data rate of 540 Mbps.

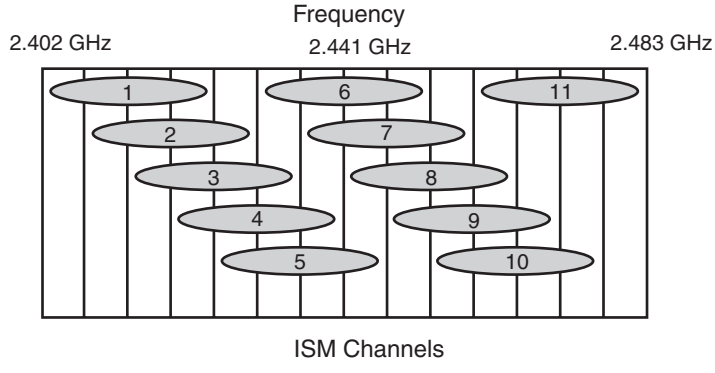
ISM and UNII Frequencies

ISM frequencies are set aside by ITU-R radio regulations 5.138 and 5.150. In the U.S., the Federal Communications Commission (15.247) specifies the ISM bands for unlicensed use. Several bands are specified in the following ranges:

- 900 to 928 MHz
- 2.4 to 2.5 GHz
- 5.75 to 5.875 GHz

Of these, channels located in the 2.4-GHz range are used for 802.11b and 802.11g. As shown in Figure 4-1, 11 overlapping channels are available for use. Each channel is 22 MHz wide. It is common to use channels 1, 6, and 11 in the same areas, because these three channels do not overlap.

Figure 4-1 *ISM 2.4 Channels*



The UNII radio bands were specified for use with 802.11a wireless. UNII operates over three ranges:

- UNII 1—5.15 to 5.25 GHz and 5.25 to 5.35 GHz.
- UNII 2—5.47 to 5.725 GHz. This range is used by High Performance Radio LAN (HiperLAN) in Europe.
- UNII 3—5.725 to 5.875 GHz. This range overlaps with ISM.

UNII provides 12 nonoverlapping channels for 802.11a.

Summary of Wireless LAN Standards

Table 4-2 summarizes WLAN standards, frequencies, and data rates.

Table 4-2 *WLAN Standards Summary*

IEEE Protocol	Standard Release Date	Frequency	Typical Data Rate	Maximum Data Rate
Legacy	1997	ISM	1 Mbps	2 Mbps
802.11a	1999	UNII	25 Mbps	54 Mbps
802.11b	1999	ISM	6.5 Mbps	11 Mbps
802.11g	2003	ISM	25 Mbps	54 Mbps
802.11n	2007 (draft)	ISM or UNII	200 Mbps	540 Mbps

Service Set Identifier (SSID)

WLANs use an SSID to identify the WLAN's "network name." The SSID can be 2 to 32 characters long. All devices in the WLAN must have the same configured SSID to communicate. It is similar to a VLAN identifier in a wired network. The difficulty in large networks is configuring the SSID, frequency, and power settings for hundreds of remotely located access points. Cisco addresses this problem with the Cisco Wireless Control System (WCS). WCS is covered in more detail in the "Cisco UWN Architecture" section.

WLAN Layer 2 Access Method

The IEEE 802.11 Media Access Control (MAC) layer implements carrier sense multiple access collision avoidance (CSMA/CA) as an access method. With CSMA/CA, each WLAN station listens to see whether a station is transmitting. If no activity is occurring, the station transmits. If activity is occurring, the station uses a random countdown timer. When the timer expires, the station transmits.

WLAN Security

WLANs provide an effective solution for hard-to-reach locations and enable mobility to a level that was previously unattainable. However, WLANs without any encryption present a security risk, because publicly available software can obtain the SSIDs. The productivity improvements with WLANs are just beginning, however. The Wired Equivalent Privacy (WEP) security protocol, used in the IEEE 802.11b standard, is considered faulty and vulnerable to numerous attacks. The 802.11b protocol is the most commonly deployed wireless protocol, and although it has the ability to use 64-bit or 128-bit encryption, readily available software can crack the encryption scheme.

In June 2004, the IEEE 802.11i standard was ratified to provide additional security in WLAN networks. IEEE 802.11i is also known as Wi-Fi Protected Access 2 (WPA2). The 802.11i architecture contains the following components:

- 802.1X for authentication (entailing the use of Extensible Authentication Protocol [EAP] and an authentication server)
- Robust Security Network (RSN) for keeping track of associations
- Advanced Encryption Standard (AES) for confidentiality, integrity, and origin authentication

Unauthorized Access

A problem that confronts WLANs comes from the fact that wireless signals are not easily controlled or contained. WEP works at the data link layer, sharing the same key for all nodes that communicate. The 802.11 standard was deployed because it allowed bandwidth speed up to 11 Mbps and it is based on DSSS technology. DSSS also enables APs to identify WLAN cards via their MAC addresses. Because traditional physical boundaries do not apply to wireless networks, attackers can gain access using wireless from outside the physical security perimeter. Attackers achieve unauthorized access if the wireless network does not have a mechanism to compare a MAC address on a wireless card to a database that contains a directory with access rights. An individual can roam within an area, and each AP that comes into contact with that card must also rely on a directory. Statically allowing access via a MAC address is also insecure, because MAC addresses can be spoofed.

Some APs can implement MAC address and protocol filtering to enhance security or limit the protocols used over the WLAN. With hundreds of WLAN clients, MAC address filtering is not a scalable solution. Again, attackers can hack MAC address filtering. A user can listen for transmissions, gather a list of MAC addresses, and then use one of those MAC addresses to connect to the AP.

WLAN Security Design Approach

The WLAN security design approach makes two assumptions, which this chapter describes. The assumptions are that all WLAN devices are connected to a unique IP subnet and that most services available to the wired network are also available to the wireless nodes. Using these two assumptions, the WLAN security designs offer two basic security approaches:

- Use of Lightweight Extensible Authentication Protocol (LEAP) to secure authentication
- Use of virtual private networks (VPN) with IP Security (IPsec) to secure traffic from the WLAN to the wired network

Considering WLAN as an alternative access methodology, remember that the services these WLAN users access are often the same as those accessed by the wired users. WLAN opens a new world of access for the hacker, and you should consider the risks before deployment.

To enhance security, you can implement WLANs with IPsec VPN software, use the IEEE 802.1X-2001 port-based access control protocol, and use dynamic WEP keys.

IEEE 802.1X-2001 Port-Based Authentication

IEEE 802.1X-2001 is a port-based authentication standard for LANs. It authenticates a user before allowing access to the network. You can use it on Ethernet, Fast Ethernet, and WLAN networks.

With IEEE 802.1X-2001, client workstations run client software to request access to services. Clients use EAP to communicate with the LAN switch. The LAN switch verifies client information with the authentication server and relays the response to the client. LAN switches use a Remote Authentication Dial-In User Service (RADIUS) client to communicate with the server. The RADIUS authentication server validates the client's identity and authorizes the client. The server uses RADIUS with EAP extensions to make the authorization.

Dynamic WEP Keys and LEAP

Cisco also offers dynamic per-user, per-session WEP keys to provide additional security over statically configured WEP keys, which are not unique per user. For centralized user-based authentication, Cisco developed LEAP. LEAP uses mutual authentication between the client and the network server and uses IEEE 802.1X for 802.11 authentication messaging. LEAP uses a RADIUS server to manage user information.

LEAP is a combination of 802.1X and EAP. It combines the capability to authenticate to various servers such as RADIUS with forcing the WLAN user to log in to an access point that compares the login information to RADIUS. This solution is more scalable than MAC address filtering.

Because the WLAN access depends on receiving an address, using Dynamic Host Configuration Protocol (DHCP), and the authentication of the user using RADIUS, the WLAN needs constant access to these back-end servers. In addition, LEAP does not support one-time passwords (OTP), so you must use good password-security practices. The password issue and maintenance practice are a basic component of corporate security policy.

Controlling WLAN Access to Servers

In the same way you place Domain Name System (DNS) servers accessible via the Internet on a demilitarized zone (DMZ) segment, you should apply a similar strategy to the RADIUS and DHCP servers accessible to the WLAN. These servers should be secondary servers that are on a different segment (separate VLAN) from their primary counterparts. Access to this VLAN is

filtered. Such placement ensures that any attacks launched on these servers are contained within that segment.

You should control network access to the servers. Consider the WLAN an unsecured segment and apply appropriate segmentation and access lists. Such a step ensures that WLAN access is controlled and directed to only those areas that need it. For example, you might not want to permit WLAN access to management servers and HR servers.

You must also protect these servers against network attack. The criticality of these servers makes them an ideal target for denial-of-service (DoS) attacks. Consider using host-based intrusion detection systems (IDS) to detect network attacks against these devices.

Cisco Unified Wireless Network

This section covers the Cisco UWN architecture, LWAPP, WLAN controller components, roaming, and mobility groups. Cisco UWN components provide scalable wireless LAN solutions using WLAN controllers to manage lightweight access points. The CCDA must understand how these components work with each other, how they scale, and how roaming and mobility groups work.

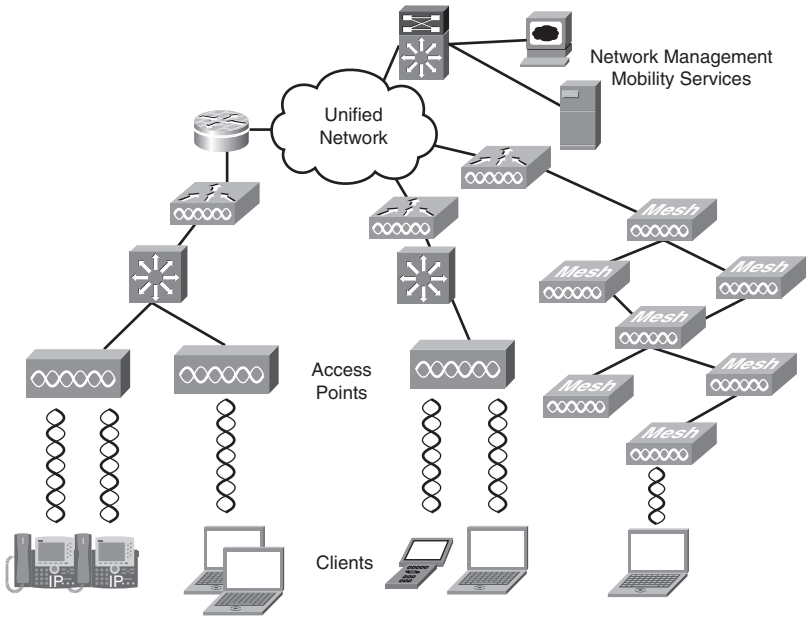
Cisco UWN Architecture

With the explosion of wireless solutions in and out of the enterprise, designers must create solutions that provide mobility and business services while maintaining network security. The Cisco Unified Wireless Network (UWN) architecture combines elements of wireless and wired networks to deliver scalable, manageable, and secure WLANs. As shown in Figure 4-2, the Cisco UWN architecture is composed of five network elements:

- **Client devices**—These include laptops, workstations, IP phones, PDAs, and manufacturing devices to access the WLAN.
- **Access points**—These devices provide access to the wireless network. APs are placed in strategic locations to minimize interference.
- **Network unification**—The WLAN system should be able to support wireless applications by providing security policies, QoS, intrusion prevention, and radio frequency (RF) management. Cisco WLAN controllers provide this functionality and integration into all major switching and routing platforms.
- **Network management**—The Cisco Wireless Control System (WCS) provides a central management tool that lets you design, control, and monitor wireless networks.

- **Mobility services**—These include guest access, location services, voice services, and threat detection and mitigation.

Figure 4-2 *Cisco UWN Architecture*



Cisco UWN provides the following benefits:

- Reduced Total Cost of Ownership (TCO)
- Enhanced visibility control
- Dynamic RF management
- WLAN security
- Unified wired and wireless network
- Enterprise mobility
- Enhanced productivity and collaboration

LWAPP

Lightweight Access Point Protocol (LWAPP) is a draft Internet Engineering Task Force (IETF) standard for control messaging for setup, authentication, and operations between access points (AP) and wireless LAN controllers (WLC).

With Cisco's UWN Split-MAC operation, the control and data messages are split. Lightweight Access Points (LWAP) communicate with the WLCs using control messages over the wired network. LWAPP data messages are encapsulated and forwarded to and from wireless clients. The WLC manages multiple APs, providing configuration information and firmware updates as needed.

LWAP MAC functions are

- **802.11**—Beacons, probe response
- **802.11 Control**—Packet acknowledgment and transmission
- **802.11e**—Frame queuing and packet prioritization
- **802.11i**—MAC layer data encryption/decryption

Controller MAC functions are

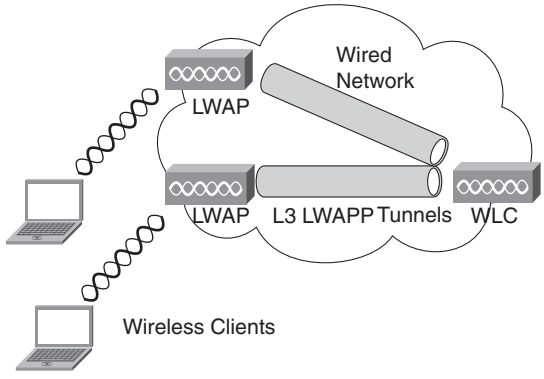
- **802.11 MAC Management**—Association requests and actions
- **802.11e Resource Reservation**—To reserve resources for specific applications
- **802.11i**—Authentication and key management

In the LWAPP RFC draft, LWAPP control messages can be transported at Layer 2 tunnels or Layer 3 tunnels. Layer 2 LWAPP tunnels were the first method developed in which the APs did not require an IP address. The disadvantage of Layer 2 LWAPP was that the WLC needed to be on every subnet on which the AP resides. Layer 2 LWAPP is a deprecated solution for Cisco. Layer 3 LWAPP is the preferred solution.

NOTE Layer 2 LWAPP tunnels use Ethertype code 0xBBBB.

As shown in Figure 4-3, Layer 3 LWAPP tunnels are used between the LWAP and the WLC. Messages from the WLC use UDP port 12223 for control and UDP port 12222 for data messages. In this solution, access points require an IP address, but the WLC does not need to reside on the same segment.

Figure 4-3 *Layer 3 LWAPP*



LWAPP Access Point Modes

LWAPP access points operate in one of six different modes:

- **Local mode**—This is the default mode of operation. In this mode, every 180 seconds the AP spends 60 milliseconds on channels it does not operate on. During this 60 ms, the AP performs noise floor measurements, measures interference, and scans for IDS events.
- **Remote Edge AP (REAP) mode**—This mode enables an LWAP to reside across a WAN link and still be able to communicate with the WLC and provide the functionality of a regular LWAP. Currently, REAP mode is supported only on the 1030 LWAPs.
- **Monitor mode**—Monitor mode is a feature designed to allow specified LWAPP-enabled APs to exclude themselves from handling data traffic between clients and the infrastructure. They instead act as dedicated sensors for location-based services (LBS), rogue access point detection, and intrusion detection (IDS). When APs are in Monitor mode, they cannot serve clients and continuously cycle through all configured channels, listening to each channel for approximately 60 ms.
- **Rogue detector mode**—LWAPs that operate in Rogue Detector mode monitor the rogue APs. They do not transmit or contain rogue APs. The idea is that the rogue detector (RD) should be able to see all the VLANs in the network, because rogue APs can be connected to any of the VLANs in the network (thus, we connect it to a trunk port). The switch sends all the rogue AP/client MAC address lists to the RD. The RD then forwards those to the WLC to compare with the MAC addresses of clients that the WLC APs have heard over the air. If the MAC addresses match, the WLC knows that the rogue AP to which those clients are connected is on the wired network.

- **Sniffer mode**—An LWAPP that operates in Sniffer mode functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information on the time stamp, signal strength, packet size, and so on. The Sniffer feature can be enabled only if you run AiroPeek, a third-party network analyzer software that supports decoding of data packets.
- **Bridge mode**—The Bridge mode feature on the Cisco 1030 (typically indoor usage) and 1500 access points (typically outdoor mesh usage) provides cost-effective, high-bandwidth wireless bridging connectivity. Applications supported are point-to-point bridging, point-to-multipoint bridging, point-to-point wireless access with integrated wireless backhaul, and point-to-multipoint wireless access with integrated wireless backhaul.

LWAPP Discovery

When LWAPs are placed on the network, they first perform DHCP discovery to obtain an IP address. Then Layer 3 LWAPP discovery is attempted. If there is no WLC response, the access point reboots and repeats this process. The Layer 3 LWAPP discovery algorithm is as follows:

1. The AP sends a Layer 3 LWAPP Discovery Request.
2. All WLCs that receive the Discovery Request reply with a unicast LWAPP Discovery Response Message.
3. The AP compiles a list of WLCs.
4. The AP selects a WLC based on certain criteria.
5. The AP validates the selected WLC and sends an LWAPP Join Response. An encryption key is selected, and future messages are encrypted.

Layer 3 Discovery Requests are sent as listed:

- Local subnet broadcast
- Unicast LWAPP Discovery Requests to WLC IP addresses advertised by other APs
- To previously stored WLC IP addresses
- To IP addresses learned by DHCP option 43
- To IP addresses learned by DNS resolution of CISCO-LWAPP-CONTROLLER.locadomain

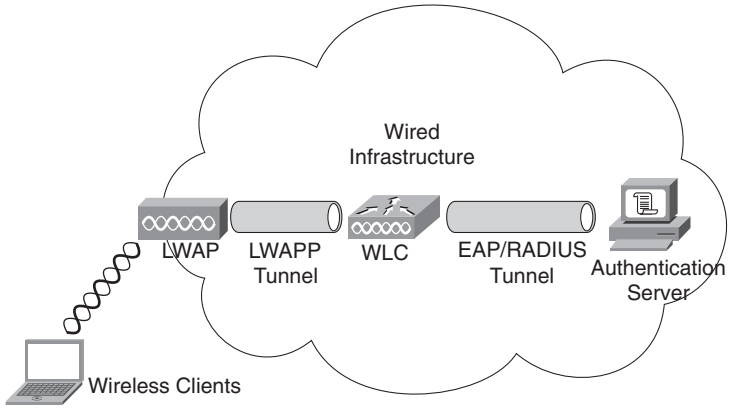
The selected WLC is based on the following:

- Previously configured primary, secondary, and/or tertiary WLCs
- The WLC configured as the Master controller
- The WLC with the most capacity for AP associations

WLAN Authentication

Wireless clients first associate to an access point. Then wireless clients need to authenticate with an authentication server before the access point allows access to services. As shown in Figure 4-4, the authentication server resides in the wired infrastructure. An EAP/RADIUS tunnel occurs between the WLC and the authentication server. Cisco's Secure Access Control Server (ACS) using EAP is an example of an authentication server.

Figure 4-4 *WLAN Authentication*



Authentication Options

Wireless clients communicate with the authentication server using EAP. Each EAP type has advantages and disadvantages. Trade-offs exist between the security provided, EAP type manageability, the operating systems supported, the client devices supported, the client software and authentication messaging overhead, certificate requirements, user ease of use, and WLAN infrastructure device support. The following summarizes the authentication options:

- **EAP-Transport Layer Security (EAP-TLS)** is an IETF open standard that is well-supported among wireless vendors but rarely deployed. It uses PKI to secure communications to the RADIUS authentication server using TLS and digital certificates.

- **Protected Extensible Authentication Protocol (PEAP)** is a joint proposal by Cisco Systems, Microsoft, and RSA Security as an open standard. PEAP/MSCHAPv2 is the most common version, and it is widely available in products and widely deployed. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication. PEAP-GTC allows more generic authentication to a number of databases such as Novell Directory Services (NDS).

- **EAP-Tunneled TLS (EAP-TTLS)** was codeveloped by Funk Software and Certicom. It is widely supported across platforms and offers very good security, using PKI certificates only on the authentication server.
- **Cisco Lightweight Extensible Authentication Protocol (LEAP)** is an early proprietary EAP method supported in the Cisco Certified Extensions (CCX) program. It is vulnerable to dictionary attacks.
- **EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)** is a proposal by Cisco Systems to fix the weaknesses of LEAP. EAP-FAST uses a Protected Access Credential (PAC), and use of server certificates is optional. EAP-FAST has three phases. Phase 0 is an optional phase in which the PAC can be provisioned manually or dynamically. In Phase 1, the client and the AAA server use the PAC to establish the TLS tunnel. In Phase 2, the client sends user information across the tunnel.

WLAN Controller Components

The CCDA candidate must understand the three major components of WLCs:

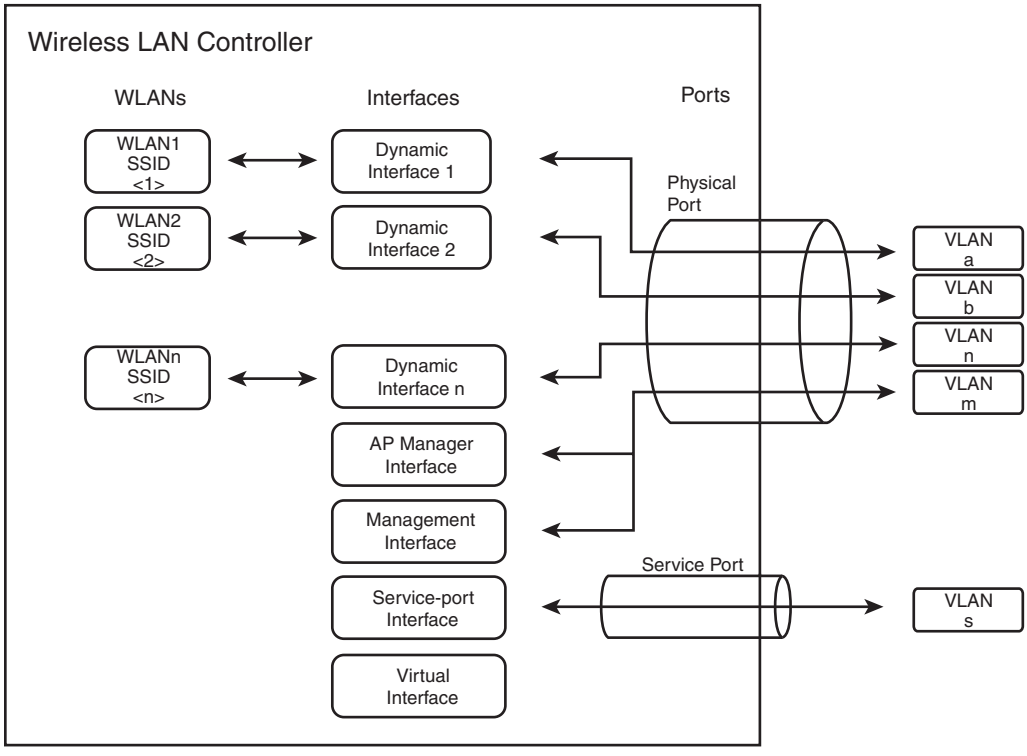
- Wireless LANs
- Interfaces
- Ports

Wireless LANs are identified by unique SSID network names. The LAN is a logical entity. Each WLAN is assigned to an interface in the WLC. Each WLAN is configured with radio policies, QoS, and other WLAN parameters.

A WLC interface is a logical connection that maps to a VLAN on the wired network. Each interface is configured with a unique IP address, default gateways, physical ports, VLAN tag, and DHCP server.

The port is a physical connection to the neighboring switch or router. By default, each port is an IEEE 802.1Q trunk port. There may be multiple ports on a WLC into a single port-channel interface. These ports can be aggregated using Link Aggregation (LAG). Some WLCs have a service port that is used for out-of-band management. Figure 4-5 shows the WLC components.

Figure 4-5 *WLAN Controller Components*



WLC Interface Types

A WLC has five interface types:

- **Management interface** is used for in-band management, connectivity to AAA, and Layer 2 discovery and association.
- **Service-port interface** is used for out-of-band management. It is an optional interface that is statically configured.
- **AP manager interface** is used for Layer 3 discovery and association. It has the source IP address of the AP that is statically configured.
- **Dynamic interface** is analogous to VLANs and is designated for WLAN client data.
- **Virtual interface** is used for Layer 3 security authentication, DHCP relay support, and mobility management.

AP Controller Equipment Scaling

Cisco provides different solutions to support the differing numbers of access points present in enterprise customers. Standalone devices, modules for integrated services routers (ISR), and modules for 6500 switches support numerous APs. Table 4-3 lists the platforms and the number of APs supported.

Table 4-3 *WLAN Controller Platforms*

Platform	Number of Supported Access Points
Cisco 2000 series WLC	6
Cisco WLC for ISRs	6
Catalyst 3750 Integrated WLC	50
Cisco 4400 series WLC	100
Cisco 6500 series WLC Module	300

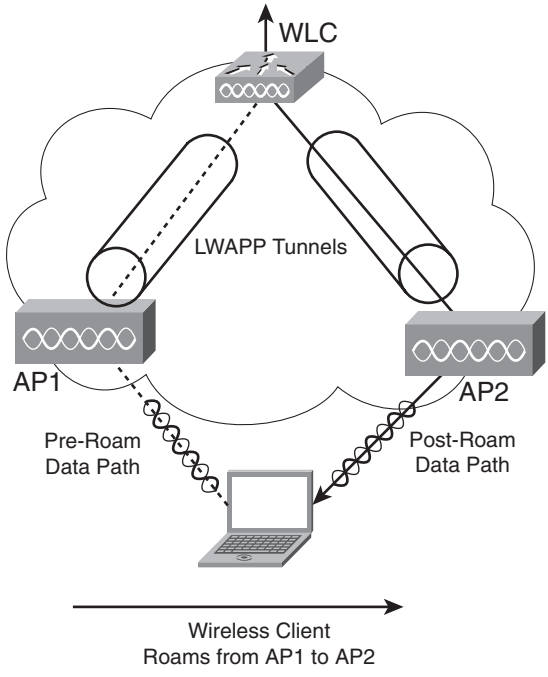
Roaming and Mobility Groups

The primary reason to have wireless networks is the ability to access network resources from common areas and in areas difficult to run cables. End clients might want to move from one location to another. Mobility allows users to access the network from several locations. Roaming occurs when the wireless client changes association from one access point to another. The challenge is to scale the wireless network to allow client roaming. Roaming can be intracontroller or intercontroller.

Intracontroller Roaming

Intracontroller roaming, shown in Figure 4-6, occurs when a client moves association from one AP to another AP that is joined to the same WLC. The WLC updates the client database with the new associated AP and does not change the client's IP address. If required, clients are reauthenticated, and a new security association is established. The client database remains on the same WLC.

Figure 4-6 *Intracontroller Roaming*



Layer 2 Intercontroller Roaming

Intercontroller roaming occurs when a client moves association from one AP to another AP that is joined to a different WLC. The Layer 2 roam occurs when the client traffic is bridged to the same IP subnet. Figure 4-7 shows Layer 2 intercontroller roaming. Traffic remains of the same IP subnet, and no IP address changes to the client occur. The client database is moved from WLC1 to WLC2. The client is reauthenticated, and a new security session is established.

Layer 3 Intercontroller Roaming

With Layer 3 intercontroller roaming, shown in Figure 4-8, a client moves association from one AP to another AP that is joined to a different WLC. Then the traffic is bridged onto a different IP subnet. When the client associates to AP2, WLC2 then exchanges mobility messages with WLC1. The original client database is not moved to WLC. Instead, WLC1 marks the client with an "Anchor" entry in its database. The database entry is copied to WLC2's database and is marked as a "Foreign" entry. The wireless client maintains its original IP address and is reauthenticated. A new security session is then established.

Figure 4-7 *Layer 2 Intercontroller Roaming*

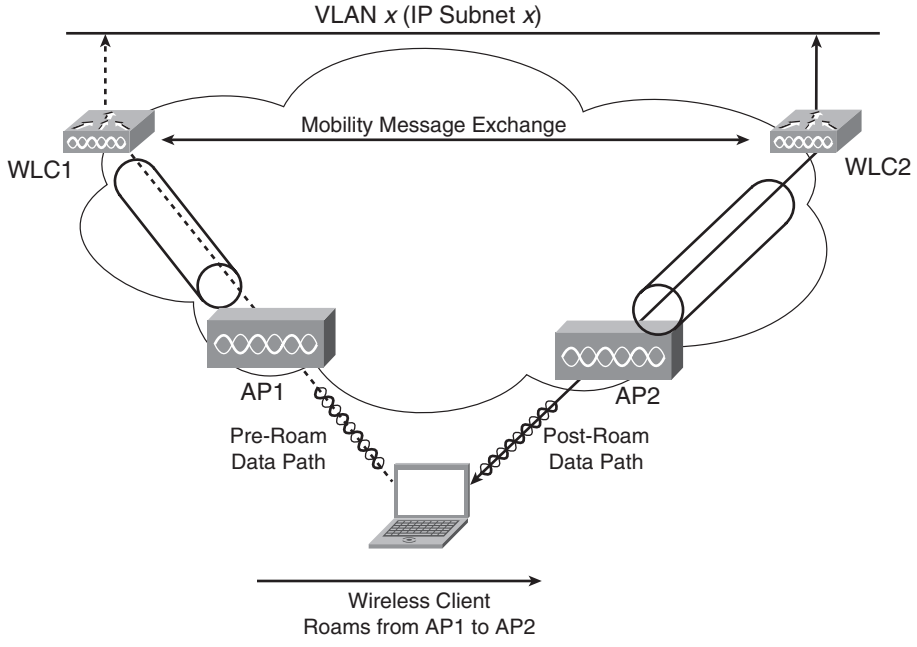
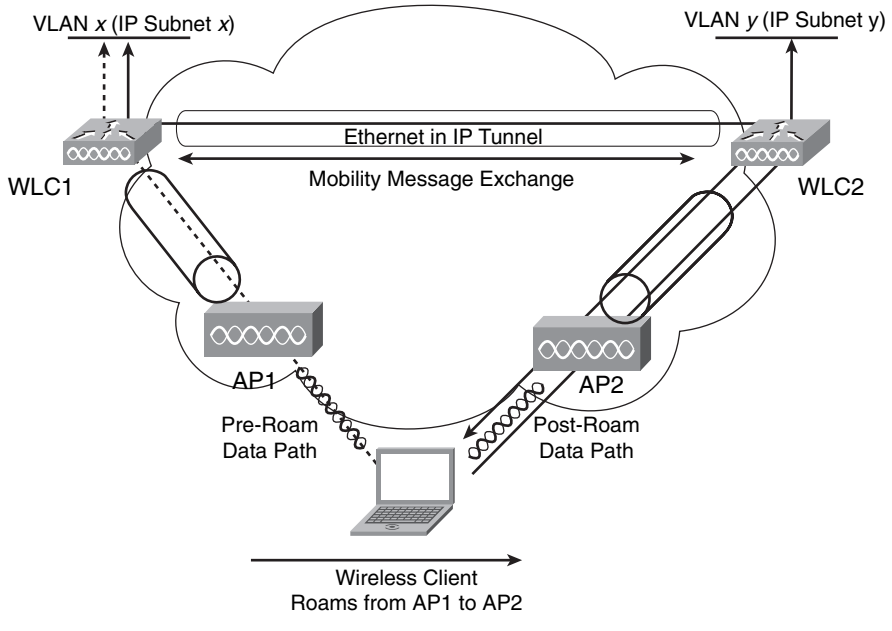


Figure 4-8 *Layer 3 Intercontroller Roaming*



Client traffic then routes in an asymmetric manner. Traffic from the client is forwarded by the Foreign WLC, but traffic to the client arrives at the Anchor WLC, which forwards it through an Ethernet-in-IP (EtherIP) tunnel to the Foreign WLC. The Foreign WLC forwards the data traffic to the client.

Mobility Groups

When you assign WLCs to mobility groups, the WLCs dynamically exchange mobility messages and tunnel data via EtherIP. Mobility groups support up to 24 controllers. The upper limit of APs is bounded by the controller types and the number of APs supported by each controller. Each WLC is configured with a list of the members in the mobility group. The WLCs exchange messages using UDP port 16666 for unencrypted messages or UDP port 16667 for encrypted messages. As an example of the scalability, if 24 Cisco 2000 WLCs are used, 24 * 6 = 144 APs are supported.

Cisco recommends minimizing intercontroller roaming in the network. It is also recommended that there be less than 10 ms of round-trip time latency between controllers. Cisco also states that Layer 2 roaming is more efficient than Layer 3 roaming because of the asymmetric communication of Layer 3 roaming.

Wireless LAN Design

This section covers controller redundancy design, radio frequency groups, site survey, and wireless LAN design considerations.

Controller Redundancy Design

WLCs can be configured for dynamic or deterministic redundancy. For deterministic redundancy, the access point is configured with a primary, secondary, and tertiary controller. This requires more upfront planning but allows better predictability and faster failover times. Deterministic redundancy is the recommended best practice. N+1, N+N, and N+N+1 are examples of deterministic redundancy.

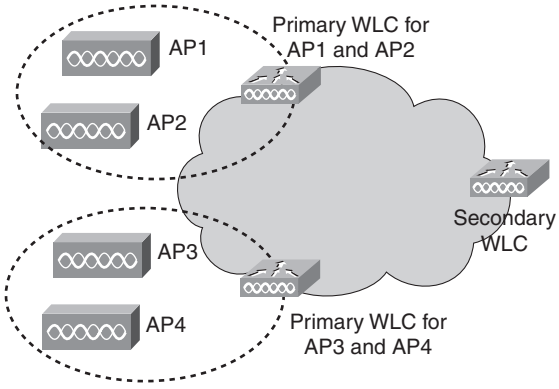
Dynamic controller redundancy uses LWAPP to load-balance APs across WLCs. LWAPP populates APs with a backup WLC. This solution works better when WLCs are in a centralized cluster. This solution is easier to deploy than the deterministic solution and allows APs to load-balance. The disadvantages are longer failover times and unpredictable operation. An example is adjacent APs registering with differing WLCs.

N+1 WLC Redundancy

With N+1 redundancy, shown in Figure 4-9, a single WLC acts as the backup of multiple WLCs. The backup WLC is configured as the secondary WLC on each AP. One design constraint is that

the backup WLC may become oversubscribed if there are too many failures of the primary controllers. The secondary WLC is the backup controller for all APs.

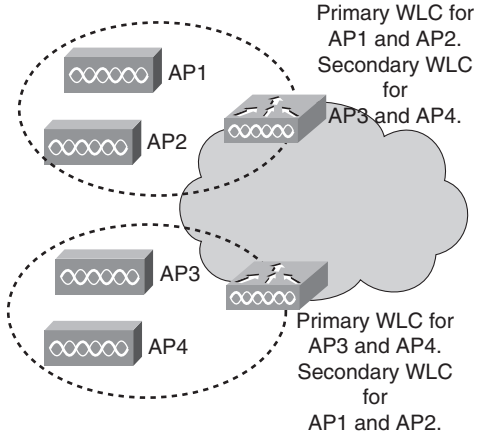
Figure 4-9 *N+1 Controller Redundancy*



N+N WLC Redundancy

With N+N redundancy, shown in Figure 4-10, an equal number of controllers back up each other. For example, a pair of WLCs on one floor serves as a backup to a second pair on another floor. The top WLC is primary for AP1 and AP2 and secondary for AP3 and AP4. The bottom WLC is primary for AP3 and AP4 and secondary for AP1 and AP2.

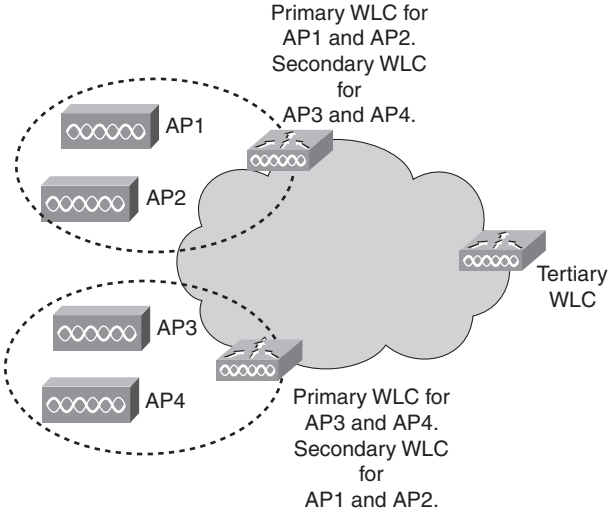
Figure 4-10 *N+N Controller Redundancy*



N+N+1 WLC Redundancy

With N+N+1 redundancy, shown in Figure 4-11, an equal number of controllers back up each other (as with N+N), plus a backup WLC is configured as the tertiary WLC for the access points. N+N+1 redundancy functions the same as N+N redundancy plus a tertiary controller that backs up the secondary controllers.

Figure 4-11 *N+N+1 Controller Redundancy*



Radio Management and Radio Groups

The limit of available channels in the ISM frequencies used by the IEEE 802.11b/g standard presents challenges to the network designer. There are three nonoverlapping channels (channels 1, 6, and 11). The recommended best practice per AP is up to 20 data devices, or no more than seven concurrent voice over WLAN (VoWLAN) calls using g.711 or eight concurrent VoWLAN calls using g.729. Additional APs should be added as user population grows to maintain this ratio of data and voice per AP.

Cisco Radio Resource Management (RRM) is a method to manage AP radio frequency channel and power configuration. Cisco WLCs use the RRM algorithm to automatically configure, optimize, and self-heal. Cisco RRM functions are as follows:

- **Radio resource monitoring**—Cisco LWAPs monitor all channels. Collected packets are sent to the WLC, which can detect rouge APs, clients, and interfering APs.
- **Dynamic channel assignment**—WLCs automatically assign channels to avoid interference.

- **Interference detection and avoidance**—As Cisco LWAPs monitor all channels, interference is detected by a predefined threshold (10 percent by default). Interference can be generated by rouge APs, Bluetooth devices, or neighboring WLANs.
- **Dynamic transmit power control**—The WLCs automatically adjust power levels.
- **Coverage hole detection and correction**—WLCs may adjust the power output of APs if clients report that a low Received Signal Strength Indication (RSSI) level is detected.
- **Client and network load balancing**—Clients can be influenced to associate with certain APs to maintain network balance.

Radio Frequency (RF) Groups

An RF group is a cluster of WLC devices that coordinate their RRM calculations. When the WLCs are placed in an RF group, the RRM calculation can scale from a single WLC to multiple floors, buildings, or even the campus. With an RF group, APs send neighbor messages to other APs. If the neighbor message is above –80 dBm, the controllers form an RF group. The WLCs elect an RF group leader to analyze the RF data. The RF group leader exchanges messages with the RF group members using UDP port 12114 for 802.11b/g and UDP port 12115 for 802.11a.

RF Site Survey

Similar to performing an assessment for a wired network design, RF site surveys are done to determine design parameters for wireless LANs and customer requirements. RF site surveys help determine the coverage areas and check for RF interference. This helps determine the appropriate placement of wireless APs.

The RF site survey has the following steps:

Step 1 **Define customer requirements**, such as service levels and support for VoIP.

Step 2 **Identify coverage areas and user density**, including peak use times and conference room locations.

Step 3 **Determine preliminary AP locations**, which need power, wired network access, mounting locations, and antennas.

Step 4 **Perform the actual survey** by using an AP to survey the location and received RF strength based on the targeted AP placement. Consider the effects of electrical machinery. Microwave ovens and elevators may distort the ration signal from the APs.

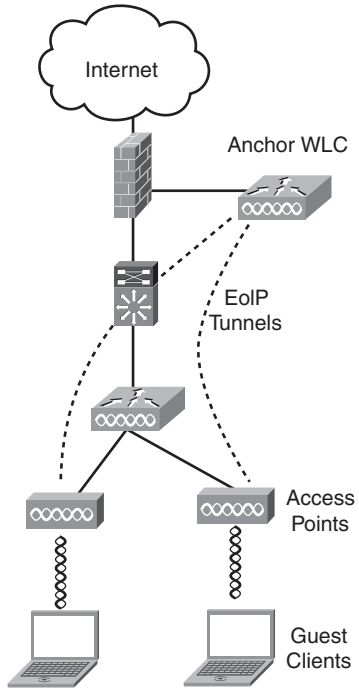
Step 5 **Document the findings** by recording the target AP locations, data rates, and signal readings.

Using EoIP Tunnels for Guest Services

Basic solutions use separate VLANs for guest and corporate users to segregate guest traffic from corporate traffic. The guest SSID is broadcast, but the corporate SSID is not. All other security parameters are configured. Another solution is to use Ethernet over IP (EoIP) to tunnel the guest traffic from the LWAPP to an anchor WLC.

As shown in Figure 4-12, EoIP is used to logically segment and transport guest traffic from the edge AP to the anchor WLC. There is no need to define guest VLANs in the internal network, and corporate traffic is still locally bridged. The Ethernet frames from the guest clients are maintained across the LWAPP and EoIP tunnels.

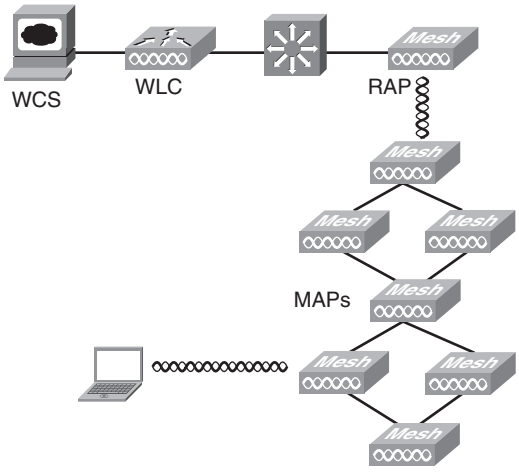
Figure 4-12 *EoIP Tunnels*



Wireless Mesh for Outdoor Wireless

Traditionally, outdoor wireless solutions have been limited to point-to-point and point-to-multipoint bridging between buildings. With these solutions, each AP is wired to the network. The Cisco Wireless Mesh networking solution, shown in Figure 4-13, eliminates the need to wire each AP and allows users to roam from one area to another without having to reconnect.

Figure 4-13 *Wireless Mesh Components*



The wireless mesh components are as follows:

- **Wireless Control System (WCS)** is the wireless mesh SNMP management system that allows network-wide configuration and management.
- **Wireless LAN Controller (WLC)** links the mesh APs to the wired network and performs all the tasks previously described for a WLC.
- **Rooftop AP (RAP)** connects the mesh to the wired network and serves as the root (or gateway). It also communicates with the MAPs.
- **Mesh Access Points (MAP)** are remote APs. They communicate with the RAP to connect to the wired network.

Mesh Design Recommendations

The following are Cisco recommendations (and considerations) for mesh design:

- There is a 2- to 3-ms typical latency per hop.
- For outdoor deployment, four or fewer hops are recommended for best performance. A maximum of eight hops is supported.
- For indoor deployment, one hop is supported.
- 20 MAP nodes per RAP are recommended for best performance. Up to 32 MAPs are supported.

Campus Design Considerations

When designing for the Cisco Unified Wireless Network, you need to be able to determine how many LWAPs to place and how they will be managed with the WLCs. Table 4-4 summarizes campus design considerations.

Table 4-4 *WLAN Design Considerations*

Design Item	Description
Number of APs	The design should have enough APs to provide full RF coverage for wireless clients for all the expected locations in the enterprise. Cisco recommends 20 data devices per AP and 7 g.711 concurrent or 8 g.729 concurrent VoWLAN calls.
Placement of APs	APs are placed in a centralized location of the expected area for which they are to provide access. APs are placed in conference rooms to accommodate peak requirements.
Power for APs	Traditional wall power can be used, but the preferred solution is to use power over Ethernet (PoE) to power APs and provide wired access.
Number of WLCs	The number of WLCs depends on the selected redundancy model based on the client's requirements. The number of controllers is also dependent on the number of required APs and the number of APs supported by the differing WLC models.
Placement of WLCs	WLCs are placed on secured wiring closets or in the data center. Deterministic redundancy is recommended, and intercontroller roaming should be minimized. WLCs can be placed in a central location or distributed in the campus distribution layer.

Table 4-5 summarizes AP features for Cisco APs.

Table 4-5 *Supported Features and Specifications for Cisco APs*

Feature	10x0 Series	1121 Series	1130 Series	1230 Series	1240 Series	1300 Series	1500 Series
Autonomous/LWAPP	LWAPP	Both	Both	Both	Both	Both	LWAPP
External antenna	Yes	No	No	Yes	Yes	Yes	Yes
Outdoor install	No	No	No	No	No	Yes	Yes
REAP/Hybrid REAP (H-REAP)	REAP	No	H-REAP	No	H-REAP	No	Yes
Dual radio	Yes	No (only 11b/g)	Yes	Yes	Yes	No (only 11b/g)	Yes

Table 4-5 *Supported Features and Specifications for Cisco APs (Continued)*

Feature	10x0 Series	1121 Series	1130 Series	1230 Series	1240 Series	1300 Series	1500 Series
Power (watts)	13	6	15	14	15	—	—
Memory (Mb)	16	16	32	16	32	16	16
WLANs supported	16	8	8	8	8	8	16

Branch Design Considerations

For branch networks you need to consider the number and placement of APs, which depends on the location and expected number of wireless clients at the branch office. It may not be cost-justifiable to place a WLC at each branch office of an enterprise. One requirement is that the round-trip time (RTT) between the AP and the WLC should not exceed 100 ms. For centralized controllers, it is recommended that you use REAP or Hybrid REAP (H-REAP).

Local MAC

LWAPP supports local media access control (local MAC), which can be used in branch deployments. Unlike with split-MAC, the AP provides MAC management support for association requests and actions. Local MAC terminates client traffic at the wired port of the access point versus at the WLC. This allows direct local access to branch resources without requiring the data to travel to the WLC at the main office. Local MAC also allows the wireless client to function even if a WAN link failure occurs.

REAP

REAP is designed to support remote offices by extending LWAPP control timers. It is the preferred solution for LWAPs to connect to the WLC over the WAN. With REAP control, traffic is still encapsulated over a LWAPP tunnel and is sent to the WLC. Management control and RF management are done over the WAN. Client data is locally bridged. With REAP, local clients still have local connectivity if the WAN fails.

WLCs support the same number of REAP devices as APs. REAP devices support only Layer 2 security policies, do not support NAT, and require a routable IP address.

Hybrid REAP

H-REAP is an enhancement to REAP that provides additional capabilities such as NAT, more security options, and the ability to control up to three APs remotely.

H-REAP operates in two security modes:

- **Standalone mode**—H-REAP does the client authentication itself when the WLC cannot be reached.
- **Connected mode**—The device uses the WLC for client authentication.

H-REAP is more delay-sensitive than REAP. The RTT must not exceed 100 ms between the AP and the WLC.

Branch Office Controller Options

For branch offices, Cisco recommends one of four options:

- **Cisco 2006**—Supports six APs.
- **Cisco 4402-12 and 4402-25**—These devices support 12 and 25 APs, respectively.
- **WLC Module in Integrated Services Router (ISR)**—Supports six APs.
- **3750 with WLAN controller**—Depending on the model, this can support 25 or 50 APs.

References and Recommended Readings

Cisco Outdoor Wireless Network Solution, http://www.cisco.com/en/US/netsol/ns621/networking_solutions_package.html

Cisco Unified Wireless Network, http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

Cisco Wireless Control System, http://www.cisco.com/en/US/products/ps6305/index.html

"Enterprise Mobility 3.0 Design Guide," http://www.cisco.com/univercd/cc/td/doc/solution/emblty30.pdf

IEEE Std 802.11g-2003. Amendment to IEEE Std 802.11, 1999 Edition.

Lightweight Access Point FAQ, http://www.cisco.com/en/US/products/ps6306/products_qanda_item09186a00806a4da3.shtml

"Light Weight Access Point Protocol (LWAPP), (draft-ohara-capwap-lwapp-02)," http://tools.ietf.org/html/draft-ohara-capwap-lwapp-02

"Wireless LAN MAC and Physical Layer (PHY) Specifications," IEEE 802.11-1999. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, 1999.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

Table 4-6 summarizes WLAN standards.

Table 4-6 *WLAN Standards*

IEEE Protocol	Standard Release Date	Frequency	Typical Data Rate	Maximum Data Rate
Legacy	1997	ISM	1 Mbps	2 Mbps
802.11a	1999	UNII	25 Mbps	54 Mbps
802.11b	1999	ISM	6.5 Mbps	11 Mbps
802.11g	2003	ISM	25 Mbps	54 Mbps
802.11n	2007 (draft)	ISM or UNII	200 Mbps	540 Mbps

Table 4-7 summarizes the elements of the Cisco UWN architecture.

Table 4-7 *Cisco UWN Architecture*

Cisco UWN Element	Description
Client devices	These include laptops, workstations, IP phones, PDAs, and manufacturing devices to access the WLAN.
Access points	Provide access to the network.
Network unification	The WLAN system should be able to support wireless applications by providing security policies, QoS, intrusion prevention, RF management, and wireless controllers.
Network management	Cisco Wireless Control System (WCS) provides a central management tool that lets you design, control, and monitor wireless networks.
Mobility services	Include guest access, location services, voice services, and threat detection and mitigation.

Table 4-8 summarizes the LWAPP AP operation modes.

Table 4-8 *LWAPP Access Point Modes*

LWAPP Mode	Description
Local mode	The default mode of operation.
REAP mode	For remote LWAP management across WAN links.
Monitor mode	The APs exclude themselves from handling data traffic and dedicate themselves to location-based services (LBS).
Rogue Detector mode	Monitors for rouge APs.
Sniffer mode	Captures and forwards all packets of a remote sniffer.
Bridge mode	For point-to-point and point-to-multipoint solutions.

Table 4-9 summarizes the wireless controller components.

Table 4-9 *WLC Components*

WLC Component	Description
Wireless LAN	Identified by a unique SSID and assigned to an interface.
Interface	A logical connection that maps to a VLAN in the wired network.
Port	A physical connection to the wired LAN.

Table 4-10 summarizes WLC interface types.

Table 4-10 *WLC Interface Types*

WLC Interface Type	Description
Management interface	For in-band management.
Service-port interface	For out-of-band management.
AP manager interface	For Layer 3 discovery and association.
Dynamic interface	Dedicated to WLAN client data; analogous to VLANs.
Virtual interface	For Layer 3 authentication and mobility management.

Table 4-11 shows how many APs each WLC model supports.

Table 4-11 *WLAN Controller Platform Scalability*

Platform	Number of Supported Access Points
Cisco 2000 series WLC	6
Cisco WLC for ISRs	6
Catalyst 3750 Integrated WLC	50
Cisco 4400 series WLC	100
Cisco 6500 series WLC Module	300

Table 4-12 describes the three types of controller roaming.

Table 4-12 *Controller Roaming Types*

WLC Roaming Type	Description
Intracontroller roaming	The client moves the association from one AP to another AP that is joined to the same WLC. The client entry in the database is updated. No client IP changes occur.
Layer 2 intercontroller roaming	The client moves the association from one AP to another AP that is joined to a different WLC. The Layer 2 roam occurs when the client traffic is bridged to the same IP subnet. The client entry in the database is moved to the new WLC. No IP changes occur.
Layer 3 intercontroller roaming	The client moves the association from one AP to another AP that is joined to a different WLC, and the traffic is bridged onto a different IP subnet. The client entry in the database is copied to the new WLC and is marked as foreign.

Table 4-13 summarizes some of the UDP ports used by WLAN protocols.

Table 4-13 *UDP Ports Used by WLAN Protocols*

WLAN Protocol	UDP Port
LWAPP Control	UDP 12223
LWAPP Data	UDP 12222
WLC Exchange Messages (unencrypted)	UDP 16666
WLC Exchange Messages (encrypted)	UDP 16667
RF Group IEEE 802.11b/g	UDP 12114
RF Group IEEE 802.11a	UDP 12115

Deterministic controller design is the recommended practice in WLAN controller redundancy design. Table 4-14 summarizes WLC redundancy options.

Table 4-14 *WLC Redundancy*

WLC Redundancy	Description
N+1	A single WLC acts as the backup for multiple WLCs. The backup WLC is configured as the secondary on APs.
N+N	An equal number of controllers back up each other.
N+N+1	An equal number of controllers back up each other. The backup WLC is configured as the tertiary on APs.

The Cisco Wireless Mesh networking solution eliminates the need to wire each AP and allows users to roam from one area to another without having to reconnect. Table 4-15 describes the Wireless Mesh Components.

Table 4-15 *Wireless Mesh Components*

Wireless Mesh Component	Description
Wireless Control System (WCS)	The wireless mesh SNMP management system allows network-wide configuration and management.
Wireless LAN Controller (WLC)	Links the mesh APs to the wired network.
Rooftop AP (RAP)	Connects the mesh to the wired network and serves as the root.
Mesh Access Point (MAP)	Remote APs, typically located on top of a pole. Connects to the RAP.

The following points summarize wireless LAN design:

- An RF site survey is used to determine a wireless network's RF characteristics and access point placement.
- Guest services are easily supported using EoIP tunnels in the Cisco Unified Wireless Network.
- Outdoor wireless networks are supported using outdoor access points and Cisco Wireless Mesh Networking access points.
- Campus wireless network design provides RF coverage for wireless clients in the campus using LWAPs. The LWAPs are managed by WLCs.
- Branch wireless network design provides RF coverage for wireless clients in the branch. Central management of REAP or H-REAP access points can be supported.
- The recommended AP limit is roughly seven (g.711) to eight (g.729) voice calls over VoWLAN or up to 20 data devices, because all devices share bandwidth.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What is the maximum data rate of IEEE 802.11g?
2. What is the typical data rate of IEEE 802.11n?
3. What are some difficulties with having to manage hundreds of standalone access points?
4. What standard does IEEE 802.11i use for confidentiality, integrity, and authentication?
5. List at least four benefits of Cisco UWN.
6. True or false: With Split-MAC, the control and data frames are load-balanced between the LWAP and the WLC.
7. True or false: With Split-MAC, the WLC, not the LWAP, is responsible for authentication and key management.
8. What LWAPP transport mode is the preferred and most scalable?
   a. Intra
   b. Layer 2
   c. Layer 3
   d. EoIP
9. What is the preferred intercontroller roaming option?
   a. Intra
   b. Layer 2
   c. Layer 3
   d. EoIP
10. What device places user traffic on the appropriate VLAN?
    a. Lightweight AP
    b. WLAN controller
    c. MAP
    d. RAP

11. How many access points are supported in a mobility group using Cisco 4400 series WLCs?
    a. 144
    b. 1200
    c. 2400
    d. 7200
12. What is the recommended number of data devices an AP can support for best performance?
    a. About 6
    b. 7 to 8
    c. 10 to 15
    d. About 20
13. What is the recommended number of VoWLAN devices an AP can support for best performance?
    a. 2 to 3
    b. 7 to 8
    c. 10 to 15
    d. About 20
14. What method is used to manage radio frequency channels and power configuration?
    a. WLC
    b. WCS
    c. RRM
    d. MAP
15. What is the typical latency per wireless mesh hop in milliseconds?
    a. 2 to 3
    b. 7 to 8
    c. 10 to 15
    d. About 20
16. What is the recommended maximum RTT between an AP and the WLC?
    a. 20 ms
    b. 50 ms
    c. 100 ms
    d. 200 ms

17. What is the recommended controller redundancy technique?
    a. N+1+N
    b. Static
    c. Dynamic
    d. Deterministic
18. What is the recommended best practice for guest services?
    a. Use separate VLANs
    b. Use separate routers and access lists
    c. Obtain a DSL connection and bridge to the local LAN
    d. Use EoIP to isolate traffic to the DMZ
19. What is the recommended best practice for branch WLANs?
    a. Use H-REAP with centralized controllers
    b. Use local-MAP
    c. Use wireless mesh design
    d. Use EoIP
20. What are two recommended best practices for WLC design?
    a. Maximize intercontroller roaming
    b. Minimize intercontroller roaming
    c. Use distributed controller placement
    d. Use centralized controller placement
21. How many APs does the Cisco 6500 WLC module support?
    a. 6
    b. 50
    c. 100
    d. 300
22. Match each LWAPP access point mode with its description:

    i. Local

    ii. REAP

    iii. Monitor

    iv. Rogue detector

v. Sniffer

vi. Bridge

a. For location-based services

b. Captures packets

c. For point-to-point connections

d. Default mode

e. Management across the WAN

f. Monitors rouge APs

23. Match each WLC interface type with its description:

i. Management

ii. Service-port

iii. AP manager

iv. Dynamic

v. Virtual

a. Authentication and mobility

b. Analogous to user VLANs

c. Discovery and association

d. Out-of-band management

e. In-band management

24. Match each roaming technique with its client database entry change:

i. Intracluster roaming

ii. Layer 2 intercluster roaming

iii. Layer 3 intercluster roaming

a. The client entry is moved to a new WLC

b. The client entry is updated on the same WLC

c. The client entry is copied to a new WLC

25. Match each UDP port with its protocol:

i. LWAPP data

ii. RF group 802.11b/g

iii. WLC encrypted exchange

iv. LWAPP control

v. WLC unencrypted exchange

a. UDP 12114

b. UDP 12222

c. UDP 12223

d. UDP 16666

e. UDP 16667

26. Match each wireless mesh component with its description:

i. WCS

ii. WLC

iii. RAP

iv. MAP

a. Root of the mesh network

b. Remote APs

c. Networkwide configuration and management

d. Links APs to the wired network

27. How many MAP nodes are recommended per rooftop AP?

a. 6

b. 20

c. 500

d. 100

28. Which of the following shows the correct order of the steps in an RF site survey?

- **a.** Define requirements, document findings, perform the survey, determine preliminary AP locations, identify coverage areas.
- **b.** Define requirements, perform the survey, determine preliminary AP locations, identify coverage areas, document findings.
- **c.** Identify coverage areas, define requirements, determine preliminary AP locations, perform the survey, document findings.
- **d.** Define requirements, identify coverage areas, determine preliminary AP locations, perform the survey, document findings.

29. What technique performs dynamic channel assignment, power control, and interference detection and avoidance?

- **a.** LWAPP
- **b.** RRM
- **c.** Mobility
- **d.** LEAP

30. What are the three nonoverlapping channels of IEEE 802.11b/g?

- **a.** Channels A, D, and G
- **b.** Channels 1, 6, and 11
- **c.** Channels 3, 8, and 11
- **d.** Channels A, E, and G

31. Which of the following statements is true?

- **a.** IEEE 802.11g is backward-compatible with 802.11b; 802.11a is not compatible with 802.11b.
- **b.** IEEE 802.11a is backward-compatible with 802.11b; 802.11g is not compatible with 802.11b.
- **c.** IEEE 802.11b is backward-compatible with 802.11a; 802.11g is not compatible with 802.11b.
- **d.** IEEE 802.11n is backward-compatible with 802.11a and 802.11g.

32. What is necessary when you use LEAP for authentication?

- **a.** WLC
- **b.** WCS
- **c.** RADIUS server
- **d.** LWAP

This chapter covers the following subjects:

- WAN Technology Overview
- WAN Design Methodology
- Optimizing Bandwidth Using QoS

CHAPTER 5

WAN Technologies

This chapter reviews wide-area network technologies. Expect plenty of questions about the use of WAN technologies. The CCDA must understand WAN technologies and what makes them different from each other. This chapter also covers WAN design methodologies and how some QoS techniques can make better use of the available bandwidth.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 5-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 5-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
WAN Technology Overview	1, 2, 3, 5, 6, 7, 8
WAN Design Methodology	4, 9
Optimizing Bandwidth Using QoS	10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. What are two modules or blocks used in the Enterprise Edge?
   a. Internet and Campus Core
   b. Core and Building Access
   c. Internet Connectivity and WAN
   d. WAN and Building Distribution
2. What signaling protocol does Frame Relay use between the switch and the router?
   a. DLCI
   b. LMI
   c. TDM
   d. SONET/SDH
3. How much bandwidth does a T1 circuit provide?
   a. 155 Mbps
   b. 64 kbps
   c. 1.544 kbps
   d. 1.544 Mbps
4. What methodology is used when designing the Enterprise Edge?
   a. Cisco-powered network
   b. ISL
   c. PPDIOO
   d. IEEE
5. SONET/SDH technology is what kind of technology?
   a. Packet-based
   b. Cell-based
   c. Circuit-based
   d. Segment-based
6. Which DSL technology uses higher download speeds than upload speeds and is popular in residential deployments?
   a. IDSL
   b. ADSL
   c. SDSL
   d. TDSL

7. What Frame Relay DE bit value is of lower importance and can be discarded first?

   a. 2

   b. 1

   c. 0

   d. 2.1

8. When designing a network for four separate sites, what technology allows a full mesh by using only one link per site instead of point-to-point TDM circuits?

   a. Dark fiber

   b. Cable

   c. ISDN

   d. Frame Relay

9. The _____ size specifies the maximum number of frames that are transmitted without receiving an acknowledgment.

   a. Segment

   b. Access

   c. TCP

   d. Window

10. Which of the following adds strict PQ to modular class-based QoS?

    a. LLQ

    b. FIFO

    c. CBWFQ

    d. WFQ

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers WAN topics that you need to master for the CCDA exam. It covers the different WAN modules used in the Enterprise Edge. WAN technologies and factors that are used in technology selection are covered. It covers the specifics of several WAN technologies that are available today. The chapter goes on to outline methodologies used for designing WANs. Finally, this chapter covers ways to use quality of service (QoS) to prioritize network traffic and improve the use of available bandwidth.

WAN Technology Overview

WAN technologies provide network connectivity for the Enterprise Edge and remote branch edge locations as well as the Internet. Many WAN choices are available, and new ones are continually emerging. When you're selecting WAN transport technologies, it is important to consider factors such as cost, speed, reliability, hardware, and media. In addition, enterprise branch offices can take advantage of cable and DSL technologies for remote connectivity back to the headquarters or main office.

WAN Defined

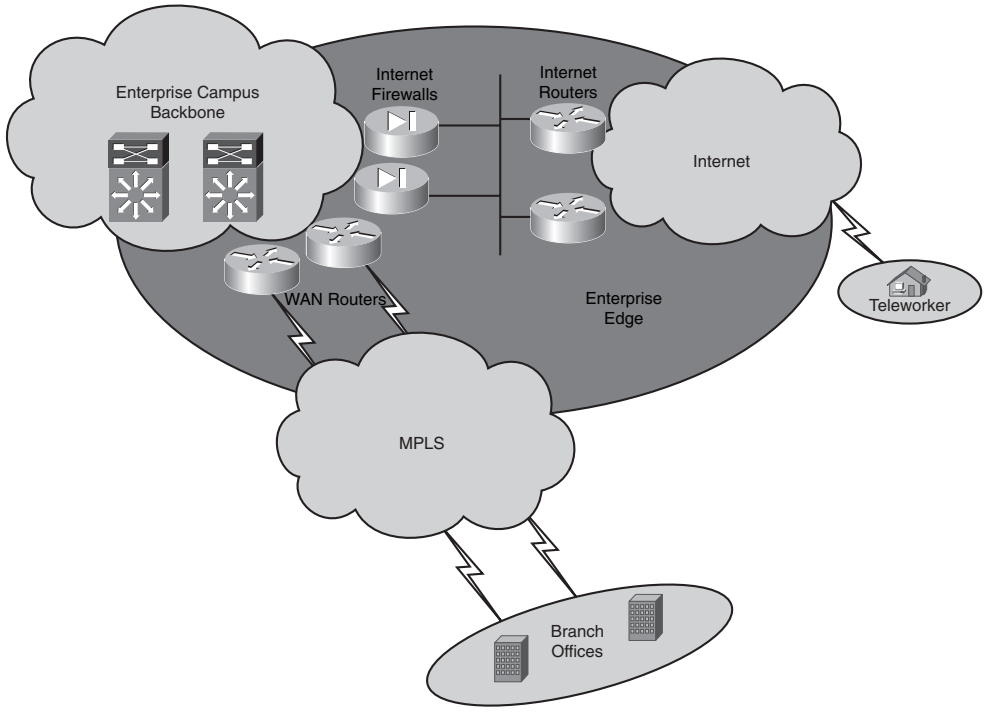
Wide-area networks (WANs) are communication networks that can span great distances to provide connectivity. They generally are offered by service providers or carriers. WANs typically carry data traffic, but many now support voice and video as well. Service providers charge fees for providing WAN services or communications to their customers. Sometimes the term "service" is referred to as the WAN communications provided by the carrier.

Figure 5-1 depicts the Enterprise Edge with campus backbone, Internet, and MPLS clouds.

When designing a WAN, you should become familiar with the design's requirements, which are typically derived from these two important goals:

- **Application availability**—Networked applications rely on the network between the client and server to provide its functions to users.
- **Cost and usage**—To select the correct reliable WAN service, you must consider the budget and usage requirements of the WAN service.

Figure 5-1 *Enterprise WAN*



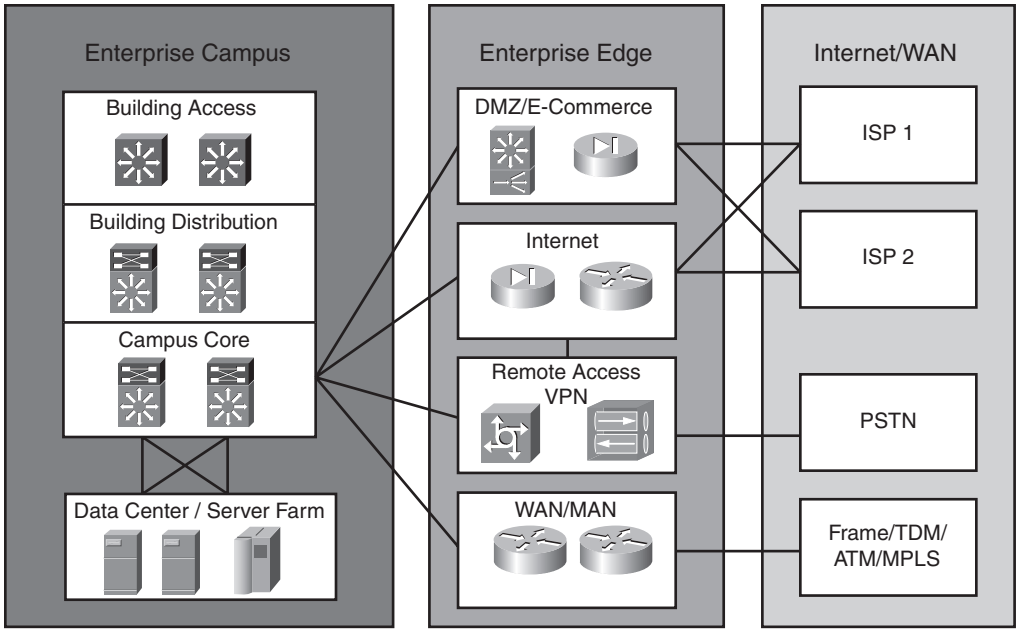
WAN Connection Modules

The Enterprise Edge can have multiple WAN interconnections. Common connectivity modules include but are not limited to the Internet, the demilitarized zone (DMZ), and the WAN. Internet service providers (ISPs) offer many connectivity options for the Internet and DMZ modules of the Enterprise Edge. Internal WAN connectivity between an organization's headquarters and remote sites generally is across a service provider or carrier network. PSTN connectivity still exists for teleworkers and more recently because of the increasing use of VoIP offnet services.

WAN technologies such as Frame Relay exist for point-to-point (P2P) and multipoint WAN services. Service providers also offer full IP WAN solutions such as MPLS where the Enterprise Edge router interacts with service providers at Layer 3. Public WAN connections over the Internet are also available through the use of cable and/or DSL technologies. Typically, these services do not provide any guarantee of network availability, as do Frame Relay and MPLS network solutions.

Figure 5-2 illustrates the use of modules, or blocks, in the Enterprise Edge.

Figure 5-2 *WAN Interconnections*



WAN Comparison

Table 5-2 examines some WAN technologies and highlights some common factors that are used to make WAN technology selections. This information also reflects the different characteristics of each WAN technology. However, keep in mind that your service provider offerings limit the WAN technology choices available to you during your selection.

Table 5-2 *WAN Comparison*

WAN Technology	Bandwidth	Reliability	Latency	Cost
Dialup	Low	Low	High	Low
ISDN	Low	Medium	Medium	Low
Frame Relay	Low/Medium	Medium	Low	Medium
TDM	Medium	High	Low	Medium
SONET/SDH	High	High	Low	High
MPLS	High	High	Low	High
Dark fiber	High	High	Low	High

Table 5-2 *WAN Comparison (Continued)*

WAN Technology	Bandwidth	Reliability	Latency	Cost
DWDM	High	High	Low	High
DSL	Low/Medium	Low	Medium	Low
Cable	Low/Medium	Low	Medium	Low
Wireless	Low/Medium	Low	Medium	Medium

The following sections offer more details about each WAN technology covered in Table 5-2.

Dialup

Dialup technology provides connectivity over the PSTN using analog modems. Although the bandwidth is relatively low, the availability of analog is very widespread. Dialup connectivity is ideal for low-bandwidth conversations of 56 kbps or less. Despite the high availability of dialup technology over analog lines, it is generally not a viable option anymore. However, a common use of dialup is when a remote worker or teleworker uses it as a backup network solution if his or her DSL or cable connection goes down.

ISDN

Integrated Services Digital Network (ISDN) is an all-digital phone line connection that was standardized in the early 1980s. ISDN allows both voice and data to be transmitted over the digital phone line instead of the analog signals used in dialup connections. ISDN provides greater bandwidth and lower latency compared to dialup analog technology. ISDN comes in two service types—Basic Rate Interface (BRI) and Primary Rate Interface (PRI).

ISDN is comprised of digital devices and reference points. ISDN devices consist of terminals, terminal adapters, network-termination, line-termination, and exchange-termination equipment. Native ISDN devices are referred to as terminal equipment 1 (TE1), and nonnative ISDN is referred to as terminal equipment 2 (TE2). However, TE2-type devices can be connected to an ISDN system with the help of a terminal adapter (TA).

Working toward the service provider after the TE1 and TE2 devices, the next connection devices are network termination 2 (NT2) and network termination 1 (NT1). These connection devices connect the five-wire to the two-wire local loop. In North America, the NT1 is a CPE device or customer premises equipment. This means that the customer, not the carrier, provides the device. However, in most other parts of the world, the carrier provides the NT1.

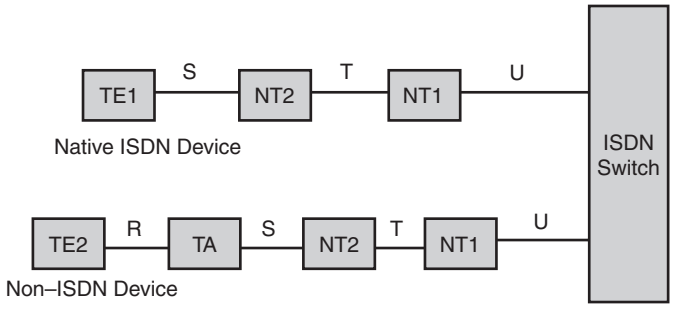
NOTE Some Cisco IOS interface cards have the NT1 built in designated by a U, whereas others require an external NT1 device.

ISDN has a series of reference points that define logical interfaces between ISDN devices such as TAs and NT1s:

- **R**—Reference point between non-ISDN equipment and a TA
- **S**—Reference point between terminals and NT2 devices
- **T**—Reference point between NT2 and NT1 devices
- **U**—Reference point between NT1 and the line termination equipment in the carrier's network

Figure 5-3 illustrates how ISDN devices and reference points relate to each other.

Figure 5-3 *ISDN Devices and Reference Points*



ISDN BRI Service

ISDN BRI consists of two B channels and one D channel (2B+D). Both of the BRI B channels operate at 64 kbps and carry user data. The D channel handles the signaling and control information and operates at 16 kbps. Another 48 kbps is used for framing control and other overhead, for a total bit rate of 192 kbps.

ISDN PRI Service

ISDN PRI service offers 23 B channels and one D channel (23B+D) in both North America and Japan. Each channel (including the D channel) operates at 64 kbps, for a total bit rate of 1.544 Mbps, including overhead. In other parts of the world, such as Europe and Australia, the ISDN PRI service provides 30 B channels and one 64-kbps D channel.

Frame Relay

Frame Relay is a connection-oriented Layer 2 WAN protocol. It is similar to X.25 but has faster performance due to the lack of error checking and retransmitting features. The data link layer establishes connections in Frame Relay using a DTE device such as a router and a DCE device such as a frame switch.

In the early 1980s, networks were growing using more and more point-to-point leased-line connections. Full-mesh connections were used to ensure redundancy between sites. However, full-mesh network configurations presented a larger cost because of the number of leased lines needed. A full mesh requires that each site have a connection to the other sites participating in the full mesh. For example, if you have five WAN sites, each site needs four leased lines to the other sites to complete the full mesh. However, because Frame Relay uses a cloud of switches, each site can use only one connection to the Frame Relay cloud and then can be configured to emulate a full mesh. This reduces the leased-line cost and requires only one leased line per site. This allows the network to achieve full-mesh-like behavior needed for network redundancy.

Frame Relay circuits between sites can be either permanent virtual circuits (PVC) or switched virtual circuits (SVC). PVCs are used more predominantly due to the connections' permanent nature. SVCs, on the other hand, are temporary connections created for each data transfer session.

A point-to-point PVC between two routers or endpoints uses a data-link connection identifier (DLCI) to identify the local end of the PVC. The DLCI is a locally significant numeric value that can be reused through the Frame Relay WAN if necessary.

Local Management Interface

Frame Relay uses a signaling protocol between the Frame Relay router and the Frame Relay switch called the Local Management Interface (LMI). The LMI protocol sends periodic keepalive messages and notifications of additions or removals of PVCs. Three types of LMI protocols are available. The service provider usually informs you on which one to use. LMI also offers a number of features or extensions, including global addressing, virtual circuit status messages, and multicasting. By default, Cisco routers will try all three LMI types until a match is found.

Discard Eligibility

The Discard Eligibility (DE) bit is used in Frame Relay to identify whether a frame has lower importance than other frames. The DE bit is part of the Frame Relay header and can have a value of 1 or 0. Routers or DTE devices can set the value of the DE bit to 1 to indicate that the frame has lower importance than frames marked with a 0. During periods of congestion, the Frame Relay network discards frames marked with the DE bit of 1 before those marked with 0. This reduces the chance of critical data being dropped, because you can identify what traffic gets marked with a DE bit value of 1.

Time-Division Multiplexing

Time-Division Multiplexing (TDM) is a type of digital multiplexing in which multiple channels such as data, voice, and video are combined over one communication medium by interleaving pulses representing bits from different channels. Basic DS0 channel bandwidth is defined at 64 kbps. In North America, a DS1 or T1 circuit provides 1.544 Mbps of bandwidth consisting of 24 time slots of 64 kbps each and an 8-kbps channel for control information. In addition, a DS3 or T3 circuit provides 44.736 Mbps of bandwidth. Other parts of the world, such as Europe, follow E1 standards, which allow for 30 channels at 2.048 Mbps of bandwidth. Service providers can guarantee or reserve the bandwidth used on TDM networks. The customers' TDM transmissions are charged for their exclusive access to these circuits. On the other hand, packet-switched networks typically are shared, thereby allowing the service providers more flexibility in managing their networks and the services they offer.

SONET/SDH

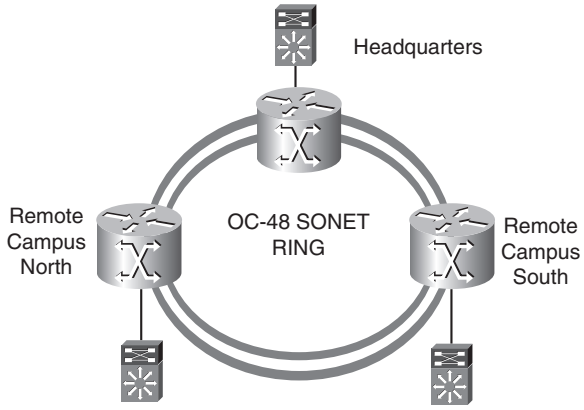
The architecture of Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) is circuit-based and delivers high-speed services over an optical network. The term SONET is defined by the American National Standards Institute (ANSI) specification, and SDH is defined by the International Telecommunication Union (ITU). SONET/SDH guarantees bandwidth and has line rates of 155 Mbps to more than 10 Gbps. Common circuit sizes are OC-3, or 155 Mbps, and OC-12, or 622 Mbps.

SONET/SDH uses a ring topology by connecting sites and providing automatic recovery capabilities and has self-healing mechanisms. SONET/SDH rings support ATM or packet over SONET (POS) IP encapsulations. The Optical Carrier (OC) rates are the digital bandwidth hierarchies that are part of the SONET/SDH standards. The optical carrier speeds supported are as follows:

- OC-1 = 51.85 Mbps
- OC-3 = 155.52 Mbps
- OC-12 = 622.08 Mbps
- OC-24 = 1.244 Gbps
- OC-48 = 2.488 Gbps
- OC-192 = 9.952 Gbps
- OC-255 = 13.21 Gbps

Figure 5-4 shows an OC-48 SONET ring with connections to three sites that share the ring.

Figure 5-4 *SONET/SDH*



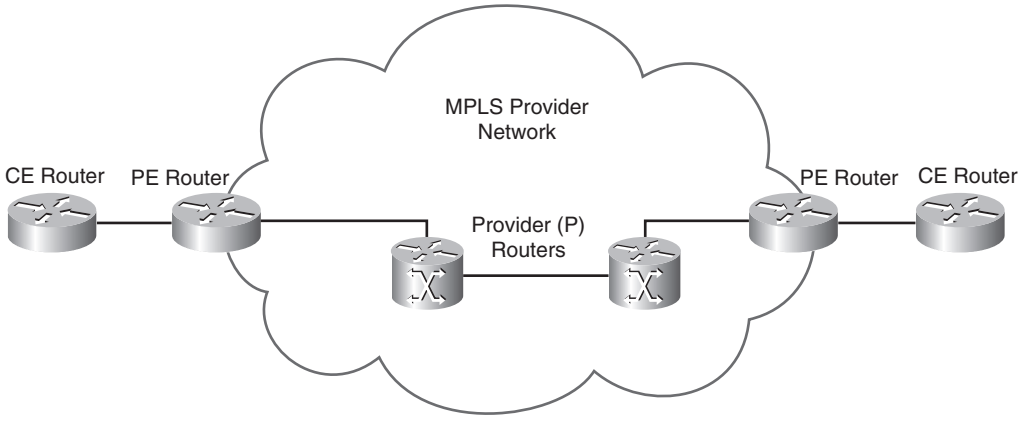
Multiprotocol Label Switching

MPLS is technology for the delivery of IP services using labels (numbers) to forward packets. In normal routed environments, packets are forwarded by the router performing a Layer 3 destination address lookup and rewriting the Layer 2 addresses. MPLS functions by encapsulating packets with headers that include the label information. As soon as packets are marked with a label, specific paths through the network can be designed to correspond to that distinct label. MPLS labels can be based on parameters such as source addresses, Layer 2 circuit ID, or QoS value. The labels can be used to implement traffic engineering by overriding the routing tables. MPLS packets can run over most Layer 2 technologies, such as ATM, Frame Relay, POS, and Ethernet. The goal of MPLS is to maximize switching using labels and minimize Layer 3 routing.

In most MPLS implementations, the equipment is called the customer edge (CE) and provider edge (PE) routers. Typically the customer-owned internal WAN router peers with the CE router. The CE router then connects to the PE router, which is the ingress to the MPLS service provider network. The PE router is in the service provider network.

Figure 5-5 shows an MPLS WAN and how the CE routers connect to the provider.

Figure 5-5 *MPLS*



Other WAN Technologies

This section briefly discusses other WAN technologies that are becoming very popular in the network access space as well as some other service provider architectures.

Digital Subscriber Line

Digital Subscriber Line (DSL) is a technology that provides high-speed Internet data services over ordinary copper telephone lines. It achieves this by using frequencies that are not used in normal voice telephone calls.

The term *x*DSL describes the various competing forms of DSL available today. Some of the DSL technologies available include asymmetric (ADSL), symmetric (SDSL), high bit rate (HDSL), very high bit rate (VDSL), rate-adaptive (RADSL) and IDSL (based on ISDN).

Table 5-3 summarizes the types of DSL specifications.

Table 5-3 *DSL Specifications*

Service	Maximum Distance to Central Office	Maximum Upload Speed	Maximum Download Speed	Notes
Full-rate ADSL	18,000 ft (5500 m)	1500 kbps	9 Mbps	Asymmetrical.
ADSL G.lite	18,000 ft (5500 m)	384 kbps	1.5 Mbps	No splitter is required.
RADSL	18,000 ft (5500 m)	384 kbps	8 Mbps	Rate adapts based on distance and quality.

Table 5-3 *DSL Specifications (Continued)*

Service	Maximum Distance to Central Office	Maximum Upload Speed	Maximum Download Speed	Notes
IDSL	35,000 ft (10,070 m)	144 kbps	144 kbps	DSL over ISDN (BRI).
SDSL	22,000 ft (6700 m)	2.3 Mbps	2.3 Mbps	Targets T1 replacement. Symmetrical DSL service.
HDSL	18,000 ft (5500 m)	1.54 Mbps	1.54 Mbps	Four-wire, similar to T1 service.
HDSL-2	24,000 ft (7333 m)	2 Mbps	2 Mbps	Two-wire version of HDSL or four-wire at 2 times the rate.
VDSL	3000 ft (916 m)	16 Mbps	52 Mbps	Few installations.

ADSL is the most popular DSL technology and is widely available. The key to ADSL is that the downstream bandwidth is asymmetric or higher than the upstream bandwidth. Some limitations include that ADSL can be used only in close proximity to the local DSLAM, typically less than 2 km. The local DSLAM, or digital subscriber line access multiplexer, allows telephone lines to make DSL connections to the Internet. Download speeds usually range from 768 kbps to 9 Mbps, and upload speeds range from 64 kbps to 1.5 Mbps. Generally, the equipment used is a DSL modem or (CPE) router that connects back to the ISP's DSLAM.

Although DSL is primarily used in the residential community, this technology can also be used as a WAN technology for an organization. However, keep in mind that because this is a public network connection over the Internet, it is recommended that this technology be used in conjunction with a firewall/VPN solution back into your corporate enterprise network. The high speeds and relatively low cost make this a very popular Internet access WAN technology.

Cable

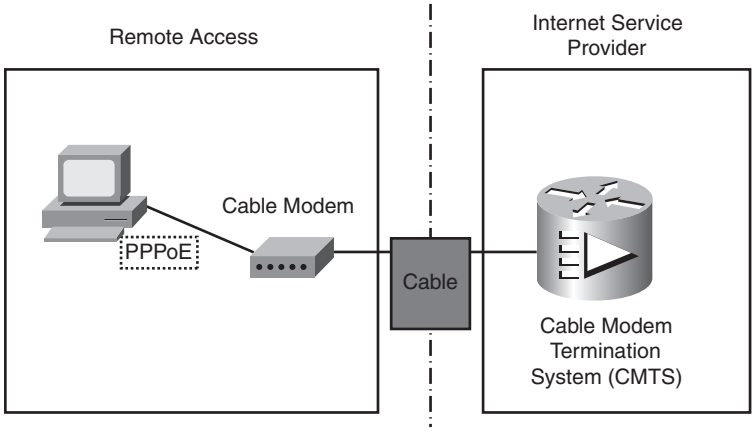
Broadband cable is a technology used to transport data using a coaxial cable medium over cable distribution systems. The equipment used on the remote-access side is the cable modem, which connects to the Cable Modem Termination System (CMTS) on the ISP side. The Universal Broadband Router (uBR) provides the CMTS services and is deployed at the cable company headend. The uBR forwards traffic upstream through the provider's WAN core or the local PSTN, depending on the services being provided.

The Data Over Cable Service Interface Specifications (DOCSIS) protocol defines the cable procedures that the equipment needs to support. DOCSIS 2.0 was released in 2002 and remains

the current version that most cable modems use today. DOCSIS 3.0 specifications released in 2006 include support for IPv6 and channel bonding.

Figure 5-6 illustrates how a cable modem connects to the CMTS.

Figure 5-6 *Data Over Cable*



Wireless

Wireless as a technology uses electromagnetic waves to carry the signal between endpoints. Everyday examples of wireless technology include cell phones, wireless LANs, cordless computer equipment, and satellite television.

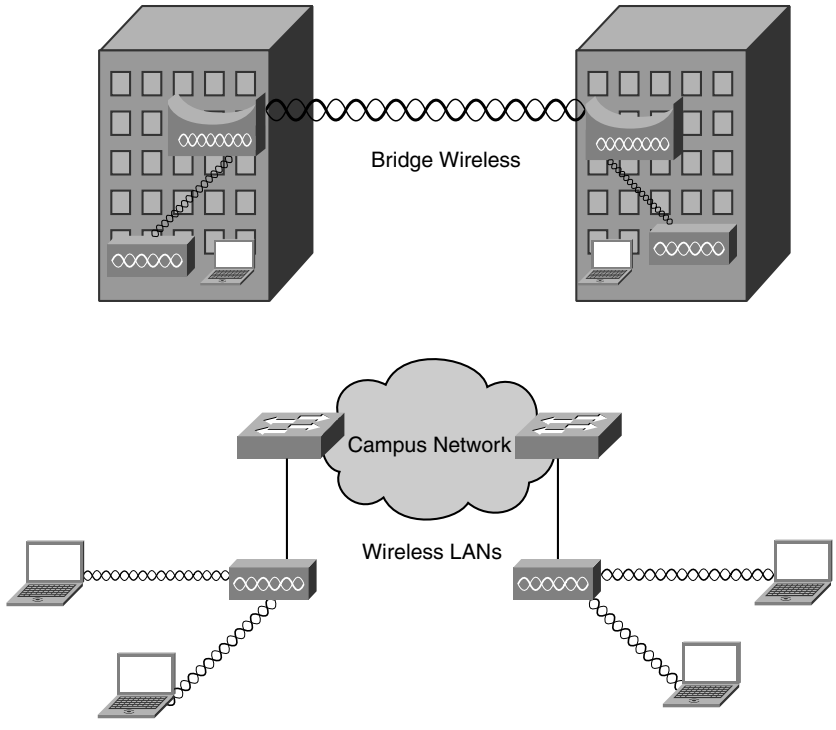
Here are some examples of wireless implementations:

- **Mobile wireless**—Consists of cellular applications and mobile phones. Most wireless technologies such as the second and third generations are migrating to more digital services to take advantage of the higher speeds. Mobile wireless technologies include GSM, GPRS, and UMTS:
  - **GSM**—Global system for mobile communications. A digital mobile radio standard that uses Time-Division Multiplex Access (TDMA) technology in three bands—900, 1800, and 1900 MHz. The data transfer rate is 9600 bps and includes the ability to roam internationally.
  - **GPRS**—General Packet Radio Service. Extends the capability of GSM speeds from 64 kbps to 128 kbps.
  - **UMTS**—Universal Mobile Telecommunications Service. Also known as 3G broadband. Provides packet-based transmission of digitized voice, video, and data at rates up to 2.0 Mbps. UMTS also provides a set of services available to mobile users, location-independent throughout the world.

- **Wireless LAN**—WLANs have increased too in both residential and business environments to meet the demands of LAN connections over the air. Commonly called IEEE 802.11a/b/g or Wi-Fi wireless networks. Currently, 802.11n is in development and provides typical data rates of 200 Mb/s. The growing range of applications includes guest access, voice over wireless, and support services such as advanced security and location of wireless endpoints. A key advantage of WLANs is the ability to save time and money by avoiding costly physical layer wiring installations.
- **Bridge wireless**—Wireless bridges connect two separate wireless networks, typically located in two separate buildings. This technology enables high data rates for use with line-of-sight applications. When interconnecting hard-to-wire sites, temporary networks, or warehouses, a series of wireless bridges can be connected to provide connectivity.

Figure 5-7 shows bridge wireless and wireless LANs.

Figure 5-7 *Wireless Implementations*



NOTE Additional information on wireless LANs is provided in Chapter 4, "Wireless LAN Design."

Dark Fiber

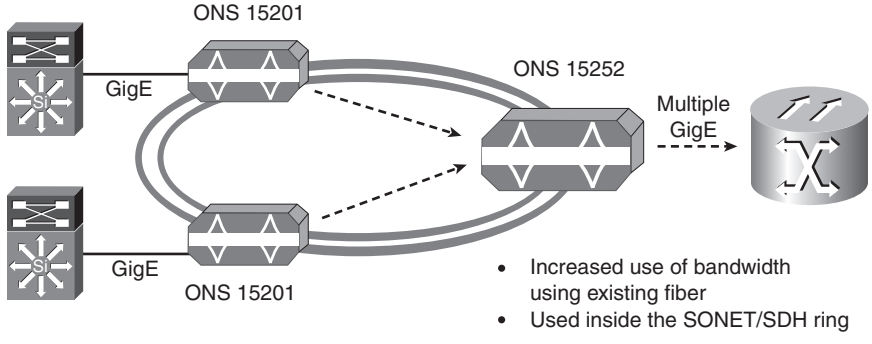
Dark fiber is fiber-optic cable that has been installed in the ground or where right-of-way issues are evident. To maintain signal integrity and jitter control over long distances, signal regenerators are used in some implementations. The framing for dark fiber is determined by the enterprise, not the provider. The edge devices can use the fiber just like within the enterprise, which allows for greater control of the services provided by the link. Dark fiber is owned by service providers in most cases and can be purchased similarly to leased-line circuits for use in both the MAN and WAN. The reliability of these types of links also needs to be designed by the enterprise and is not provided by the service provider. This contrasts with SONET/SDH, which has redundancy built into the architecture.

Dense Wave Division Multiplexing

Dense Wave Division Multiplexing (DWDM) increases fiber optic's bandwidth capabilities by using different wavelengths of light called channels over the same fiber strand. It maximizes the use of the installed base of fiber used by service providers and is a critical component of optical networks. DWDM allows for service providers to increase the services offered to customers by adding new bandwidth to existing channels on the same fiber. DWDM lets a variety of devices access the network, including IP routers, ATM switches, and SONET terminals.

Figure 5-8 illustrates the use of DWDM using Cisco ONS devices and a SONET/SDH ring.

Figure 5-8 *DWDM*



Ordering WAN Technology and Contracts

When you order WAN transport technology, early planning is key. It usually takes at least 60 days for the carrier to provision circuits. Generally, the higher a circuit's capacity, the more lead time is required to provision. When ordering bandwidth overseas, a lead time of 120 days is fairly common.

WAN transport in most cases includes an access circuit charge and, at times, distance-based charges. However, some carriers have eliminated TDM distance-based charges because T1s are readily available from most carriers. In rare cases, construction is necessary to provide fiber access, which requires more cost and time delays. You should compare pricing and available WAN technology options from competing carriers.

When ordering Frame Relay and ATM, a combination of access circuit charges, per-PVC charges, and per-bandwidth Committed Information Rate (CIR) charges are customary. CIR is the rate that the provider guarantees it will provide. Some carriers set the CIR to half the circuit's speed, thereby allowing customers to burst 2 times above the CIR. Frame Relay speeds can be provisioned up to T3 speeds, but typically they are less than 10 Mbps.

MPLS VPNs have been very competitive with ATM and Frame Relay rates. Service providers are offering MPLS VPNs with higher bandwidth at lower rates to persuade their customers away from traditional ATM and Frame Relay services. However, other service providers see more value in MPLS VPNs and price them higher than ATM and Frame Relay because of the added benefits of traffic engineering.

When you're selecting a standard carrier package, it takes about a month to contract a WAN circuit. If you want to negotiate a detailed service level agreement (SLA), expect to take another five months or more, including discussions with the service provider's legal department. The bigger the customer, the more influence it has over the SLAs and the contract negotiations.

Contract periods for most WAN services are one to five years. Contracts are usually not written for longer durations because of the new emerging technologies and better offerings from providers. An exception is dark fiber, which is usually contracted for a 20-year term. In this case you also want to have the right of nonreversion written in the SLA. This means that no matter what happens to the service provider, the fiber is yours for the 20-year period.

Tariffed commercial WAN services are available at published rates but are subject to restrictions. However, carriers are moving toward unpublished rates to be more competitive and to offer more options.

WAN Design Methodology

The methodology used when designing the Enterprise Edge is called prepare, plan, design, implement, operate, and optimize (PPDIOO). Some keys to PPDIOO are the processes of analyzing network requirements, characterizing the existing network, and designing the topology:

- **Analyzing the network requirements** includes reviewing the types of applications, the traffic volume, and the traffic patterns in the network.

- **Characterizing the existing network** reviews the technologies used and the locations of hosts, servers, network equipment, and other end nodes.
- **Designing the topology** is based on the availability of technology, the projected traffic usage, network performance, constraints, reliability, and implementation planning.

New network designs should be flexible and adaptable to future technologies and should not limit the customer's options going forward. Voice over IP (VoIP) is an example of a technology that network designs should be able to support if the customer decides to move to a converged network. The customer should not have to undergo major hardware and software upgrades to implement these types of technologies. Another important consideration is the design's cost-effectiveness throughout the design and implementation stages. For example, the support and management of the network should be an important factor.

Response Time

Response time measures the time between the client user request and the response from the server host. The end user will accept a certain level of delay in response time and still be satisfied. However, there is a limit to how long the user will wait. This amount of time can be measured and serves as a basis for future application response times. Users perceive the network communication in terms of how quickly the server returns the requested information and/or how fast the screen updates. Some applications, such as a request for an HTML web page, require short response times. On the other hand, a large FTP transfer may take a while, but this is generally acceptable.

Throughput

In network communications, throughput is the measure of data transferred from one host to another in a given amount of time. Bandwidth-intensive applications have more of an impact on a network's throughput than interactive traffic such as a Telnet session. Most high-throughput applications usually involve some type of file-transfer activity.

Reliability

Reliability is the measure of a given application's availability to its users. Some organizations require rock-solid application reliability; this has a higher price than most other applications. For example, financial and security exchange commissions require nearly 100 percent uptime for their applications. These types of networks are built with a high amount of physical and logical redundancy. It is important to ascertain the level of reliability needed for a network that is being designed. Reliability goes further than availability by measuring not only whether the service is there but whether it is performing as it should.

Bandwidth Considerations

Table 5-4 compares a number of different WAN technologies, along with the speeds and media types associated with them.

Table 5-4 *Physical Bandwidth Comparison*

Bandwidth	Less Than 2 Mbps	2 Mbps to 45 Mbps	45 Mbps to 100 Mbps	100 Mbps to 10 Gbps
Copper	Serial, ISDN, Frame Relay, TDM, DSL	Frame Relay, Ethernet, DSL, cable, T3	Fast Ethernet	Gigabit Ethernet
Fiber	—	Ethernet	FastEthernet, ATM	Gigabit Ethernet, 10Gigabit Ethernet, ATM, SONET/SDH, POS, dark fiber
Wireless	802.11b	802.11b, wireless WAN (varies)	802.11a/g	802.11n

The WAN designer must engineer the network with enough bandwidth to support the needs of the users and applications that will use the network. How much bandwidth a network needs depends on the services and applications that will require network bandwidth. For example, more bandwidth is needed for VoIP traffic than interactive SSH traffic. A large number of graphics or CAD drawings require an extensive amount of bandwidth compared to simple text-based information being transferred on the network, such as HTML files.

When designing bandwidth for the WAN, remember that implementation and recurring costs are always important factors. QoS techniques become increasingly important when delay-sensitive traffic such as VoIP is using the limited bandwidth available on the WAN.

LAN bandwidth, on the other hand, is inexpensive and plentiful. To provide connectivity on the LAN, you typically need to be concerned only with hardware and implementation costs.

Window Size

The window size defines the upper limit of frames that can be transmitted without getting a return acknowledgment. Transport protocols such as TCP rely on acknowledgments to provide connection-oriented reliable transport of data segments. For example, if the TCP window size is set to 8192, the source stops sending data after 8192 bytes if no acknowledgment has been received from the destination host. In some cases the window size might need to be modified because of unacceptable delay for larger WAN links. If the window size is not adjusted to coincide

with the delay factor, retransmissions can occur, which affects throughput significantly. It is recommended that you adjust the window size to achieve better connectivity conditions.

Data Compression

Compression reduces the packet to a smaller size that can be transmitted and then decompressed on the other side of the WAN link. More CPU or hardware time is required to compress and decompress the data, but in return this saves bandwidth and reduces delay on the WAN link.

Compression is available in both software and hardware. Hardware data compression aids the main CPU by offloading the compression and decompression tasks by using the hardware CPU instead. The hardware compression modules can be installed in an available slot on a modular router.

Optimizing Bandwidth Using QoS

QoS is an effective tool for managing a WAN's available bandwidth. Keep in mind that QoS does not add bandwidth; it only helps you make better use of it. For chronic congestion problems, QoS is not the answer; you need to add more bandwidth. However, by prioritizing traffic, you can make sure that your most critical traffic gets the best treatment and available bandwidth in times of congestion. One popular QoS technique is to classify your traffic based on a protocol type or ACL and then give treatment to the class. You can define many classes to match or identify your most important traffic classes. The remaining unmatched traffic then uses a default class in which the traffic can be treated as best effort.

Queuing, Traffic Shaping, and Policing

Cisco has developed many different QoS mechanisms such as queuing, policing, and traffic shaping to enable network operators to manage and prioritize the traffic flowing on the network. Applications that are delay-sensitive require special treatment to avoid dissatisfaction by the user community, such as Voice over *X* technologies. Two types of output queues are available on routers—the hardware queue and the software queue. The hardware queue uses the strategy of first in, first out (FIFO). The software queue schedules packets first and then places them in the hardware queue. Keep in mind that the software queue is used only during periods of congestion. The software queue uses QoS techniques such as Priority Queuing, Custom Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing, Low-Latency Queuing, and traffic shaping and policing.

Priority Queuing

Priority Queuing (PQ) is a queuing method that establishes four interface output queues that serve different priority levels—high, medium, default, and low. Unfortunately, PQ can starve other queues if too much data is in one queue.

Custom Queuing

Custom Queuing (CQ) uses up to 16 individual output queues. Byte size limits are assigned to each queue so that when the limit is reached, it proceeds to the next queue. The network operator can customize these byte size limits. CQ is more fair than PQ because it allows some level of service to all traffic. This queuing method is considering legacy due to the improvements in the queuing methods.

Weighted Fair Queuing

Weighted Fair Queuing (WFQ) ensures that traffic is separated into individual flows or sessions without requiring that you define access control lists (ACL). WFQ uses two categories to group sessions—high bandwidth and low bandwidth. Low-bandwidth traffic has priority over high-bandwidth traffic. High-bandwidth traffic shares the service according to assigned weight values. WFQ is the default QoS mechanism on interfaces below 2.0 Mbps.

Class-Based Weighted Fair Queuing

Class-Based Weighted Fair Queuing (CBWFQ) extends WFQ capabilities by providing support for modular user-defined traffic classes. CBWFQ lets you define traffic classes that correspond to match criteria, including ACLs, protocols, and input interfaces. Traffic that matches the class criteria belongs to that specific class. Each class has a defined queue that corresponds to an output interface.

After traffic has been matched and belongs to a specific class, you can modify its characteristics, such as assigning bandwidth, maximum queue limit, and weight. During periods of congestion, the bandwidth assigned to the class is the guaranteed bandwidth that is delivered to the class.

One of CBWFQ's key advantages is its modular nature, which makes it extremely flexible for most situations. Many classes can be defined to separate your network traffic as needed. CBWFQ is becoming the "standard QoS mechanism" for networks that are not using VoIP.

Low-Latency Queuing

Low-Latency Queuing (LLQ) adds a strict priority queue to CBWFQ. The strict priority queue allows delay-sensitive traffic such as voice to be sent first, before other queues are serviced. That gives voice preferential treatment over the other traffic types.

Without LLQ, CBWFQ would not have a priority queue for real-time traffic. The additional classification of other traffic classes is done using the same CBWFQ techniques. LLQ is the standard QoS method of choice for Voice over IP networks.

Traffic Shaping and Policing

Traffic shaping and policing are mechanisms that take an action based on the traffic's characteristics, such as DSCP or IP precedence bits set in the IP header.

Traffic shaping slows down the rate at which packets are sent out an interface by matching certain criteria. Traffic shaping uses a token bucket technique to release the packets into the output queue at a preconfigured rate. Traffic shaping helps eliminate potential bottlenecks by throttling back the traffic rate at the source.

Policing tags or drops traffic depending on the match criteria. Generally, policing is used to set the limit of incoming traffic coming into an interface.

When contrasting traffic shaping with policing, remember that traffic shaping buffers packets while policing can be configured to drop packets.

References and Recommended Readings

"Cisco IOS Quality of Service Solutions Configuration Guide Release 12.2," http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

"Frame Relay," http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm

"Integrated Services Digital Network," http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/isdn.htm

Module 4, "Designing Remote Connectivity," Designing for Cisco Internetwork Solution Course (DESGN) v2.0

"TDM: Time Division Multiplex and Multiplexer," http://www.networkdictionary.com/telecom/tdm.php

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

This chapter has examined the use of WANs in the Enterprise Edge. It also looked at many of the technologies used in the Enterprise Edge and how they relate to each other. It reviewed the methodology used when designing the Enterprise Edge—PPDIOO. Finally, this chapter discussed several factors that affect bandwidth and ways to optimize bandwidth using QoS techniques.

Table 5-5 examines some WAN technologies and highlights some common factors that are used to make WAN technology selections.

Table 5-5 *WAN Comparison*

WAN Technology	Bandwidth	Reliability	Latency	Cost
Dialup	Low	Low	High	Low
ISDN	Low	Medium	Medium	Low
Frame Relay	Low/Medium	Medium	Low	Medium
TDM	Medium	High	Low	Medium
SONET/SDH	High	High	Low	High
MPLS	High	High	Low	High
Dark fiber	High	High	Low	High
DWDM	High	High	Low	High
DSL	Low/Medium	Low	Medium	Low
Cable	Low/Medium	Low	Medium	Low
Wireless	Low/Medium	Low	Medium	Medium

Table 5-6 summarizes the types of DSL specifications.

Table 5-6 *DSL Specifications*

Service	Maximum Distance to Central Office	Maximum Upload Speed	Maximum Download Speed	Notes
Full-rate ADSL	18,000 ft (5500 m)	1500 kbps	9 Mbps	Asymmetrical.
ADSL G.lite	18,000 ft (5500 m)	384 kbps	1.5 Mbps	No splitter is required.
RADSL	18,000 ft (5500 m)	384 kbps	8 Mbps	Rate adapts based on distance and quality.
IDSL	35,000 ft (10,070 m)	144 kbps	144 kbps	DSL over ISDN (BRI).
SDSL	22,000 ft (6700 m)	2.3 Mbps	2.3 Mbps	Targets T1 replacement. Symmetrical DSL service.
HDSL	18,000 ft (5500 m)	1.54 Mbps	1.54 Mbps	Four-wire, similar to T1 service.
HDSL-2	24,000 ft (7333 m)	2 Mbps	2 Mbps	Two-wire version of HDSL or four-wire at 2 times the rate.
VDSL	3000 ft (916 m)	16 Mbps	52 Mbps	Few installations.

Table 5-7 compares a number of different WAN technologies, along with the speeds and media types associated with them.

Table 5-7 *Physical Bandwidth Comparison*

Bandwidth	Less Than 2 Mbps	2 Mbps to 45 Mbps	45 Mbps to 100 Mbps	100 Mbps to 10 Gbps
Copper	Serial, ISDN, Frame Relay, TDM, DSL	Frame Relay, Ethernet, DSL, cable, T3	Fast Ethernet	Gigabit Ethernet
Fiber	—	Ethernet	FastEthernet, ATM	Gigabit Ethernet, 10Gigabit Ethernet, ATM, SONET/SDH, POS, dark fiber
Wireless	802.11b	802.11b, wireless WAN (varies)	802.11a/g	802.11n

Q&A

As mentioned in the introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. When using PPDIOO design methodology, what should a network designer do after identifying the customer requirements?
   a. Design the network topology
   b. Design a test network
   c. Plan the implementation
   d. Characterize the existing network
2. Which module within the Enterprise campus connects to the Enterprise Edge module?
   a. Server module
   b. Campus Core
   c. Building Distribution
   d. Remote access/VPN module
3. What WAN technology is most cost effective and suitable for the telecommuter?
   a. MPLS
   b. Dark fiber
   c. ISDN
   d. DSL
4. What two modules are found in the Enterprise Edge?
   a. Campus Core
   b. Building Access
   c. Internet
   d. MAN/WAN

5. Which of the following statements best describes window size for good throughput?
   a. A large window size reduces the number of acknowledgments.
   b. A small window size reduces the number of acknowledgments.
   c. A small window size provides better performance.
   d. None of the above
6. What is the default queuing mechanism for router interfaces below 2.0 Mbps?
   a. Traffic shaping
   b. WFQ
   c. CBWFQ
   d. LLQ
7. Which of the following best describes the PPDIOO design methodology? (Select three.)
   a. Analyze the network requirements
   b. Characterize the existing network
   c. Implement the network management
   d. Design the network topology
8. Which of the following modules belongs in the Enterprise Edge?
   a. Building Distribution
   b. Campus Core
   c. Network Management
   d. DMZ/E-commerce
9. Which network modules connect to ISPs in the Enterprise Edge? (Select two.)
   a. Building Distribution
   b. Campus Core
   c. Internet
   d. DMZ/E-commerce
10. Which Enterprise Edge network module(s) connect(s) using the PSTN connectivity?
   a. Remote Access/VPN
   b. Campus Core
   c. Building Access
   d. DMZ/E-commerce

11. Which Enterprise Edge network module(s) connect(s) using Frame Relay and ATM?
    a. Remote Access/VPN
    b. WAN/MAN
    c. Building Distribution
    d. Server Farm
12. During which part of the PPDIOO design methodology does implementation planning occur?
    a. Analyze the network requirements
    b. Design the topology
    c. Characterize the existing network
    d. None of the above
13. What functional area provides connectivity between the central site and remote sites?
    a. DMZ/E-commerce
    b. Campus Core
    c. Building Distribution
    d. MAN/WAN
14. What WAN technology allows the enterprise to control framing?
    a. Cable
    b. Wireless
    c. DWDM
    d. Dark fiber
15. Which QoS method uses a strict PQ in addition to modular traffic classes?
    a. CBWFQ
    b. Policing
    c. WFQ
    d. LLQ
16. A T1 TDM circuit uses how many timeslots?
17. True or false: ISDN uses LMI for its signaling protocol.
18. True or false: DSL technology is analog technology over coaxial cable.
19. True or false: SONET/SDH supports automated recovery and self-healing mechanisms.
20. True or false: The DE bit set to 0 on a frame indicates to the Frame Relay network that this frame can be dropped.

21. Which wireless implementation is designed to connect two wireless networks in different buildings?
    a. Mobile wireless
    b. GPRS
    c. Bridge wireless
    d. UMTS
22. What improves the utilization of optical fiber strands?
23. On the ISP side of a cable provider, cable modems connect to what system?
24. If Frame Relay, ATM, and SONET technologies are used, what Enterprise Edge network module would they connect to?
    a. WAN/MAN
    b. VPN/Remote Access
    c. Internet
    d. DMZ/E-commerce
25. True or false: Network design requirements are driven by two primary goals: application availability and cost of investment/usage.
26. True or false: Analog dialup technology is a good backup solution for DSL and cable modem access.
27. True or false: Frame Relay SVCs are used more predominantly than PVCs.
28. True or false: ADSL uses the downstream bandwidth, which is higher than the upstream bandwidth, or asymmetrical.
29. What protocol describes data-over-cable procedures that the equipment must support?

This chapter covers the following subjects:

- Traditional WAN Technologies
- Remote-Access Network Design
- VPN Network Design
- WAN Backup Design
- Layer 3 Tunneling
- Enterprise WAN Architecture
- Enterprise Edge Components
- Enterprise Branch Architecture
- Enterprise Teleworker (Branch of One) Design

CHAPTER 6

WAN Design

This chapter reviews wide-area network (WAN) designs for the Enterprise WAN and Enterprise Branch. Expect plenty of questions on both architectures. The CCDA must understand WAN architectures and what makes them different from each other. This chapter also covers hardware and software selections used in WAN design.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 6-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 6-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Traditional WAN Technologies	1
Remote-Access Network Design	2
VPN Network Design	3
WAN Backup Design	4
Layer 3 Tunneling	—
Enterprise WAN Architecture	5, 6
Enterprise Edge Components	7
Enterprise Branch Architecture	8
Enterprise Teleworker (Branch of One) Design	9, 10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. Which of the following are examples of packet- and cell-switched technologies used in the Enterprise Edge?
   a. Frame Relay and ATM
   b. ISDN and T1
   c. Cable and DSL
   d. Analog voice and T1
2. Typical remote-access network requirements include which of the following? (Select all that apply.)
   a. Best-effort interactive and low-volume traffic patterns
   b. Voice and VPN support
   c. Connections to the Enterprise Edge using Layer 2 WAN technologies
   d. Connecting the server farm to the campus core
3. Which VPN infrastructure is used for business partner connectivity and uses the Internet or a private infrastructure?
   a. Access VPN
   b. Intranet VPN
   c. Extranet VPN
   d. Self-deployed MPLS VPN
4. What backup option allows for both a backup link and load-sharing capabilities using the available bandwidth?
   a. Dial backup
   b. Secondary WAN link
   c. Shadow PVC
   d. Dial-on-demand routing

5. Which common factor is used for WAN architecture selection that involves eliminating single points of failure to increase uptime and growth?

   a. Network segmentation

   b. Ease of management

   c. Redundancy

   d. Support for growth

6. What WAN/MAN architecture is provided by the service provider and has excellent growth support and high availability?

   a. Private WAN

   b. ISP service

   c. SP MPLS/IP VPN

   d. Private MPLS

7. Which Cisco IOS software family has been designed for the Enterprise Core and the SP edge?

   a. IOS T Releases 12.3, 12.4, 12.3T, and 12.4T

   b. IOS S Releases 12.2SB and 12.2SR

   c. IOS XR

   d. IOS SX

8. When designing Enterprise Branch Architecture using the SONA framework, which of the following are common network components? (Select all that apply.)

   a. Routers supporting WAN edge connectivity

   b. Switches providing the Ethernet LAN infrastructure

   c. Network management servers

   d. IP phones

9. Which design supports 50 to 100 users and provides Layer 3 redundancy features?

   a. Single-tier

   b. Dual-tier

   c. Multi-tier

   d. Branch of One

10. Which branch profile supports 100 to 1000 users, dual routers, dual ASAs, and multilayer switches, including the aggregation of the access layer switch connections?

    a. Single-tier
    b. Dual-tier
    c. Multi-tier
    d. Branch of One

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers WAN design topics that you need to master for the CCDA exam. It begins by discussing physical WAN technology and WAN topologies used in the Enterprise Edge. Next is a review of typical remote-access requirements used to design remote-access networks. The chapter goes on to cover the specifics of VPN design and connectivity options available for VPNs.

This chapter also describes the backup strategies used when designing WANs. Then it covers the considerations used in developing WAN architectures. This chapter discusses the hardware and software options used when selecting components for your network design. A section then covers the framework used in designing branch offices. This chapter ends with a review of several options for designing different sizes of branch offices.

Traditional WAN Technologies

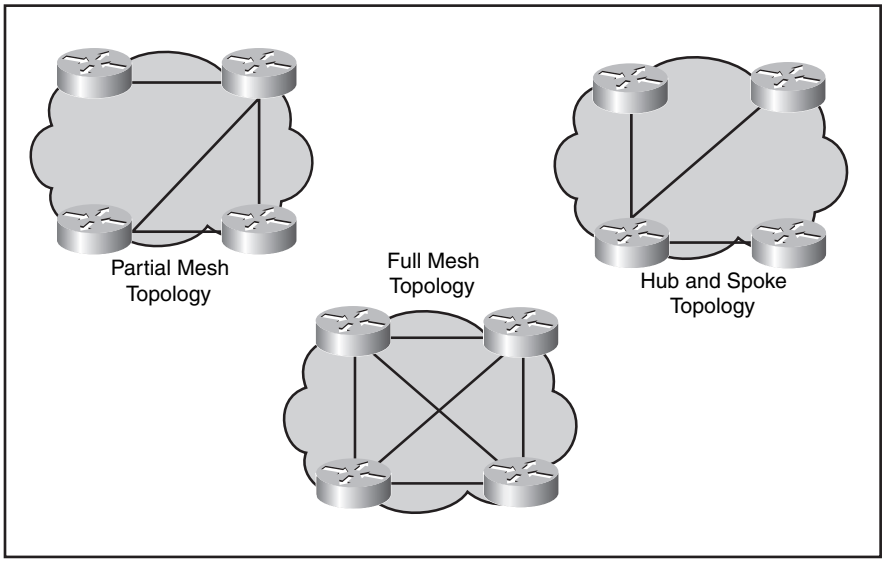
When selecting a particular WAN technology, you should be familiar with the three major categories that represent traditional WANs:

- **Circuit-switched**—Data connections that can be brought up when needed and terminated when finished. Examples include ordinary PSTN phone service, analog modems, and ISDN. Carriers reserve that call path through the network for the duration of the call.
- **Leased lines**—A dedicated connection provided by the service provider. These types of connections are point-to-point and generally more expensive. TDM-based leased lines usually use synchronous data transmission.
- **Packet- and cell-switched**—Connections that use virtual circuits (PVC/SVC) established by the service provider. Packet-switched technologies include Frame Relay and cell-switched technologies such as ATM. The virtual circuits are part of the shared ATM/Frame Relay service provider backbone network. This gives the service provider greater flexibility with its service offerings.

WAN Topologies

When designing a WAN, you should become familiar with the basic design approaches for packet-switched networks. These approaches include hub-and-spoke, partial-mesh, and full-mesh topologies, as shown in Figure 6-1.

Figure 6-1 *WAN Topologies*



Hub-and-Spoke Topology

A star or hub-and-spoke topology provides a hub router with connections to the spoke routers through the WAN cloud. Network communication between the sites flows through the hub router. Significant WAN cost savings and simplified management are benefits of the hub-and-spoke topology. Hub and spoke topologies also tend to be the most popular WAN topologies.

A major disadvantage of this approach is that the hub router represents a single point of failure. The hub-and-spoke topology limits overall performance when accessing resources at the central hub router from the spoke routers, which affects scalability.

Full-Mesh Topology

With full-mesh topologies, each site has a connection to all other sites in the WAN cloud (any-to-any). As the number of sites grows, so does the number of spoke connections needed. Consequently, the full-mesh topology is not viable in very large networks. However, a key advantage of this topology is that it has plenty of redundancy in the event of network failures. But redundancy implemented with this approach does have a high price associated with it.

Here are some issues inherent with full-mesh topologies:

- Many virtual circuits (VCs) are required to maintain the full mesh
- Issues occur with duplication of packets for each site

- Complex configurations are needed
- High cost

Partial-Mesh Topology

A partial-mesh topology has fewer VC connections than a full-mesh topology. Therefore, not all sites in the cloud are required to be connected to each other. However, some sites on the WAN cloud have full-mesh characteristics. Partial-mesh topologies can give you more options and flexibly as far as where you may want to place the high-redundancy VCs given your specific requirements.

Remote-Access Network Design

When designing remote-access networks, the goal is to provide a unified solution that allows for seamless connectivity as if the users are on site. Connection requirements drive the technology selection process. It is important to analyze the application and network requirements in addition to reviewing the available service provider options.

The following summarizes typical remote-access requirements:

- Best-effort interactive and low-volume traffic patterns
- Connections to the Enterprise Edge using Layer 2 WAN technologies (consider capital and recurring costs)
- Voice and VPN support

Remote-access network connections are enabled over permanent always-on connections or dial-on-demand connections:

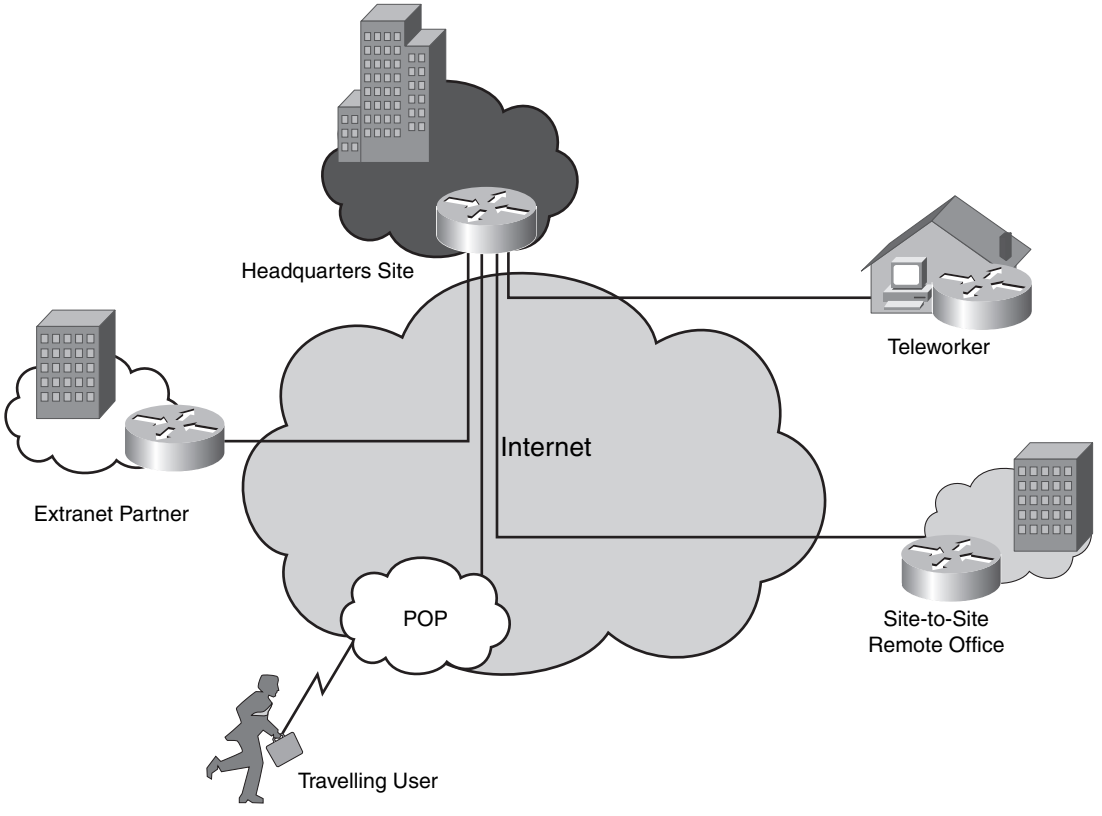
- Dialup analog, ISDN (dial-on-demand)
- DSL, cable, wireless hotspot (permanent)

VPN Network Design

Virtual private networks typically are deployed over some kind of shared infrastructure. VPNs are similar to tunnels in that they carry traffic over an existing IP infrastructure. VPN infrastructures include the Internet, ATM/Frame Relay WANs, and point-to-point connected IP infrastructures. A disadvantage of using VPNs over public networks is that the connectivity is best-effort in nature and troubleshooting is also very difficult because you don't have visibility into the service provider's infrastructure.

Figure 6-2 shows VPN connectivity options.

Figure 6-2 *VPN Examples*



The three VPN groups are divided by application:

- **Access VPN**—These types of VPN connections give users connectivity over shared networks such as the Internet to their corporate intranets. Users connect remotely using dialup, ISDN, Cable/DSL, or via wireless hotspots. Remote network connectivity into the corporate network over the Internet is typically outsourced to an ISP, and the VPN clients are supported by the internal help desk. Two architectural options are used to initiate the VPN connections: client-initiated or network access server (NAS)-initiated VPN connections. Client-initiated VPN connections let users establish IPsec encrypted sessions over the Internet to the corporate VPN terminating device. NAS-initiated VPN connections are where users first connect to the NAS and then the NAS sets up a VPN tunnel to the corporate network.

- **Intranet VPN**—Intranet VPNs or site-to-site VPNs connect remote offices to the headend offices. Generally, the remote sites use their Internet connection to establish the VPN connection back to the corporate headend office. But they could use a VPN tunnel over an IP backbone provided by the service provider. The main benefits of intranet VPNs are reduced WAN infrastructure, lower WAN charges, and reduction in the cost of ownership.
- **Extranet VPN**—VPN infrastructure for business partner connectivity also uses the Internet or a private infrastructure for network access. Keep in mind that it is important to have secure extranet network policies to restrict the business partners' access.

Overlay VPNs

Overlay VPNs are built using traditional WAN technologies such as Frame Relay and ATM. The service provider provides the virtual circuits to enable connectivity between the locations. The underlying network emulates Layer 3 point-to-point links between sites. Secure VPN tunnels are then built over the IP infrastructure using Generic Routing Encapsulation (GRE) and IPsec protocols. Because the network is secure, the provider has no visibility into the Layer 3 traffic and provides only the transport services. However, this incurs a higher cost because of the bandwidth and virtual circuits needed at each site.

Virtual Private Dialup Networks

Virtual Private Dialup Networks (VPDN) provide remote network access using tunnels over traditional dialup, ISDN, DSL cable, and wireless network access connections. This method involves the ISP terminating network connections and then forwarding the traffic onto the company's corporate network. Virtual tunnels are used between the company sites and the ISP using Layer 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP) tunnels. Network configuration and security remain under the company's control, not the ISP's.

Peer-to-Peer VPNs

With peer-to-peer VPNs, the service provider plays an active role in enterprise routing. This approach uses modern MPLS VPN technology. Organizations can then use any IP address space, thus avoiding issues with overlapping IP address space. MPLS VPN networks learn routing information from normal IP routing sources; however, they use an additional label to specify the VPN tunnel and the corresponding VPN destination network.

VPN Benefits

The major benefits of using VPNs are flexibility, cost, and scalability. VPNs are easy to set up and deploy in most cases. VPNs enable network access to remote users, remote sites, and extranet business partners. VPNs lower the cost of ownership by reducing the WAN and dialup recurring monthly charges. The geographic coverage of VPNs is nearly everywhere Internet access is

available, which makes VPNs highly scalable. In addition, VPNs simplify WAN operations because they can be deployed in a consistent manner.

WAN Backup Design

Redundancy is critical in WAN design for the remote site because of the unreliable nature of WAN links. Most Enterprise Edge solutions require high availability between the primary and remote site. Because WAN links have lower reliability and lack bandwidth, they are good candidates for most WAN backup designs.

Branch offices should have some type of backup strategy in the event of a primary link failure. Backup links can be either dialup or permanent connections.

WAN backup options are as follows:

- **Dial backup**—ISDN provides backup dialup services in the event of a primary failure of a WAN circuit. The backup link is initiated if a failure occurs with the primary link. The ISDN backup link provides network continuity until the primary link is restored, and then the backup link is terminated such as with floating static route techniques.
- **Secondary WAN link**—The addition of a secondary WAN link makes the network more fault-tolerant. This solution offers two key advantages:
  - Backup link—Provides for network connectivity if the primary link fails. Dynamic or static routing techniques can be used to provide routing consistency during backup events. Application availability can also be increased because of the additional backup link.
  - Additional bandwidth—Load sharing allows both links to be used at the same time, increasing the available bandwidth. Load balancing can be achieved over the parallel links using automatic routing protocol techniques.
- **Shadow PVC**—Service providers can offer shadow PVCs, which provide additional PVCs for use if needed. The customer is not charged for the PVC if it does not exceed limits set by the provider while the primary PVC is available. If the limit is exceeded, the service provider charges the customer accordingly.

Load-Balancing Guidelines

Load balancing can be implemented per packet or per destination using fast switching. If WAN links are less than 56 kbps, per-packet load balancing is preferred. Fast switching is enabled on WAN links that are faster than 56 kbps, and per-destination load balancing is preferred.

A major disadvantage of using duplicate WAN links is cost. Duplicate WAN links require additional WAN circuits for each location, and more network interfaces are required to terminate the connections. However, the loss of productivity if a site loses network connectivity and becomes isolated can be greater than the cost of the duplicate WAN link.

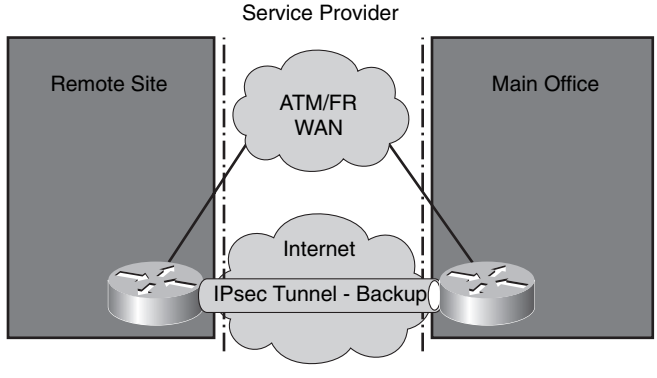
WAN Backup over the Internet

Another alternative for WAN backup is to use the Internet as the connectivity transport between sites. However, keep in mind that this type of connection does not support bandwidth guarantees. The enterprise also needs to work closely with the ISP to set up the tunnels and advertise the company's networks internally so that remote offices have reachable IP destinations.

Security is of great importance when you rely on the Internet for network connectivity, so a secure tunnel using IPsec needs to be deployed to protect the data during transport.

Figure 6-3 illustrates connectivity between the headend or central site and a remote site using traditional ATM/FR connections for the primary WAN link. The IPsec tunnel is a backup tunnel that provides redundancy for the site if the primary WAN link fails.

Figure 6-3 *WAN Backup over the Internet*



IPsec tunnels are configured between the source and destination routers using tunnel interfaces. Packets that are destined for the tunnel have the standard formatted IP header. IP packets that are forwarded across the tunnel need an additional GRE/IPsec header placed on them as well. As soon as the packets have the required headers, they are placed on the tunnel with a destination address of the tunnel endpoint. After the packets cross the tunnel and arrive on the far end, the GRE/IPsec headers are removed. The packets are then forwarded normally using the original IP packet headers.

Layer 3 Tunneling

Two methods exist for tunneling private networks over a public IP network:

- **Generic Routing Encapsulation (GRE)**—Developed by Cisco to encapsulate a variety of protocols inside IP tunnels. This approach is simple for basic IP VPNs but lacks in security and scalability. In fact, GRE tunnels do not use any encryption to secure the packets during transport.
- **IP Security (IPsec)**—IPsec provides secure transmission of data over unsecured networks such as the Internet. IPsec operates in either tunnel mode or transport mode. Packet payloads can be encrypted, and IPsec receivers can authenticate packets' origin. Internet Key Exchange (IKE) and Public-Key Infrastructure (PKI) can also be used with IPsec. IKE is the protocol used to set up a security association (SA) with IPsec. PKI is an arrangement that provides for third-party verification of identities.

Enterprise WAN Architecture

When selecting an enterprise WAN architecture, you should identify and understand the connectivity and business requirements. It is important to review sample network designs that could meet the identified requirements. Here are some common factors that influence decisions for WAN architecture selection:

- **High availability**—Most businesses need a high level of availability, especially for their critical applications. The goal of high availability is to remove the single points of failure in the design, either by software, hardware, or power. Redundancy is critical in providing high levels of availability. Some technologies have built-in techniques that enable them to be highly available. For technologies that do not, other techniques can be employed, such as using additional WAN circuits and/or backup power supplies.
- **Support for growth**—Often enterprises want to provide for growth in their WAN architectures, considering the amount of effort and time required to connect additional sites. High-growth WAN technologies can reduce the amount of effort and cost involved in network expansions. WAN technologies that do not provide growth require significantly more effort, time, and cost to add new branches or remote offices.
- **Ongoing expenses**—Private line and traditional ATM/Frame Relay tend to have higher recurring expenses than Internet-based IP VPNs. Public networks such as the Internet can be used for WAN services to reduce cost, but there are some trade-offs with reliability and security compared to private or ATM/Frame Relay-type transports. Moreover, public networks make it more difficult to provide advanced technologies such as real-time voice and video.

- **Ease of management**—The expertise of the technical staff who are required to maintain and support MAN and WAN technologies varies. Most enterprises have the internal IT knowledge to handle most traditional MAN and WAN upgrades without the need for much training. However, some of the advanced technologies usually reserved for service providers may require additional training for the IT staff if the support is brought in-house. Depending on the technology and the design, you have opportunities to reduce the complexity through network management.

- **Cost to implement**—In most cases, the implementation cost is a major concern. During the design process it is important to evaluate the initial and recurring costs along with the design's benefits. Sometimes an organization can migrate from legacy connectivity to new technology with minimal investment in terms of equipment, time, and resources. In other cases, a network migration can require a low initial cost in terms of equipment and resources but can provide recurring operational savings and greater flexibility over the long term.

- **Network segmentation support**—Segmentation provides for Layer 2/3 logical separation between networks instead of physically separate networks. Advantages include reduced costs associated with equipment, maintenance, and carrier charges. In addition, separate security polices can be implemented per department or by functional area of the network to restrict access as needed.

- **Support for Voice and Video**—There is an increased demand for the support of voice over MAN and WAN technologies. Some WAN providers offer Cisco QoS-Certified IP VPNs, which can provide the appropriate levels of QoS needed for voice and video deployments. In cases where Internet or public network connections are used, QoS cannot always be assured. When voice and video are required for small offices, teleworkers, or remote agents, 768 kbps upstream bandwidth or greater is recommended.

Cisco Enterprise MAN/WAN

The Cisco Enterprise MAN/WAN architecture uses several technologies that work together in a cohesive relationship.

Here is the list of Cisco Enterprise MAN/WAN architectures:

- Private WAN (optional encryption)
- Private WAN with self-deployed MPLS
- ISP service (Internet with site-to-site and remote-access VPN)
- Service provider-managed IP/MPLS VPN

These architectures provide integrated QoS, security, reliability, and ease of management that is required to support enterprise business applications and services. As you can see, alternative technologies to the traditional private WAN can allow for network growth and reduced monthly carrier charges.

Enterprise WAN/MAN Architecture Comparison

Enterprise WAN/MAN architectures have common characteristics that allow the network designer to compare the advantages and disadvantages of each approach. Table 6-2 compares the characteristics of Private WAN, ISP Service, SP MPLS/IP VPN, and Private MPLS architectures.

Table 6-2 *WAN/MAN Architecture Comparison*

Characteristic	Private WAN	ISP Service	SP MPLS/ IP VPN	Private MPLS
High availability	Excellent	Good	Excellent	Excellent
Growth support	Moderate	Good	Excellent	Excellent
Security	IPsec (optional)	IPsec (mandatory)	IPsec (optional)	IPsec (optional)
Ongoing expenses	High	Low	Moderate to high	Moderate to high
Ease of management	High	Medium	Medium	High
Voice/video support	Excellent	Moderate	Excellent	Excellent
Effort to migrate from private WAN	Low	Moderate	Moderate	High

The Cisco Enterprise MAN/WAN architecture includes Private WAN, ISP Service, SP MPLS/IP VPN, and Private MPLS:

- **Private WAN** generally consists of Frame Relay, ATM, private lines, and other traditional WAN connections. If security is needed, private WAN connections can be used in conjunction with encryption protocols such as Digital Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). This technology is best suited for an enterprise with moderate growth outlook where some remote or branch offices will need to be connected in the future. Businesses that require secure and reliable connectivity to comply with IT privacy standards can benefit from IPsec encrypted connectivity over the private WAN. Disadvantages of private WANs are that they have high recurring costs from the carriers and they are not the preferred technology for teleworkers and remote call center agents. Some enterprises may use encryption on the network, connecting larger sites and omitting encryption on the smaller remote offices with IP VPNs.

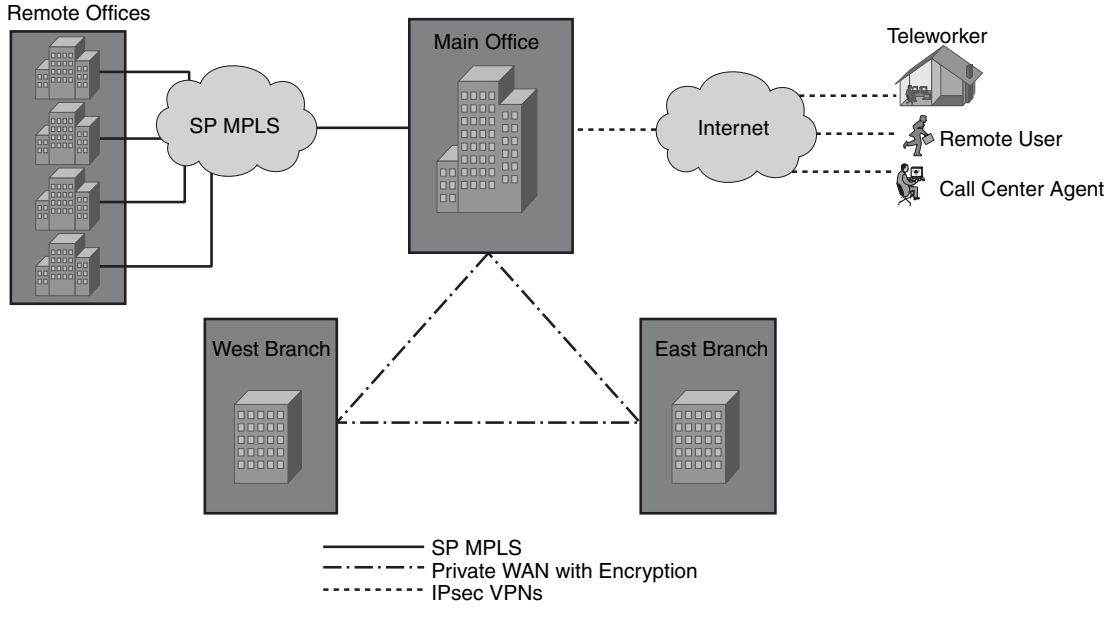
- **ISP Service (Internet with site-to-site and remote-access VPN)** uses strong encryption standards such as DES, 3DES, and AES, which make this WAN option more secure than the private WAN. ISP service also provides compliance with many new information security regulations imposed on some industries, such as healthcare and finance. This technology is best suited for basic connectivity over the Internet. However, if you need to support voice and video, consider IPsec VPN solutions that have the desired QoS support needed to meet your network requirements. The cost of this technology is relatively low. It is useful for connecting large numbers of teleworkers, remote contact agents, and remote offices.

- **SP MPLS/IP VPN** is similar to private WAN technology, but with added scalability and flexibility. MPLS-enabled IP VPNs enable mesh-like behavior or any-to-any branch-type connectivity. SP MPLS networks can support enterprise QoS requirements for voice and video, especially those with high growth potential. SP MPLS features secure and reliable technology with generally lower carrier fees. This makes it a good option for connecting branch offices, teleworkers, and remote call center agents.

- **Private WAN with self-deployed MPLS** usually is reserved for very large enterprises that are willing to make substantial investments in equipment and training to build out the MPLS network. The IT staff needs to be well trained and comfortable with supporting complex networks.

Figure 6-4 illustrates SP MPLS, Private WAN with encryption, and IPsec VPNs WAN architectures.

Figure 6-4 *WAN Architectures*



Enterprise Edge Components

When selecting Enterprise Edge hardware and software, you must keep in mind several considerations. Here are some factors to examine during the selection process:

- Hardware selection involves the data link functions and features offered by the device. Considerations include the following:
  - Port density
  - Types of ports supported
  - Modularity (add-on hardware)
  - Backplane and packet throughput
  - Redundancy (CPU and/or power)
  - Expandability for future use
- Software selection focuses on the network performance and the feature sets included in the software. Here are some factors to consider:
  - Forwarding decisions
  - Technology feature support
  - Bandwidth optimization
  - Security vulnerabilities
  - Software issues

Hardware Selection

When evaluating hardware, use the Cisco documentation online to research hardware and determine the equipment's capabilities. Remember to consider the port densities and types of ports the device offers. In addition, other factors to investigate include modularity, packet throughput, redundancy capabilities, and the device's expandability. Finally, keep in mind what power options the hardware supports.

Software Selection

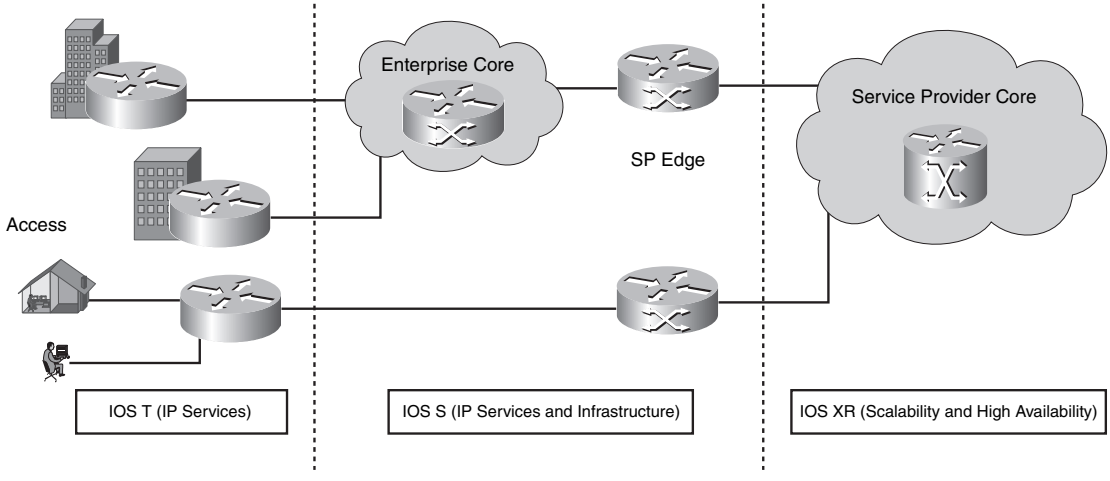
The architecture of Cisco IOS software is designed to meet the requirements of different markets (enterprise, SP, and commercial) and divisions of the network, such as the access, core, distribution, and edge. The Cisco IOS software family consists of IOS T (access), IOS S (Enterprise core, SP edge), and IOS XR (SP Core).

Cisco IOS T supports advanced technology business solutions aimed at access, wireless, data center, security, and Unified Communications (UC). Cisco IOS S focuses on high-end enterprise cores, service provider edge networks, VPNs (MPLS, Layer 2/Layer 3), video, and multicast. Cisco IOS XR is suited for large-scale networks within the service provider core that offer high availability and in-service software upgrades.

The IOS Software families share a common base of technologies. Most of the T family features are also available in the IOS S and IOS XR families.

Figure 6-5 illustrates each of the Cisco IOS software families and where they reside in relationship to each other within the different markets.

Figure 6-5 *Cisco IOS Software Families*



Cisco IOS Packaging

Cisco IOS packaging involves consolidating and organizing the IOS software using consistent and standardized naming across all router platforms. The four base service categories are as follows:

- **IP Base**—Entry-level IOS supporting IP data
- **IP Voice**—Supports converged voice and data
- **Advanced Security**—Security features and VPN
- **Enterprise Base**—Enterprise Layer 3 protocols and IBM support

In addition, three additional premium packages offer new IOS software features that focus on more complex networking environments:

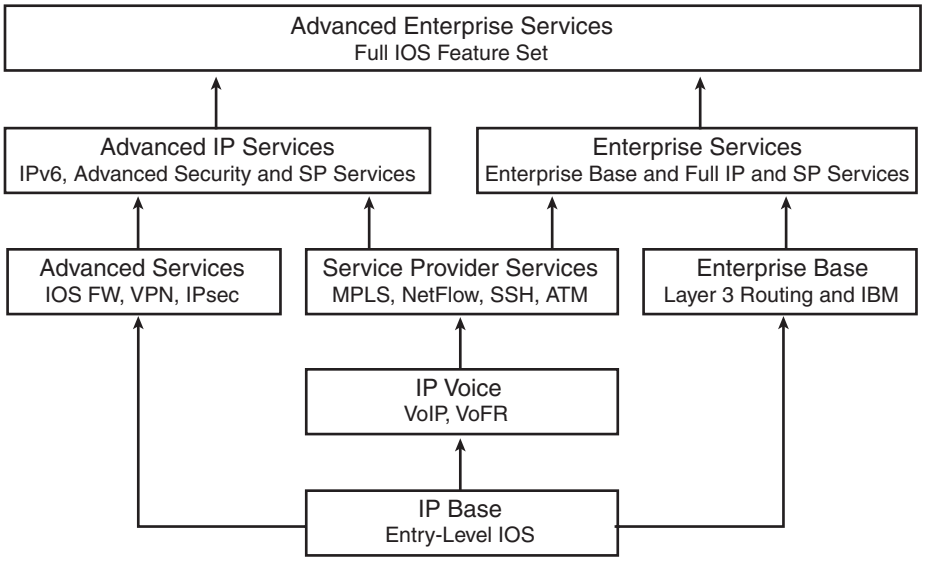
- **SP Services**—Adds features such as MPLS, ATM, SSH, and NetFlow to the lower IP Voice package
- **Advanced IP Services**—Adds support for IPv6 and the features of both the Advanced Security and SP services packages
- **Enterprise Services**—Adds full IBM support and the features of both the Enterprise Base and SP services packages

The features of the lower-tier packages are inherited in the higher-tier packages flowing upward.

At the top is the premium package, Advanced Enterprise Services. It combines all features and supports all routing protocols with voice, security, and VPN technologies.

Figure 6-6 shows the Cisco IOS packaging and how IOS features are inherited.

Figure 6-6 *Cisco IOS Packaging*



Inheritance of IOS features from one IOS to the next higher level IOS is an important aspect of Cisco IOS packaging. Therefore, as soon as a feature is introduced to an IOS package, it is maintained during upgrades to higher-level IOS packages.

Table 6-3 illustrates the major features and inheritance available with IOS packages.

Table 6-3 *IOS Package Comparison*

Feature Set	IP Data	VoIP, VoFR	ATM, MPLS	AppleTalk, IPX, IBM	Firewall, IDS, VPN
IP Base	×				
IP Voice	×	×			
Advanced Security	×				×
SP Services	×	×	×		
Enterprise Base	×			×	
Advanced IP Services	×	×	×		×
Enterprise Services	×	×	×	×	
Advanced Enterprise Services	×	×	×	×	×

Comparing Hardware and Software

Table 6-4 compares the Cisco router and switch hardware platforms and their associated software families, releases, and functional descriptions.

Table 6-4 *Cisco Router/Switch Platform and Software Comparison*

Router/Switch Hardware	Software	Description
800, 1800, 2800, 3800, 7200	Cisco IOS T Releases 12.3, 12.4, 12.3T, and 12.4T	Access routing platforms supporting fast and scalable delivery of data for enterprise applications.
7x00, 10000	Cisco IOS S Release 12.2SB	Delivers midrange routing services for the Enterprise and SP edge networks.
7600	Cisco IOS S Release 12.2SR	Delivers high-end LAN switching for Enterprise access, distribution, core, and data center. Also supports Metro Ethernet for the SP edge.
12000, CRS-1	Cisco IOS XR	High availability, providing large scalability and flexibility for the SP core and edge.
2970, 3560, 3750	Cisco IOS S Release 12.2SE	Provides low-end to midrange LAN switching for Enterprise access and distribution deployments.

continues

Table 6-4 *Cisco Router/Switch Platform and Software Comparison (Continued)*

Router/Switch Hardware	Software	Description
4500, 4900	Cisco IOS S Release 12.2SG	Provides midrange LAN switching for Enterprise access and distribution in the campus. Also supports Metro Ethernet.
6500	Cisco IOS S Release 12.2SX	Delivers high-end LAN switching for Enterprise access, distribution, core, and data center. Also supports Metro Ethernet for the SP edge.

Enterprise Branch Architecture

Enterprise Branch architectures encompass a wide range of services that customers want to deploy at the edge of the enterprise. These architectures allow for a variety of connection options, and distance typically is not an issue. The services in this architecture give customers new opportunities to increase security, converge their voice and data traffic, improve productivity, and reduce costs.

Cisco Enterprise Branch Architecture is based on Cisco's Service-Oriented Network Architecture (SONA), which includes plug-in modules that provide remote connectivity to network endpoints. The Enterprise Architecture is a flexible and secure framework for extending headend application functionality to the remote site. Common network components that use the SONA framework for the branch include

- Routers supporting the WAN edge connectivity
- Switches providing the Ethernet LAN infrastructure
- Security appliances securing the branch devices
- Wireless APs allowing for roaming mobility
- Call processing providing Unified Communications and video support
- IP phones and PCs for the end-user devices

Branch Design

It is important to characterize the existing network and gather requirements to develop a suitable design for the branch.

Here are some questions you should ask:

- How many locations and existing devices are there (network devices, servers, users)?
- What amount of scalability and growth is expected?
- What level of high availability and/or redundancy is required?
- Is specific server or network protocol support needed?
- Will the network management and/or support be centralized or distributed?
- Are there any network segmentation restrictions, such as DMZ or internal networks versus external networks?
- Will wireless services be needed, and to what extent?
- What is the estimated budget for the branch design?

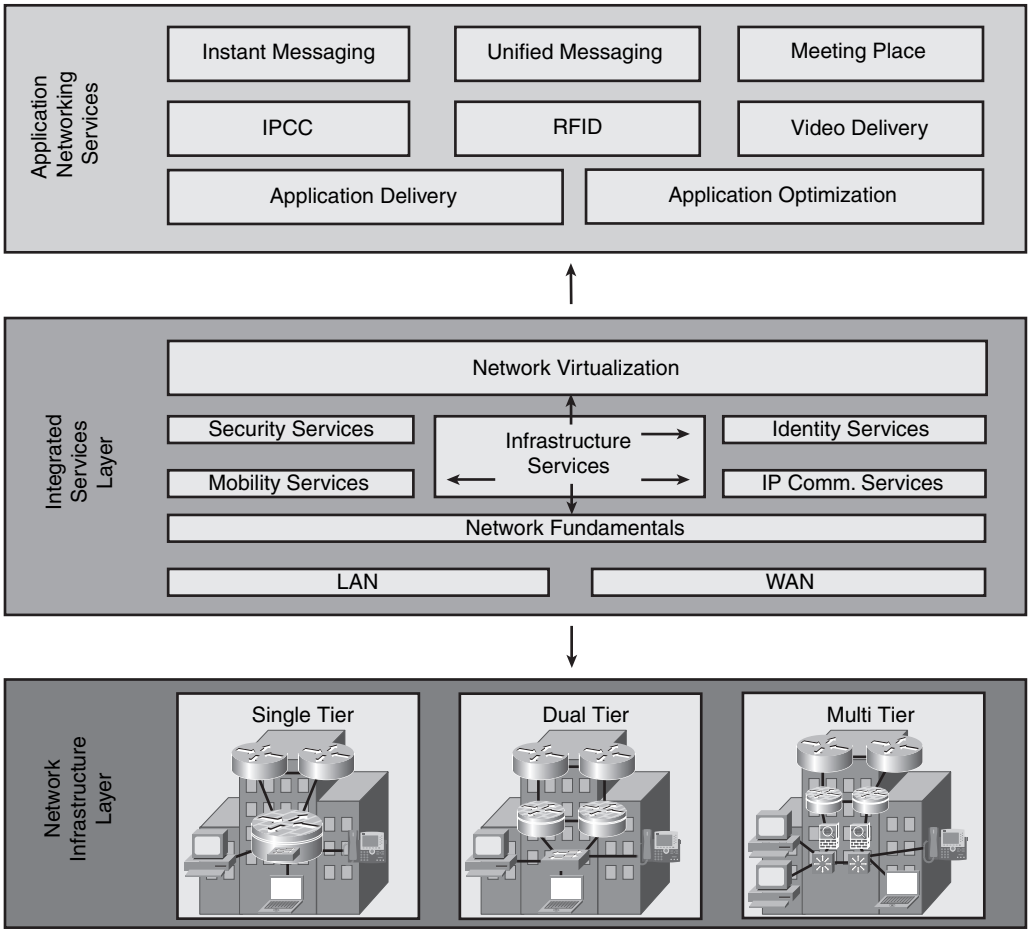
Enterprise Branch Profiles

The SONA framework has three profiles for the Enterprise Branch. They are based on the number of users located at the branch. The profiles are not intended to be the only architectures for branch offices but rather a common set of services that each branch should include. These profiles serve as a basis on which integrated services and application networking are built. The three profiles for the SONA framework enterprise branch are as follows:

- **Single-tier design**—Up to 50 users (small)
- **Dual-tier design**—Between 50 and 100 users (medium)
- **Multi-tier design**—Between 100 and 1000 users (large)

Figure 6-7 shows the three Enterprise branch profiles and the integrated services layers and application networking services that are provided by the branch infrastructure.

Figure 6-7 *Branch Profiles*



The framework's foundation is the branch profile network infrastructure layer, which includes all the common LAN and WAN components. The integrated services layer is built on top of the infrastructure layer and is composed of security, mobility, UC, and identity services. The application networking services are built above the integrated services layer, which organizes the applications services, such as IM, UCC, unified messaging, video delivery, and application delivery services.

Requirements such as high availability, scalability, and redundancy influence the branch profile selected for a branch office.

To integrate both the WAN edge and LAN infrastructure, an integrated services router (ISR) can be used to provide voice, security, and data services. The integrated services router supports triple-speed interfaces (10/100/1000), high-speed WAN interface cards (HWIC), network modules, and embedded security capabilities.

Single-Tier Design

The single-tier design is recommended for branch offices that do not require hardware redundancy and that have a small user base of up to 50 users. This profile consists of an access router providing WAN services and connections for the LAN services. The access router can connect the Layer 2 switch ports in one of three ways:

- Using an ISR that has an optional EtherSwitch module that provides 16 to 48 Ethernet ports for client connections.
- Trunking to an access switch that aggregates the Ethernet connections and can include support for PoE for IP phones and wireless APs.
- Logical EtherChannel interface between the ISR and the access switches using the EtherSwitch module. The access switches can also provide PoE as needed.

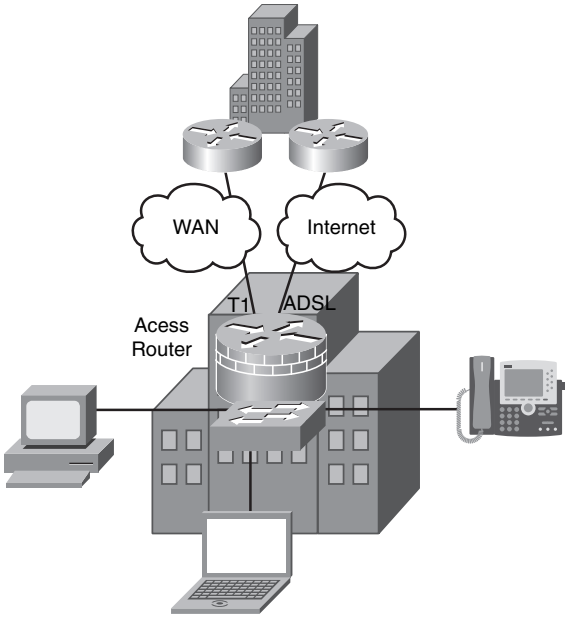
The Layer 3 WAN services are based on the WAN and Internet deployment model. A T1 is used for the primary link, and an ADSL secondary link is used for backup. Other network fundamentals are supported, such as EIGRP, floating static routes, and QoS for bandwidth protection.

The ISR can support the default gateway function and other Layer 3 services such as DHCP, NAT, and IOS Firewall.

The Layer 2 services can be provided by the ISR or access switches such as the 35*x*0 or 3750 series switches. It is recommended that you use Rapid PVST+ for all Layer 2 branch offices where loops are present. Rapid PVST+ ensures a loop-free topology when multiple Layer 2 connections are used for redundancy purposes.

Figure 6-8 illustrates the single-tier branch design connecting back to the corporate office.

Figure 6-8 *Single-Tier Profile (Small Branch)*



Dual-Tier Design

The dual-tier design is recommended for branch offices of 50 to 100 users, with an additional access router in the WAN edge allowing for redundancy services. Typically two 2821 or 2851 routers are used to support the WAN, and separate access switches are used to provide LAN connectivity.

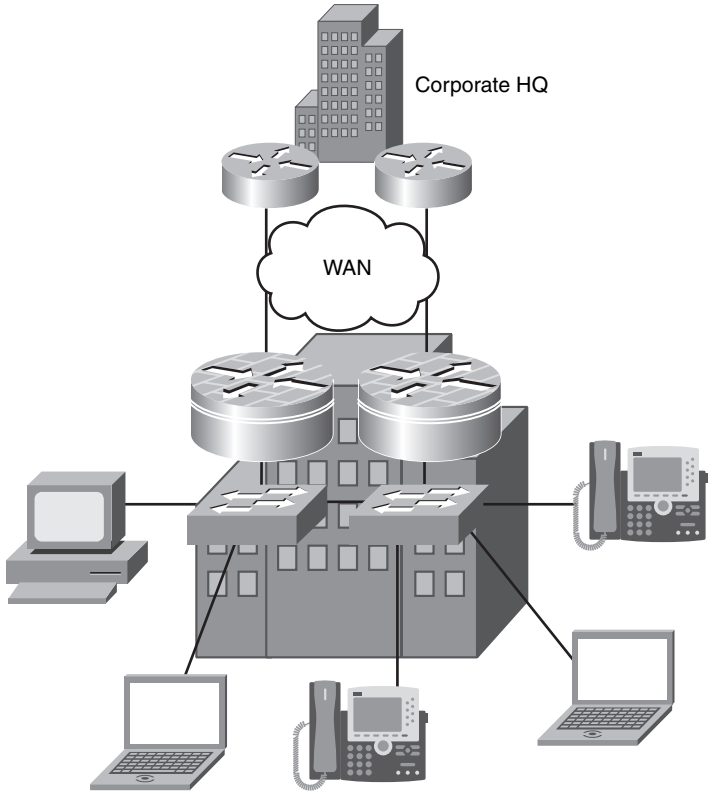
The infrastructure components are dual-access routers, external Layer 2/Layer 3 switches, laptops, desktops, printers, and IP phones. Dual Frame Relay links are used to connect to the corporate offices via both of the access routers.

Layer 3 services such as EIGRP are deployed. Because there are two routers, HSRP or GLBP can be used to provide redundancy gateway services. QoS can also be used to provide guaranteed bandwidth for VoIP, and policing can be used to restrict certain traffic classes from overwhelming the available bandwidth.

The dual-tier design supports using a higher-density external switch or using the EtherSwitch module with the ISR to create trunks to the external access switches. The Cisco Catalyst 3750 series switches have StackWise technology, allowing multiple switches to be connected and managed as one. This also increases the port density available for end-user connections. With Cisco StackWise technology, customers can connect up to nine 3750 series switches using a variety of fiber and copper ports, allowing greater flexibility with the connection options.

Figure 6-9 illustrates the dual-tier branch design using dual routers back to the corporate office.

Figure 6-9 *Dual-Tier Profile (Medium Branch)*



Multi-Tier Design

The multi-tier design is the largest of the branch profiles, supporting between 100 and 1000 users. This design profile is similar to the dual-tier design in that it also provides dual-access routers in the WAN edge. In addition, dual ASAs are used for firewall filtering, and dual distribution switches provide the multilayer switching component. The WAN services use an MPLS deployment model with dual WAN links into the WAN cloud.

Because there are dual routers, the typical redundancy services can also be provided such as EIGRP load balancing and HSRP/GLBP. The ASAs dual configuration allows for ASA failover. QoS services such as shaping and policing can be applied to all the routers and switches as required.

To meet the requirements of the larger user base, a distribution layer of multilayer switches is added to aggregate the connected access switches. A multilayer switch provides the additional

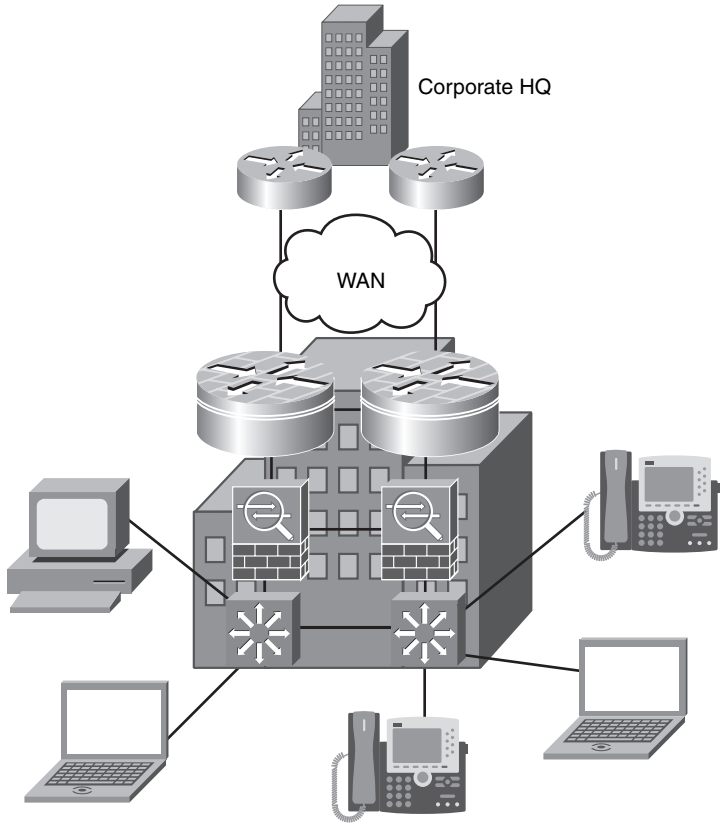
LAN switching capabilities to meet the port density requirements and allowing flexibility to support additional network devices.

A couple of hardware options for this design are the Cisco Catalyst 3750 with StackWise technology or using a modular approach with a Cisco Catalyst 4500. The Cisco 3750 series of switches provide great port densities but do not provide the redundant power without the additional Cisco RPS (external power supply). However, the Cisco 4500 switch platform not only allows for flexibility by adding port densities and interface types but also provides redundant power internally for the entire chassis when using dual power supplies.

If Cisco Catalyst 3560 and 3750 switches are used, additional Layer 2 security features such as dynamic ARP inspection, DHCP snooping, and IP source guard can be used to provide additional security enhancements.

Figure 6-10 illustrates the multi-tier branch design using dual routers, ASAs, and distribution switches.

Figure 6-10 *Multi-Tier Profile (Large Branch)*



Enterprise Teleworker (Branch of One) Design

At the remote edges of the network is another branch office called the Branch of One, also known as Enterprise Teleworkers. Organizations are continually trying to reduce costs and improve their employees' productivity. By working from home, employees can manage their work schedules more effectively and increase their productivity. This also results in greater job satisfaction and flexibility in the employees' work schedule. The work-from-home teleworker is an extension of the enterprise and serves as the basis for the Enterprise Teleworker solution.

Enterprise Teleworkers or the Branch of One needs to be differentiated from the occasional remote worker. The full-time enterprise teleworker has more extensive application access and requirements than the occasional remote worker. Occasionally remote users connect to the corporate network at a hotspot, but generally they do not have the same application demands of an Enterprise teleworker. Typically the Branch of One user connects to his or her local ISP over a cable or DSL connection and uses an analog phone line as a backup.

References and Recommended Readings

"Enterprise Branch Architecture Design Overview," http://www.cisco.com/univercd/cc/td/doc/solution/enbrover.pdf

Module 4, "Designing Remote Connectivity," Designing for Cisco Internetwork Solution Course (DESGN) v2.0

"WAN and MAN Solutions Overview," http://www.cisco.com/en/US/netsol/ns483/networking_solutions_audience_business_benefit0900aecd8033ea26.html

"What is Cisco SONA?," http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c643/cdccont_0900aecd8039b324.pdf

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics covered in this chapter:

- **Circuit-switched**—Data connections that can be brought up when needed and terminated when finished.
- **Leased lines**—A dedicated connection provided by the service provider.
- **Packet and cell-switched**—Connections that use virtual circuits (PVC/SVC) established by the service provider.
- **Hub-and-spoke (or star) topology**—Provides a hub router with connections to the spoke routers through the WAN cloud.
- **Partial-mesh topology**—Has fewer virtual circuit connections than a full-mesh topology.
- **Full-mesh topology**—Requires that each site be connected to every other site in the cloud.
- **Access VPN**—These types of VPN connections give users connectivity over shared networks such as the Internet to the corporate intranet.
- **Intranet (site-to-site) VPN**—Connect remote offices back to the headend office.
- **Extranet VPN**—VPN infrastructure for business partner connectivity that also uses the Internet or a private infrastructure for access.
- **Dial backup**—ISDN provides backup dialup services in the event of a failure of a primary WAN circuit.
- **Secondary WAN link**—The addition of a secondary WAN link makes the network more fault-tolerant.
- **Shadow PVC**—Service providers can offer shadow PVCs that provide an additional PVC for use if needed.
- **Single-tier design**—Up to 50 users (small)
- **Dual-tier design**—Between 50 and 100 users (medium)

- **Multi-tier design**—Between 100 and 1000 users (large)
- **Branch of One**—Enterprise teleworker

Table 6-5 compares the characteristics of private WAN, ISP service, SP MPLS/IP VPN, and private MPLS architectures.

Table 6-5 *WAN/MAN Architecture Comparison*

Characteristic	Private WAN	ISP Service	SP MPLS/IP VPN	Private MPLS
High availability	Excellent	Good	Excellent	Excellent
Growth support	Moderate	Good	Excellent	Excellent
Security	IPsec (optional)	IPsec (mandatory)	IPsec (optional)	IPsec (optional)
Ongoing expenses	High	Low	Moderate to high	Moderate to high
Ease of management	High	Medium	Medium	High
Voice/video support	Excellent	Moderate	Excellent	Excellent
Effort to migrate from private WAN	Low	Moderate	Moderate	High

Table 6-6 illustrates the major features and inheritance available with IOS packages.

Table 6-6 *IOS Package Comparison*

Feature Set	IP Data	VoIP, VoFR	ATM, MPLS	AppleTalk, IPX, IBM	Firewall, IDS, VPN
IP Base	×				
IP Voice	×	×			
Advanced Security	×				×
SP Services	×	×	×		
Enterprise Base	×			×	
Advanced IP Services	×	×	×		×
Enterprise Services	×	×	×	×	
Advanced Enterprise Services	×	×	×	×	×

Table 6-7 compares the Cisco router and switch hardware platforms and their associated software families, releases, and functional descriptions.

Table 6-7 *Cisco Router/Switch Platform and Software Comparison*

Router/Switch Hardware	Software	Description
800, 1800, 2800, 3800, 7200	Cisco IOS T Releases 12.3, 12.4, 12.3T, and 12.4T	Access routing platforms supporting fast and scalable delivery of data for Enterprise applications.
7x00, 10000	Cisco IOS S Release 12.2SB	Delivers midrange routing services for the Enterprise and SP edge networks.
7600	Cisco IOS S Release 12.2SR	Delivers high-end LAN switching for Enterprise access, distribution, core, and data center. Also supports Metro Ethernet for the SP edge.
12000 CRS-1	Cisco IOS XR	High availability, providing large scalability and flexibility for the SP core and edge.
2970, 3560, 3750	Cisco IOS S Release 12.2SE	Provides low-end to midrange LAN switching for Enterprise access and distribution deployments.
4500, 4900	Cisco IOS S Release 12.2SG	Provides midrange LAN switching for Enterprise access and distribution in the campus. Also supports Metro Ethernet.
6500	Cisco IOS S Release 12.2SX	Delivers high-end LAN switching for Enterprise access, distribution, core, and data center. Also supports Metro Ethernet for the SP edge.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What type of WAN technology provides a dedicated connection from the service provider?
   a. Circuit-switched data connection
   b. Leased lines
   c. Packet-switched
   d. Cell-switched
2. What type of topology suffers from a single point of failure?
   a. Hub-and-spoke topology
   b. Full-mesh topology
   c. Partial-mesh topology
   d. None of the above
3. What kind of topology requires that each site be connected to every other site in the cloud?
   a. Hub-and-spoke
   b. Full-mesh
   c. Partial-mesh
   d. All of the above
4. Which WAN technology uses connections that can be brought up when needed, such as ISDN?
   a. Circuit-switched
   b. Leased lines
   c. Packet-switched
   d. Cell-switched

5. Which VPN application gives users connectivity over shared networks?
   a. Intranet VPN
   b. Extranet VPN
   c. Access VPN
   d. None of the above
6. True or false: Overlay VPNs are built using traditional WAN technologies such as Frame Relay and ATM.
7. The service provider plays an active role in enterprise routing with what kind of VPNs?
   a. VPDNs
   b. Peer-to-peer
   c. L2TP
   d. L2F
8. Which backup option provides an additional circuit for use if needed?
   a. Secondary WAN link
   b. Shadow PVC
   c. Dial backup
   d. Load sharing
9. Which WAN backup option uses load sharing in addition to providing backup services?
   a. Dial backup
   b. Shadow PVC
   c. Secondary WAN link
   d. ISDN with DDR
10. True or false: Fast switching is enabled on WAN links that are faster than 56 kbps.
11. True or false: IPsec protects data during transport for WAN backup over the Internet.
12. What two methods are used to enable private networks over public networks?
    a. IPsec
    b. PKI
    c. GRE
    d. PSTN

13. What is not a factor for WAN architecture selection?
    a. Ease of management
    b. Ongoing expenses
    c. Spanning Tree inconsistencies
    d. High availability
14. Which Layer 3 tunneling technique enables basic IP VPNs without encryption?
    a. GRE
    b. IPsec
    c. PKI
    d. IKE
15. True or false: IPsec is optional with a Private WAN architecture.
16. What MAN/WAN architecture uses the Internet with site-to-site VPNs?
    a. Private WAN
    b. ISP Service
    c. SP MPLS/IP VPN
    d. Private WAN with a self-deployed MPLS
17. True or false: Hardware selection involves modularity of add-on hardware but not port densities.
18. True or false: Redundancy but not modularity are key considerations when you're selecting Enterprise Edge hardware.
19. True or false: The Cisco IOS software family IOS T is designed for the SP core.
20. True or false: The Cisco IOS software family IOS T is suited for large networks within the service provider core.
21. What WAN/MAN architecture is usually reserved for very large enterprises that are willing to make substantial investments in equipment and training?
    a. Private WAN
    b. Private WAN with self-deployed MPLS
    c. ISP Service
    d. SP MPLS/IP VPN
22. What entry-level IOS supports IP data?

23. True or false: The premium IOS package is Advanced Enterprise Services.

24. What IOS package supports converged voice and data?

    a. IP Base

    b. Advanced Security

    c. Enterprise Base

    d. IP Voice

25. True or false: The 2970, 3560, and 3750 switches provide low-end to midrange LAN switching for enterprise access and distribution deployments.

26. True or false: Cisco SONA includes plug-in modules for EIGRP and static routing.

27. True or false: Common network components that make up the SONA framework for the branch include IP phones and PCs.

28. Match each Branch profile design with its description:

    a. Single-tier

    b. Dual-tier

    c. Multi-tier

    d. Teleworker

    i. Single-access router

    ii. Cable modem router

    iii. Pair of access routers

    iv. Dual distribution switches

This part covers the following CCDA exam topics (to view the CCDA exam overview, visit http://www.cisco.com/web/learning/le3/current_exams/640-863.html):

- Describe IPv4 and IPv6 Addressing
- Identify Routing Protocol Considerations in an Enterprise Network
- Design a Routing Protocol Deployment

Part III: The Internet Protocol and Routing Protocols

This chapter covers the following subjects:

- IPv4 header
- IPv4 addressing
- IP address subnets
- Address assignment and name resolution

CHAPTER 7

Internet Protocol Version 4

This chapter reviews Internet Protocol Version 4 (IPv4) address structures and IPv4 address types. IPv4 is the version of the protocol that the Internet has used since the initial allocation of IPv4 addresses in 1981. The size of the enterprise indicated the address class that was allocated. This chapter covers the IPv4 header to give you an understanding of IPv4 characteristics. The mid-1990s saw the implementation of classless interdomain routing (CIDR), network address translation (NAT), and private address space to prevent the apparent exhaustion of IPv4 address space. Companies implement variable-length subnet masks (VLSM) in their networks to provide intelligent address assignment and summarization. The CCDA needs to understand all these concepts to design IPv4 addressing for a network.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 7-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 7-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
IPv4 Header	4, 10
IPv4 Addressing	1, 5, 9
IPv4 Address Subnets	2, 3, 7
Address Assignment and Name Resolution	6, 8

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following addresses is an IPv4 private address?
   a. 198.176.1.1
   b. 172.3116.1.1
   c. 191.168.1.1
   d. 224.130.1.1
2. How many IP addresses are available for hosts in the subnet 198.10.100.64/27?
   a. 14
   b. 30
   c. 62
   d. 126
3. What subnet mask should you use in loopback addresses?
   a. 255.255.255.252
   b. 255.255.255.254
   c. 255.255.255.0
   d. 255.255.255.255
4. In what IPv4 field are the precedence bits located?
   a. IP destination address
   b. IP protocol field
   c. Type-of-service field
   d. IP options field
5. What type of address is 225.10.1.1?
   a. Unicast
   b. Multicast
   c. Broadcast
   d. Anycast

6. What protocol maps IPv4 addresses to MAC addresses?
   a. Domain Name System (DNS)
   b. Address Resolution Protocol (ARP)
   c. Neighbor discovery (ND)
   d. Static
7. What is a recommended subnet mask to use in point-to-point WAN links?
   a. 255.255.255.0
   b. 255.255.255.255
   c. 255.255.255.224
   d. 255.255.255.252
8. What is DHCP?
   a. Dynamic Host Control Protocol
   b. Dedicated Host Configuration Protocol
   c. Dynamic Host Configuration Protocol
   d. Predecessor to BOOTP
9. What is the purpose of NAT?
   a. To translate source addresses to destination addresses
   b. To translate between private and public addresses
   c. To translate destination addresses to source addresses
   d. To translate class of service (CoS) to quality of service (QoS)
10. The DS field of DSCP is capable of how many codepoints?
   a. 8
   b. 32
   c. 64
   d. 128

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter reviews IPv4 headers, address classes, and assignment methods.

IP is the network-layer protocol in TCP/IP. It contains logical addressing and information for routing packets throughout the internetwork. IP is described in RFC 791, which was prepared for the Defense Advanced Research Projects Agency (DARPA) in September 1981.

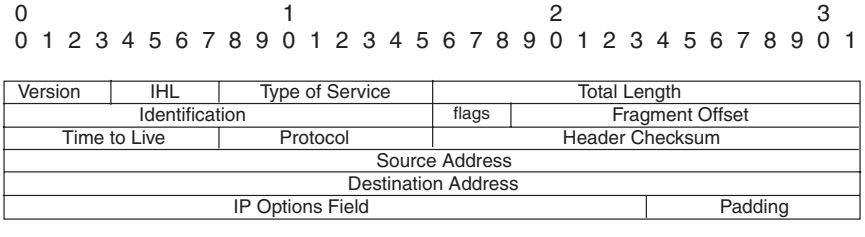
IP provides for the transmission of blocks of data, called datagrams or packets, from a source to a destination. The sources and destinations are identified by 32-bit IP addresses. The source and destination devices are workstations, servers, printers, and routers. The CCDA candidate must understand IPv4 logical address classes and assignment. The IPv4 protocol also provides for the fragmentation and reassembly of large packets for transport over networks with small maximum transmission units (MTU). The CCDA candidate must have a good understanding of this packet fragmentation and reassembly.

Appendix B, "The OSI Reference Model, TCP/IP Architecture, and Numeric Conversion," provides an overview of the TCP/IP architecture and how it compares with the OSI model. It also reviews binary numbers and numeric conversion (to decimal), which is a skill needed to understand IP addresses and subnetting.

IPv4 Header

The best way to understand IPv4 is to know the IPv4 header and all its fields. Segments from TCP or the User Datagram Protocol (UDP) are passed on to IP for processing. The IP header is appended to the TCP or UDP segment. The TCP or UDP segment then becomes the IP data. The IPv4 header is 20 bytes in length when it uses no optional fields. The IP header includes the addresses of the sending host and destination host. It also includes the upper-layer protocol, a field for prioritization, and a field for fragmentation. Figure 7-1 shows the IP header format.

Figure 7-1 *IP Header*



The following is a description of each field in the IP header:

- **Version**—This field is 4 bits in length. It indicates the IP header's format, based on the version number. Version 4 is the current version; therefore, this field is set to 0100 (4 in binary) for IPv4 packets. This field is set to 0110 (6 in binary) in IPv6 networks.

- **IHL**—Internet header length. This field is 4 bits in length. It indicates the length of the header in 32-bit words (4 bytes) so that the beginning of the data can be found in the IP header. The minimum value for a valid header (five 32-bit words) is 5 (0101).
- **ToS**—Type of Service. This field is 8 bits in length. Quality of Service (QoS) parameters such as IP precedence or DSCP are found in this field. These are explained further in this chapter.
- **Total length**—This field is 16 bits in length. It represents the length of the datagram or packet in bytes, including the header and data. The maximum length of an IP packet can be $2^{16} - 1 = 65,535$ bytes. Routers use this field to determine whether fragmentation is necessary by comparing the total length with the outgoing MTU.
- **Identification**—This field is 16 bits in length. It identifies fragments for reassembly.
- **Flags**—This field is 3 bits in length. It indicates whether the packet can be fragmented and whether more fragments follow. Bit 0 is reserved and set to 0. Bit 1 indicates May Fragment (0) or Do Not Fragment (1). Bit 2 indicates Last Fragment (0) or More Fragments to follow (1).
- **Fragment offset**—This field is 13 bits in length. It indicates (in bytes) where in the packet this fragment belongs. The first fragment has an offset of 0.
- **Time to live**—This field is 8 bits in length. It indicates the maximum time the packet is to remain on the network. Each router decrements this field by 1 for loop avoidance. If this field is 0, the packet must be discarded. This scheme permits routers to discard undeliverable packets.
- **Protocol**—This field is 8 bits in length. It indicates the upper-layer protocol. The Internet Assigned Numbers Authority (IANA) is responsible for assigning IP protocol values. Table 7-2 shows some key protocol numbers. A full list can be found at http://www.iana.org/assignments/protocol-numbers.

Table 7-2 *IP Protocol Numbers*

Protocol Number	Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
6	Transmission Control Protocol (TCP)
17	User Datagram Protocol (UDP)
88	Enhanced IGRP (EIGRP)
89	Open Shortest Path First (OSPF)
103	Protocol-Independent Multicast (PIM)

- **Header checksum**—This field is 16 bits in length. The checksum does not include the data portion of the packet in the calculation. The checksum is recomputed and verified at each point the IP header is processed.
- **Source address**—This field is 32 bits in length. It is the sender's IP address.
- **Destination address**—This field is 32 bits in length. It is the receiver's IP address.
- **IP options**—This field is variable in length. The options provide for control functions that are useful in some situations but unnecessary for the most common communications. Specific options are security, loose source routing, strict source routing, record route, and timestamp.
- **Padding**—This field is variable in length. It ensures that the IP header ends on a 32-bit boundary.

Table 7-3 summarizes the fields of the IP header.

Table 7-3 *IPv4 Header Fields*

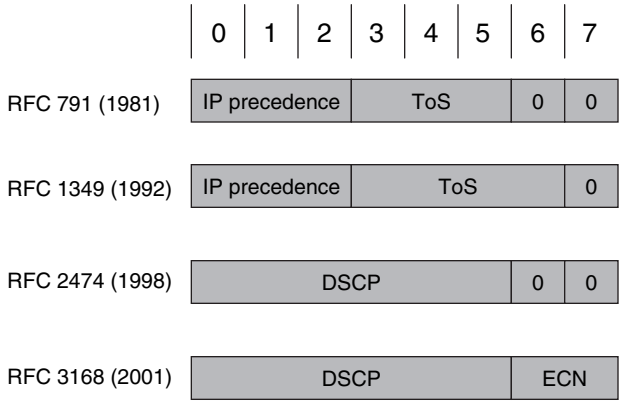
Field	Length	Description
Version	4 bits	Indicates the IP header's format, based on the version number. Set to 0100 for IPv4.
IHL	4 bits	Length of the header in 32-bit words.
ToS	8 bits	QoS parameters.
Total length	16 bits	Length of the packet in bytes, including header and data.
Identification	16 bits	Identifies a fragment.
Flags	3 bits	Indicates whether a packet is fragmented and whether more fragments follow.
Fragment offset	13 bits	Location of the fragment in the total packet.
Time to live	8 bits	Decremented by 1 by each router. When this is 0, the router discards the packet.
Protocol	8 bits	Indicates the upper-layer protocol.
Header checksum	16 bits	Checksum of the IP header; does not include the data portion.
Source address	32 bits	IP address of the sending host.
Destination address	32 bits	IP address of the destination host.
IP options	Variable	Options for security, loose source routing, record route, and timestamp.
Padding	Variable	Added to ensure that the header ends in a 32-bit boundary.

ToS

The ToS field of the IP header is used to specify QoS parameters. Routers and layer 3 switches look at the ToS field to apply policies, such as priority, to IP packets based on the settings. The ToS field has undergone several definitions since RFC 791.

Figure 7-2 shows the several formats of the ToS service field based on the evolution of RFCs 791 (1981), 1349 (1992), 2474 (1998), and 3168 (2001). The following paragraphs describe this evolution.

Figure 7-2 *Evolution of the IPv4 ToS Field*



The first 3 (leftmost) bits are the IP precedence bits. These bits define values that are used by QoS methods. The precedence bits especially help in marking packets to give them differentiated treatment with different priorities. For example, Voice over IP (VoIP) packets can get preferential treatment over regular data packets. RFC 791 describes the precedence bits as shown in Table 7-4.

Table 7-4 *IP Precedence Bit Values*

Decimal	Binary	Description
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash override
5	101	Critical
6	110	Internetwork control
7	111	Network control

All default traffic is set with 000 in the precedence bits. Voice traffic is usually set to 101 (critical) to give it priority over normal traffic. Applications such as FTP are assigned a normal priority because it tolerates network latency and packet loss. Packet retransmissions are typically acceptable for normal traffic.

RFC 1349 redefined Bits 3 and 6 (expanding for ToS bits) to reflect a desired type of service optimization. Table 7-5 shows the ToS field values that indicate service parameters to use for IP packets.

Table 7-5 *ToS Field Values*

ToS Bits 3 to 6	Description
0000	Normal service
1000	Minimize delay
0100	Maximize throughput
0010	Maximize reliability
0001	Minimize monetary cost

In 1998, RFC 2474 redefined the ToS octet as the Differentiated Services (DS) field and further specified bits 0 through 5 as the Differentiated Services Codepoint (DSCP) to support differentiated services. RFC 3168 (2001) provides updates to RFC 2474 with the specification on an Explicit Congestion Notification (ECN) field.

The DS field takes the format shown in Figure 7-2. The DS field provides more granular levels of packet classification by using 6 bits for packet marking. DS has $2^6 = 64$ levels of classification, which is significantly higher than the eight levels of the IP precedence bits. These 64 levels are called codepoints, and they have been defined to be backward-compatible with IP precedence values. The network designer uses DSCP to give priority to IP packets using Cisco routers. Routers should be configured to map these codepoints to per-hop behaviors (PHB) with queuing or other bandwidth-management techniques. Table 7-6 compares DSCP and IP precedence values used to assign priority and apply policies to IP packets.

Table 7-6 *DSCP and IP Precedence Values*

IP Precedence			DSCP		
Service Type	**Decimal**	**Binary**	**Class**	**Decimal**	**Binary**
Routine	0	000	Best effort	0	000 to 000
Priority	1	001	Assured Forwarding (AF) Class 1	8	001 to 000
Immediate	2	010	AF Class 2	16	010 to 000

Table 7-6 *DSCP and IP Precedence Values (Continued)*

IP Precedence			DSCP		
Service Type	**Decimal**	**Binary**	**Class**	**Decimal**	**Binary**
Flash	3	011	AF Class 3	24	011 to 000
Flash override	4	100	AF Class 4	32	100 to 000
Critical	5	101	Express Forwarding (EF)	40	101 to 000
Internetwork control	6	110	Control	48	110 to 000
Network control	7	111	Control	56	111 to 000

RFC 2597 defines recommended values for AF codepoints with low, medium, and high packet drop precedence. Table 7-7 shows the recommended AF codepoint values.

Table 7-7 *DSCP AF Packet Drop Precedence Values*

Precedence	AF Class 1	AF Class 2	AF Class 3	AF Class 4
Low drop precedence	001010	010010	011010	100010
Medium drop precedence	001100	010100	011100	100100
High drop precedence	001110	010110	011110	100110

IPv4 Fragmentation

One of the key characteristics of IPv4 is fragmentation and reassembly. Although the maximum length of an IP packet is 65,535 bytes, most of the common lower-layer protocols do not support such large MTUs. For example, the MTU for Ethernet is approximately 1518 bytes. When the IP layer receives a packet to send, it first queries the outgoing interface to get its MTU. If the packet's size is greater than the interface's MTU, the layer fragments the packet.

When a packet is fragmented, it is not reassembled until it reaches the destination IP layer. The destination IP layer performs the reassembly. Any router in the path can fragment a packet, and any router in the path can fragment a fragmented packet again. Each fragmented packet receives its own IP header and is routed independently from other packets. Routers and layer 3 switches in the path do not reassemble the fragments. The destination host performs the reassembly and places the fragments in the correct order by looking at the identification and fragment offset fields.

If one or more fragments are lost, the entire packet must be retransmitted. Retransmission is the responsibility of the higher-layer protocol (such as TCP). Also, you can set the Flags field in the

IP header to "Do Not Fragment" the packet. If the field indicates Do Not Fragment, the packet is discarded if the outgoing MTU is smaller than the packet.

IPv4 Addressing

This section covers the IPv4 address classes, private addressing, and NAT. The IPv4 address space was initially divided into five classes. Each IP address class is identified by the initial bits of the address. Classes A, B, and C are unicast IP addresses, meaning that the destination is a single host. IP Class D addresses are multicast addresses, which are sent to multiple hosts. IP Class E addresses are reserved. Private addresses are selected address ranges that are reserved for use by companies in their private networks. These private addresses are not routed in the Internet. NAT translates between private and public addresses.

An IP addresses is a unique logical number to a network device or interface. An IP address is 32 bits in length. To make the number easier to read, the dotted-decimal format is used. The bits are combined into four 8-bit groups, each converted into decimal numbers—for example, 10.1.1.1. If you are not familiar with binary numbers, Appendix B contains a review of binary and hexadecimal number manipulation.

The following example shows an IP address in binary and decimal formats:

Binary IP address: 01101110 00110010 11110010 00001010
Convert each byte into decimal.

For the first octet:
01101110
0+64+32+0+8+4+2+0 = 110
01101110 = 110

For the second octet:
00110010
0+0+32+16+0+0+2+0 = 50
00110010 = 50

For the third octet:
11110010
128+64+32+16+0+0+2+0 = 242
11110010 = 242

For the fourth octet:
00001010
0+0+0+0+8+0+2+0 = 10
00001010 = 10

The IP address is 110.50.242.10.

IPv4 Address Classes

IPv4 addresses have five classes—A, B, C, D, and E. In classful addressing, the most significant bits of the first byte determine the address class of the IP address. Table 7-8 shows the high-order bits of each IP address class.

Table 7-8 *High-Order Bits of IPv4 Address Classes*

Address Class	High-Order Bits*
A	0*xxxxxxx*
B	10*xxxxxx*
C	110*xxxxx*
D	1110*xxxx*
E	1111*xxxx*

**x* can be either 1 or 0, regardless of the address class.

Again, the IPv4 Class A, B, and C addresses are unicast addresses. Unicast addresses represent a single destination. Class D is for multicast addresses. Packets sent to a multicast address are sent to a group of hosts. Class E addresses are reserved for experimental use. IANA allocates the IPv4 address space. IANA delegates regional assignments to Regional Internet Registries (RIR). The five RIRs are

- ARIN (American Registry for Internet Numbers)
- RIPE NCC (Reseaux IP Europeens Network Control Center)
- APNIC (Asia Pacific Network Information Center)
- LACNIC (Latin America and Caribbean Network Information Center)
- AfriNIC (African Network Information Centre)

Updates to the IPv4 address space can be found at http://www.iana.org/assignments/ipv4-address-space.

The following sections discuss each of these classes in detail.

Class A Addresses

Class A addresses range from 0 (00000000) to 127 (01111111) in the first byte. Network numbers available for assignment to organizations are from 1.0.0.0 to 126.0.0.0. Networks 0 and 127 are reserved. For example, 127.0.0.1 is reserved for localhost or host loopback. A packet sent to a localhost address is sent to the local machine.

By default, for Class A addresses, the first byte is the network number, and the three remaining bytes are the host number. The format is *N.H.H.H*, where *N* is the network part and *H* is the host part. With 24 bits available, there are $2^{24} - 2 = 16{,}777{,}214$ IP addresses for host assignment per Class A network. We subtract two for the network number (all 0s) and broadcast address (all 1s). A network with this many hosts will surely not work with so many hosts attempting to broadcast on the network. This section discusses subnetting later as a method of defining smaller networks within a larger network address.

Class B Addresses

Class B addresses range from 128 (10000000) to 191 (10111111) in the first byte. Network numbers assigned to companies or other organizations are from 128.0.0.0 to 191.255.0.0. This section discusses the 16 networks reserved for private use later.

By default, for Class B addresses, the first two bytes are the network number, and the remaining two bytes are the host number. The format is *N.N.H.H*. With 16 bits available, there are $2^{16} - 2 = 65{,}534$ IP addresses for host assignment per Class B network. As with Class A addresses, having a segment with more than 65,000 hosts broadcasting will surely not work; you resolve this issue with subnetting.

Class C Addresses

Class C addresses range from 192 (11000000) to 223 (11011111) in the first byte. Network numbers assigned to companies are from 192.0.0.0 to 223.255.255.0. The format is *N.N.N.H*. With 8 bits available, there are $2^8 - 2 = 254$ IP addresses for host assignment per Class C network. $H = 0$ is the network number; $H = 255$ is the broadcast address.

Class D Addresses

Class D addresses range from 224 (11100000) to 239 (11101111) in the first byte. Network numbers assigned to multicast groups range from 224.0.0.1 to 239.255.255.255. These addresses do not have a host or network part. Some multicast addresses are already assigned; for example, 224.0.0.10 is used by routers running EIGRP. A full list of assigned multicast addresses can be found at http://www.iana.org/assignments/multicast-addresses.

Class E Addresses

Class E addresses range from 240 (11110000) to 254 (11111110) in the first byte. These addresses are reserved for experimental networks. Network 255 is reserved for the broadcast address, such as 255.255.255.255. Table 7-9 summarizes the IPv4 address classes. Again, each address class can be uniquely identified in binary by the high-order bits.

Table 7-9 *IPv4 Address Classes*

Address Class	High-Order Bits	Network Numbers
A	0*xxxxxxx*	1.0.0.0 to 126.0.0.0*
B	10*xxxxxx*	128.0.0.0 to 191.255.0.0
C	110*xxxxx*	192.0.0.0 to 223.255.255.0
D	1110*xxxx*	224.0.0.1 to 239.255.255.255
E	1111*xxxx*	240.0.0.0 to 254.255.255.255

*Networks 0.0.0.0 and 127.0.0.0 are reserved as special-use addresses.

IPv4 Private Addresses

Some network numbers within the IPv4 address space are reserved for private use. These numbers are not routed on the Internet. Many organizations today use private addresses in their internal networks with NAT to access the Internet. (NAT is covered later in this chapter.) Private addresses are explained in RFC 1918, *Address Allocation for Private Internets*, published in 1996. Private addresses were one of the first steps dealing with the concern that the globally unique IPv4 address space would become exhausted. The availability of private addresses combined with NAT reduces the need for organizations to carefully define subnets to minimize the waste of assigned, public, global IP addresses.

The IP network address space reserved for private internets is 10/8, 172.16/12, and 192.168/16. It includes one Class A network, 16 Class B networks, and 256 Class C networks. Table 7-10 summarizes private address space. Large organizations can use network 10.0.0.0/8 to assign address space throughout the enterprise. Midsize organizations can use one of the Class B private networks 172.16.0.0/16 through 172.31.0.0/16 for IP addresses. The smaller Class C addresses, which begin with 192.168, support only up to 254 hosts each.

Table 7-10 *IPv4 Private Address Space*

Class Type	Start Address	End Address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

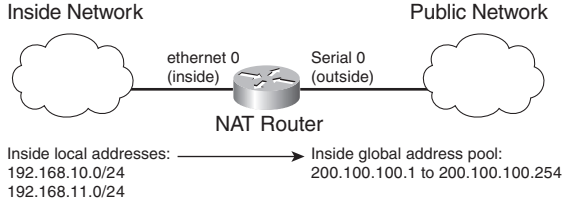
NAT

NAT devices convert internal IP address space into globally unique IP addresses. NAT was originally specified by RFC 1631; the current specification is RFC 3022. Companies use NAT to translate internal private addresses to public addresses.

The translation can be from many private addresses to a single public address or from many private addresses to a range of public addresses. When NAT performs many-to-one, the process is called port address translation (PAT) because different port numbers identify translations.

As shown in Figure 7-3, the source addresses for outgoing IP packets are converted to globally unique IP addresses. The conversion can be configured statically, or it can dynamically use a global pool of addresses.

Figure 7-3 *Network Address Translation*



NAT has several forms:

- **Static NAT**—Maps an unregistered IP address to a registered IP address; it is configured manually.
- **Dynamic NAT**—Dynamically maps an unregistered IP address to a registered IP address from a pool (group) of registered addresses. The two subsets of dynamic NAT are overloading and overlapping:
  - **Overloading**—Maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is also known as PAT, single-address NAT, or port-level multiplexed NAT.
  - **Overlapping**—Maps registered internal IP addresses to outside registered IP addresses. It can also map external addresses to internal registered addresses.

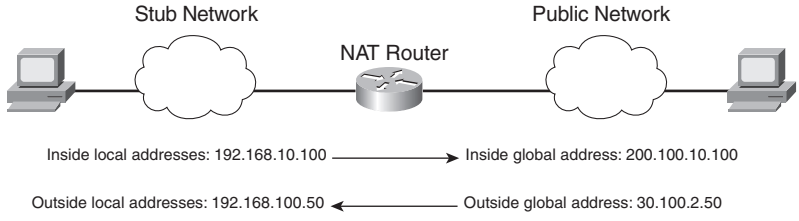
When designing for NAT, you should understand the following terminology:

- **Stub domain**—The internal network that might be using private IP addresses.
- **Public network**—Outside the stub domain, it resides in the Internet. Addresses in the public network can be reached from the Internet.

- **Inside local address**—The real IP address of the device that resides in the internal network. This address is used in the stub domain.
- **Inside global address**—The translated IP address of the device that resides in the internal network. This address is used in the public network.
- **Outside global address**—The real IP address of a device that resides in the Internet, outside the stub domain.
- **Outside local address**—The translated IP address of the device that resides in the Internet. This address is used inside the stub domain.

Figure 7-4 illustrates the terms described in the list. The real IP address of the host in the stub network is 192.168.10.100; it is the inside local address. The NAT router translates the inside local address into the inside global address (200.100.10.100). Hosts located in the Internet have their real IP address (outside global address) translated; in the example, 30.100.2.50 is translated into the outside local address of 192.168.100.50.

Figure 7-4 *Terminology Example*



IPv4 Address Subnets

Subnetting plays an important part in IPv4 addressing. The subnet mask helps determine the network, subnetwork, and host part of an IP address. The network architect uses subnetting to manipulate the default mask to create subnetworks for LAN and WAN segments. These subnetworks provide enough addresses for LANs of different sizes. Point-to-point WAN links usually get a subnet mask that allows for only two hosts because only two routers are present in the point-to-point WAN link. You should become familiar with determining subnetwork numbers, broadcast addresses, and host address ranges given an IP address and mask.

Subnet masks are used for Class A, B, and C addresses only. Multicast addresses do not use subnet masks. A subnet mask is a 32-bit number in which bits are set to 1 to establish the network portion of the address, and a 0 is the host part of the address. The mask's bits set to 1 are contiguous on the left portion of the mask; the bits set to 0 are contiguous on the right portion of the mask. Table 7-11 shows the default masks for Class A, B, and C addresses. This section addresses various ways to represent IP subnet masks. Understanding these ways is significant because the representation

of a network and its mask can appear differently in Cisco documentation or on the command-line interface.

Table 7-11 *IPv4 Default Network Address Masks*

Class	Binary Mask	Dotted-Decimal Mask
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Mask Nomenclature

There are several ways to represent IP subnet masks. The mask can be binary, hexadecimal, dotted-decimal, or a prefix "bit mask." Historically, the most common representation was the dotted-decimal format (255.255.255.0). The prefix bit mask format is now more popular. This format represents the mask by using a slash followed by the number of leading address bits that must be set to 1 for the mask. For example, 255.255.0.0 is represented as /16. Table 7-12 shows most of the mask representations. The /30 mask is common for WAN point-to-point links, and /32 is used for router loopback addresses.

Table 7-12 *Subnet Masks*

Dotted Decimal	Bit Mask	Hexadecimal
255.0.0.0	/8	FF000000
255.192.0.0	/10	FFC00000
255.255.0.0	/16	FFFF0000
255.255.224.0	/19	FFFFE000
255.255.240.0	/20	FFFFF000
255.255.255.0	/24	FFFFFF00
255.255.255.128	/25	FFFFFF80
255.255.255.192	/26	FFFFFFC0
255.255.255.224	/27	FFFFFFE0
255.255.255.240	/28	FFFFFFF0
255.255.255.248	/29	FFFFFFF8
255.255.255.252	/30	FFFFFFFC
255.255.255.255	/32	FFFFFFFF

IP Address Subnet Design Example

This example shows subnetting for a small company. Say the company has 200 hosts and is assigned the Class C network of 195.10.1.0/24. The 200 hosts are in six different LANs.

You can subnet the Class C network using a mask of 255.255.255.224. Looking at the mask in binary (11111111 11111111 11111111 11100000), the first three bytes are the network part, the first 3 bits of the fourth byte determine the subnets, and the five remaining 0 bits are for host addressing.

Table 7-13 shows the subnetworks created with a mask of 255.255.255.224. Using this mask, 2^n subnets are created, where n is the number of bits taken from the host part for the subnet mask. This example uses 3 bits, so $2^3 = 8$ subnets. With Cisco routers, you can use the all-1s subnet (LAN 7) for a subnet. You cannot use the 0s subnet by default, but with Cisco routers, you can use it by configuring the **ip subnet-zero** command. The first column of the table lists the LAN. The second column shows the binary of the fourth byte of the IP address. The third column shows the subnet number, and the fourth and fifth columns show the first host and broadcast address of the subnet.

Table 7-13 *Subnets for Network 195.1.1.0*

LAN	Fourth Byte	Subnet Number	First Host	Broadcast Address
LAN 0	**000**00000	195.10.1.0	195.10.1.1	195.10.1.31
LAN 1	**001**00000	195.10.1.32	195.10.1.33	195.10.1.63
LAN 2	**010**00000	195.10.1.64	195.10.1.65	195.10.1.95
LAN 3	**011**00000	195.10.1.96	195.10.1.97	195.10.1.127
LAN 4	**100**00000	195.10.1.128	195.10.1.129	195.10.1.159
LAN 5	**101**00000	195.10.1.160	195.10.1.161	195.10.1.191
LAN 6	**110**00000	195.10.1.192	195.10.1.193	195.10.1.223
LAN 7	**111**00000	195.10.1.224	195.10.1.225	195.10.1.255

Use the formula $2^n - 2$ to calculate the number of hosts per subnet, where n is the number of bits for the host portion. The preceding example has 5 bits in the fourth byte for host addresses. With $n = 5$, $2^5 - 2 = 30$ hosts. For LAN 1, host addresses range from 195.10.1.33 to 195.10.1.62 (30 addresses). The broadcast address for the subnet is 195.10.1.63. Each LAN repeats this pattern with 30 hosts in each subnet.

The example uses a fixed-length subnet mask. The whole Class C network has the same subnet mask, 255.255.255.224. Routing protocols such as Routing Information Protocol version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP) can use only fixed-length subnet masks;

they do not support VLSMs, in which masks of different lengths identify subnets within the network. VLSMs are covered later in this chapter.

Determining the Network Portion of an IP Address

Given an address and mask, you can determine the classful network, the subnetwork, and the subnetwork's broadcast number. You do so with a logical AND operation between the IP address and subnet mask. You obtain the broadcast address by taking the subnet number and making the host portion all 1s. Table 7-14 shows the logical AND operation. Notice that the AND operation is similar to multiplying bit 1 and bit 2; if any 0 is present, the result is 0.

Table 7-14 *The AND Logical Operation*

Bit 1	Bit 2	AND
0	0	0
0	1	0
1	0	0
1	1	1

As an example, take the IP address 150.85.1.70 with a subnet mask of 255.255.255.224, as shown in Table 7-15. Notice the 3 bold bits in the subnet mask. These bits extend the default Class C prefix (/24) 3 bits to a mask of /27. As shown in Table 7-15, you perform an AND operation of the IP address with the subnet mask to obtain the subnetwork. You obtain the broadcast number by making all the host bits 1. As shown in bold, the subnet mask reaches 3 bits in the fourth octet. The subnetwork is identified by the five rightmost zeros in the fourth octet, and the broadcast is identified by all ones in the five rightmost bits.

Table 7-15 *Subnetwork of IP Address 150.85.1.70*

	Binary First, Second, and Third Octets	Binary Fourth Octet		Dotted-Decimal IP
IP Address	10010110 01010101 00000001	010	00110	150.85.1.70
Subnet Mask	11111111 11111111 11111111	**111**	00000	255.255.255.224
Subnetwork	10010110 01010101 00000001	010	**00000**	150.85.1.64
	Major network portion	Subnet	Host	
Broadcast Address	10010110 01010101 00000001	010	**11111**	150.85.1.95

VLSMs

VLSMs are used to divide a network into subnets of various sizes to prevent wasting IP addresses. If a Class C network uses 255.255.255.240 as a subnet mask, 16 subnets are available, each with 14 IP addresses. If a point-to-point link needs only two IP addresses, 12 IP addresses are wasted. This problem scales further with Class B and Class A address space. With VLSMs, small LANs can use /28 subnets with 14 hosts, and larger LANs can use /23 or /22 masks with 510 and 1022 hosts, respectively. Point-to-point networks use a /30 mask, which supports two hosts.

VLSM Address-Assignment Example

Take Class B network 130.20.0.0/16 as an example. Using a /20 mask produces 16 subnetworks. Table 7-16 shows the subnetworks. With the /20 subnet mask, the first 4 bits of the third byte determine the subnets.

Table 7-16 *Subnets with the /20 Mask*

Third Byte	Subnetwork
00000000	130.20.0.0/20
00010000	130.20.16.0/20
00100000	130.20.32.0/20
00110000	130.20.48.0/20
01000000	130.20.64.0/20
01010000	130.20.80.0/20
01100000	130.20.96.0/20
01110000	130.20.112.0/20
10000000	130.20.128.0/20
10010000	130.20.144.0/20
10100000	130.20.160.0/20
10110000	130.20.176.0/20
11000000	130.20.192.0/20
11010000	130.20.208.0/20
11100000	130.20.224.0/20
11110000	130.20.240.0/20

With fixed-length subnet masks, the network would support only 16 networks. Any LAN or WAN link would have to use a /20 subnet. This scenario is a waste of address space and therefore is inefficient. With VLSMs, you can further subnet the /20 subnets.

For example, take 130.20.64.0/20 and subdivide it to support LANs with about 500 hosts. A /23 mask has 9 bits for hosts, producing $2^9 - 2 = 510$ IP addresses for hosts. Table 7-17 shows the subnetworks for LANs within a specified subnet.

Table 7-17 *Subnetworks for 130.20.64.0/20*

Third Byte	Subnetwork
0100**000**0	130.20.64.0/23
0100**001**0	130.20.66.0/23
0100**010**0	130.20.68.0/23
0100**011**0	130.20.70.0/23
0100**100**0	130.20.72.0/23
0100**101**0	130.20.74.0/23
0100**110**0	130.20.76.0/23
0100**111**0	130.20.78.0/23

With VLSMs, you can further subdivide these subnetworks of subnetworks. Take subnetwork 130.20.76.0/23 and use it for two LANs that have fewer than 250 hosts. It produces subnetworks 130.20.76.0/24 and 130.20.77.0/24. Also, subdivide 130.20.78.0/23 for serial links. Because each point-to-point serial link needs only two IP addresses, use a /30 mask. Table 7-18 shows the subnetworks produced.

Table 7-18 *Serial-Link Subnetworks*

Third Byte	Fourth Byte	Subnetwork
01001110	**000000**00	130.20.78.0/30
01001110	**000001**00	130.20.78.4/30
01001110	**000010**00	130.20.78.8/30
01001110	**000011**00	130.20.78.12/30
. . .	. . .	. . .
01001111	**111101**00	130.20.79.244/30
01001111	**111110**00	130.20.79.248/30
01001111	**111111**00	130.20.79.252/30

Each /30 subnetwork includes the subnetwork number, two IP addresses, and a broadcast address. Table 7-19 shows the bits for 130.20.78.8/30.

Table 7-19 *Addresses Within Subnetwork 110.20.78.8/30*

Binary Address	IP Address	Function
10000010 00010100 01001110 00001**000**	130.20.78.8	Subnetwork
10000010 00010100 01001110 00001**001**	130.20.78.9	IP address 1
10000010 00010100 01001110 00001**010**	130.20.78.10	IP address 2
10000010 00010100 01001110 00001**011**	130.20.78.11	Broadcast address

Loopback Addresses

You can also reserve a subnet for router loopback addresses. Loopback addresses provide an always-up interface to use for router-management connectivity. The loopback address can also serve as the router ID for some routing protocols. The loopback address is a single IP address with a 32-bit mask. In the previous example, network 130.20.75.0/24 could provide 255 loopback addresses for network devices starting with 130.20.75.1/32 and ending with 130.20.75.255/32.

IP Telephony Networks

You should reserve separate subnets for LANs using IP phones. IP phones are normally placed in an auxiliary VLAN that is in a logical segment separate from that of the user workstations. Separating voice and data on different subnets or VLANs also aids in providing QoS for voice traffic in regards to classifying, queuing, and buffering. This design rule also facilitates troubleshooting.

Table 7-20 shows an example of allocating IP addresses for a small network. Notice that separate VLANs are used for the VoIP devices.

Table 7-20 *IP Address Allocation for VoIP Networks*

Building Floor/Function	VLAN Number	IP Subnet
First-floor data	VLAN 11	172.16.1.0/24
Second-floor data	VLAN 12	172.16.2.0/24
Third-floor data	VLAN 13	172.16.3.0/24
First-floor VoIP	VLAN 14	172.16.4.0/24
Second-floor VoIP	VLAN 15	172.16.5.0/24
Third-floor VoIP	VLAN 16	172.16.6.0/24

CIDR and Summarization

CIDR permits the address aggregation of classful networks. It does so by using the common bits to join networks. The network addresses need to be contiguous and have a common bit boundary.

With CIDR, ISPs assign groups of Class C networks to enterprise customers. This arrangement eliminates the problem of assigning too large of a network (Class B) or assigning multiple Class C networks to a customer and having to maintain an entry for each Class C network in the routing tables. It reduces the size of the Internet routing tables and allows for more stable routing topology because the routers do not have the recomputed routing table when more specific routes cycle up and down.

You can summarize four contiguous Class C networks at the /22 bit level. For example, networks 200.1.100.0, 200.1.101.0, 200.1.102.0, and 200.1.103.0 share common bits, as shown in Table 7-21. The resulting network is 200.1.100.0/22, which you can use for a 1000-node network.

Table 7-21 *Common Bits Within Class C Networks*

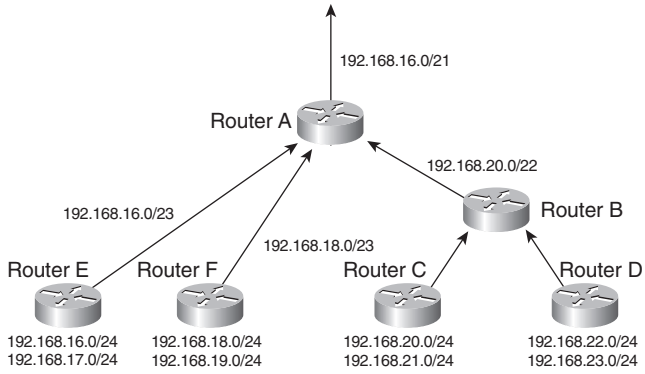
Binary Address	IP Address
11001000 00000001 01100100 00000000	200.1.100.0
11001000 00000001 01100101 00000000	200.1.101.0
11001000 00000001 01100110 00000000	200.1.102.0
11001000 00000001 01100111 00000000	200.1.103.0

It is important for an Internet network designer to assign IP networks in a manner that permits summarization. It is preferred that a neighboring router receive one summarized route, rather than 8, 16, 32, or more routes, depending on the level of summarization. This setup reduces the size of the routing tables in the network.

For route summarization to work, the multiple IP addresses must share the same leftmost bits, and routers must base their routing decisions on the IP address and prefix length.

Figure 7-5 shows an example of route summarization. All the edge routers send network information to their upstream routers. Router E summarizes its two LAN networks by sending 192.168.16.0/23 to Router A. Router F summarizes its two LAN networks by sending 192.168.18.0/23. Router B summarizes the networks it receives from Routers C and D. Routers B, E, and F send their routes to Router A. Router A sends a single route (192.168.16.0/21) to its upstream router, instead of sending eight routes. This process reduces the number of networks that upstream routers need to include in routing updates.

Figure 7-5 *Route Summarization*



Notice in Table 7-22 that all the Class C networks share a bit boundary with 21 common bits. The networks are different on the 22nd bit and thus cannot be summarized beyond the 21st bit. All these networks are summarized with 192.168.16.0/21.

Table 7-22 *Summarization of Networks*

Binary Address	IP Network
11000000 10101000 00010000 00000000	192.168.16.0
11000000 10101000 00010001 00000000	192.168.17.0
11000000 10101000 00010010 00000000	192.168.18.0
11000000 10101000 00010011 00000000	192.168.19.0
11000000 10101000 00010100 00000000	192.168.20.0
11000000 10101000 00010101 00000000	192.168.21.0
11000000 10101000 00010110 00000000	192.168.22.0
11000000 10101000 00010111 00000000	192.168.23.0

Address Assignment and Name Resolution

IP addresses, subnet masks, default gateways, and DNS servers can be assigned statically or dynamically. You should statically assign most shared network systems, such as routers and servers, but dynamically assign most client systems. This section covers the protocols you use to dynamically assign IP address parameters to a host, which are the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP). This section also covers DNS and ARP, which are two significant protocols in IP networks. DNS maps domain names to IP addresses, and ARP resolves IP addresses to MAC addresses. These protocols are important in TCP/IP networks because they simplify the methods of address assignment and resolution.

Static and Dynamic IP Address Assignment

Assign the IP addresses of routers, switches, printers, and servers statically. You need to manage and monitor these systems, so you must access them via a stable IP address.

You should dynamically assign end-client workstations to reduce the configuration tasks required to connect these systems to the network. When you assign client workstation characteristics dynamically, the system automatically learns which network segment it is assigned to and how to reach its default gateway as the network is discovered. One of the first methods used to dynamically assign IP addresses was BOOTP. The current method to assign IP addresses is DHCP.

BOOTP

The basic BOOTP was first defined in RFC 951. It has been updated by RFC 1497 and RFC 1542. It is a protocol that allows a booting host to configure itself by dynamically obtaining its IP address, IP gateway, and other information from a remote server. You can use a single server to centrally manage numerous network hosts without having to configure each host independently.

BOOTP is an application-layer protocol that uses UDP/IP for transport. The BOOTP server port is UDP Port 67. The client port is UDP Port 68. Clients send BOOTP requests to the BOOTP server, and the server responds to UDP Port 68 to send messages to the client. The destination IP of the BOOTP requests uses the all-hosts address (255.255.255.255), which the router does not forward. If the BOOTP server is one or more router hops from the subnet, you must configure the local default gateway router to forward the BOOTP requests.

BOOTP requires that you build a MAC-address-to-IP-address table on the server. You must obtain every device's MAC address, which is a time-consuming effort. BOOTP has been replaced by the more sophisticated DHCP.

DHCP

DHCP provides a way to dynamically configure hosts on the network. Based on BOOTP, it is defined in RFC 2131 and adds the capability of reusing network addresses and additional configuration options. DHCP improves on BOOTP by using a "lease" for IP addresses and providing the client with all the IP configuration parameters needed to operate in the network.

DHCP servers allocate network addresses and deliver configuration parameters dynamically to hosts. With DHCP, the computer can obtain its configuration information—IP address, subnet mask, IP default gateway, DNS servers, WINS servers, and so on—when needed. DHCP also includes other optional parameters that you can assign to clients. The configuration information is managed centrally on a DHCP server.

Routers act as relay agents by passing DHCP messages between DHCP clients and servers. Because DHCP is an extension of BOOTP, it uses the message format defined in RFC 951 for BOOTP. It uses the same ports as BOOTP: DHCP servers use UDP Port 67, and DHCP clients use UDP Port 68. Because of these similarities, the configuration to support DHCP in the routers is the same described for BOOTP.

DHCP supports permanent allocation, in which the DHCP server assigns an IP address to the client and the IP address is never reallocated to other clients. With a lease, DHCP can also assign IP addresses for a limited period of time. This dynamic-allocation mechanism can reuse the IP address after the lease expires.

An IP address is assigned as follows:

1. The client sends a **DHCPDISCOVER** message to the local network using a 255.255.255.255 broadcast.
2. BOOTP relay agents (routers) can forward the **DHCPDISCOVER** message to the DHCP server in another subnet.
3. The server sends a **DHCPOFFER** message to respond to the client, offering IP address, lease expiration, and other DHCP option information.

   Other DHCP messages include

   DHCPREQUEST—The client can request additional options or an extension on its lease of an IP address.

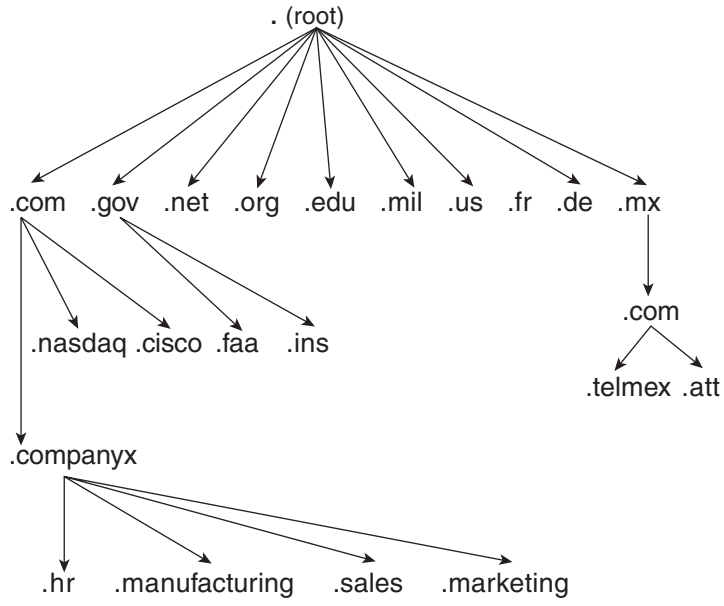
   DHCPRELEASE—The client relinquishes the IP address and cancels the remaining lease.
4. If the server is out of addresses or it determines that the client request is invalid, it sends a **DHCPNAK** message to the client.

DNS

DNS servers return destination IP addresses given a domain name. DNS is a distributed database. Separate, independent organizations administer their assigned domain name spaces and can break their domains into a number of subdomains. For example, given www.cisco.com, DNS returns the IP address 198.133.219.25. DNS was first specified by RFCs 882 and 883. The current specifications are specified in RFCs 1034 and 1035.

DNS was implemented to overcome the limitations of managing a single text-host table. Imagine creating and maintaining text files with the names and IP addresses of all the hosts in the Internet! DNS scales hostname-to-IP-address translation by distributing responsibility for the domain name space. DNS follows a reversed tree structure for domain name space, as shown in Figure 7-6. IANA (http://www.iana.org) manages the tree's root.

Figure 7-6 *DNS Tree*



DNS uses TCP and UDP Port 53. UDP is the recommended transport protocol for DNS queries. TCP is the recommended protocol for zone transfers between DNS servers. A zone transfer occurs when you place a secondary server in the domain and transfer the DNS information from the primary DNS server to the secondary server. A DNS query searches for the IP address of an FQDN, such as www.cnn.com.

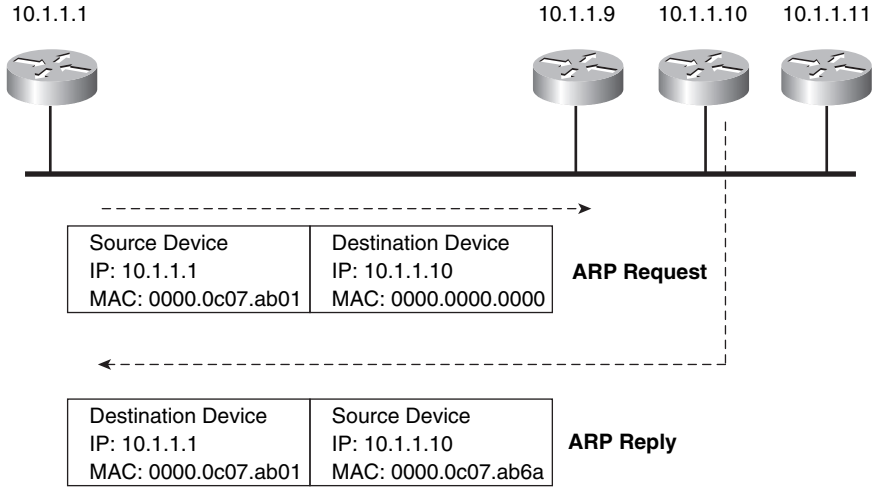
ARP

When a router needs to send an IP packet over an Ethernet network, it needs to find out what 48-bit MAC physical address to send the frame to. Given the destination IP, ARP obtains the destination MAC. The destination MAC can be a local host or the gateway router's MAC address if the destination IP is across the routed network. ARP is described in RFC 826. The local host maintains an ARP table with a list relating IP address to MAC address.

ARP operates by having the sender broadcast an ARP request. Figure 7-7 shows an example of an ARP request and reply. Suppose a router with the IP address 10.1.1.1 has a packet to send to 10.1.1.10 but does not have the destination MAC address in its ARP table. It broadcasts an ARP request to all hosts in a subnet. The ARP request contains the sender's IP and MAC address as well as the target IP address. All nodes in the broadcast domain receive the ARP request and process it. The device with the target IP address sends an ARP reply to the sender with its MAC address

information; the ARP reply is a unicast message sent to 10.1.1.1. The sender now has the target MAC address in its ARP cache and sends the frame.

Figure 7-7 *ARP Request and Reply*



References and Recommended Readings

Almquist, P. RFC 1349, *Type of Service in the Internet Protocol Suite*. Available from http://www.ietf.org/rfc.

Croft, B. and J. Gilmore. RFC 951, *Bootstrap Protocol (BOOTP)*. Available from http://www.ietf.org/rfc.

Davie, B., A. Charny, J.C.R. Bennet, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis. RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*. Available from http://www.ietf.org/rfc.

Droms, R. RFC 2131, *Dynamic Host Configuration Protocol*. Available from http://www.ietf.org/rfc.

Egevang, K. and P. Francis. RFC 1631, *The IP Network Address Translator (NAT)*. Available from http://www.ietf.org/rfc.

Heinanen, J., F. Baker, W. Weiss, and J. Wroclawski. RFC 2597, *Assured Forwarding PHB Group*. Available from http://www.ietf.org/rfc.

Information Sciences Institute. RFC 791, *Internet Protocol*. Available from http://www.ietf.org/rfc.

Mockapetris, P. RFC 1034, *Domain Names - Concepts and Facilities*. Available from http://www.ietf.org/rfc.

Mockapetris, P. RFC 1035, *Domain Names - Implementation and Specification*. Available from http://www.ietf.org/rfc.

Nichols, K., S. Blake, F. Baker, and D. Black. RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. Available from http://www.ietf.org/rfc.

Plummer, D. RFC 826, *Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. Available from http://www.ietf.org/rfc.

Ramakrishnan, K., S. Floyd, and D. Black. RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*. Available from http://www.ietf.org/rfc.

Rekhter, Y., B. Moskowitz, D. Karrenberg, G.J. de Groot, and E. Lear. RFC 1918, *Address Allocation for Private Internets*. Available from http://www.ietf.org/rfc.

Srisuresh, P. and K. Egevang. RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*. Available from http://www.ietf.org/rfc.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

This chapter covered the following topics that you will need to master for the CCDA exam:

- **IPv4 header**—Know each field of the IPv4 header.
- **IPv4 addressing**—Know IPv4 address classes, private addressing, and NAT.
- **IPv4 address subnets**—Know VLSMs with a design example.
- **Address assignment and resolution**—Know dynamic IP assignment and address-resolution protocols such as BOOTP, DHCP, DNS, and ARP.

Table 7-23 outlines the IPv4 address classes.

Table 7-23 *IPv4 Address Classes*

Address Class	High-Order Bits	Network Numbers
A	0*xxxxxxx*	1.0.0.0 to 126.0.0.0
B	10*xxxxxx*	128.0.0.0 to 191.255.0.0
C	110*xxxxx*	192.0.0.0 to 223.255.255.0
D	1110*xxxx*	224.0.0.0 to 239.255.255.255
E	1111*xxxx*	240.0.0.0 to 254.255.255.255

Table 7-24 summarizes the IPv4 private address space.

Table 7-24 *IPv4 Private Address Space*

Class Type	Start Address	End Address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

Table 7-25 shows subnet mask representations.

Table 7-25 *Subnet Mask Representations*

Dotted Decimal	Prefix	Hexadecimal
255.0.0.0	/8	FF000000
255.128.0.0	/9	FFA00000
255.192.0.0	/10	FFC00000
255.224.0.0	/11	FFE00000
255.240.0.0	/12	FFF00000
255.248.0.0	/13	FFFA0000
255.252.0.0	/14	FFFC0000
255.254.0.0	/15	FFFE0000
255.255.0.0	/16	FFFF0000
255.255.128.0	/17	FFFFA000
255.255.192.0	/18	FFFFC000
255.255.224.0	/19	FFFFE000
255.255.240.0	/20	FFFFF000
255.255.248.0	/21	FFFFFA00
255.255.252.0	/22	FFFFFC00
255.255.254.0	/23	FFFFFE00
255.255.255.0	/24	FFFFFF00
255.255.128.0	/25	FFFFFFA0
255.255.192.0	/26	FFFFFFC0
255.255.255.224	/27	FFFFFFE0
255.255.255.240	/28	FFFFFFF0
255.255.255.248	/29	FFFFFFF8
255.255.255.252	/30	FFFFFFFC
255.255.255.254	/31	FFFFFFFE
255.255.255.255	/32	FFFFFFFF

The following list reviews the various IPv4 address types:

- **Unicast**—The IP address of an interface on a single host. It can be a source or destination address.
- **Multicast**—An IP address that reaches a group of hosts. It is only a destination address.
- **Broadcast**—An IP logical address that reaches all hosts in an IP subnet. It is only a destination address.

Table 7-26 summarizes the fields of the IP header.

Table 7-26 *IPv4 Header Fields*

Field	Length	Description
Version	4 bits	Indicates the IP header's format, based on the version number. Set to 0100 for IPv4.
IHL	4 bits	Length of the header in 32-bit words.
ToS	8 bits	QoS parameters.
Total length	16 bits	Length of the packet in bytes, including header and data.
Identification	16 bits	Identifies a fragment.
Flags	3 bits	Indicates whether a packet is fragmented and whether more fragments follow.
Fragment offset	13 bits	Location of the fragment in the total packet.
Time to live	8 bits	Decremented by 1 by each router. When this is 0, the router discards the packet.
Protocol	8 bits	Indicates the upper-layer protocol.
Header checksum	16 bits	Checksum of the IP header; does not include the data portion.
Source address	32 bits	IP address of the sending host.
Destination address	32 bits	IP address of the destination host.
IP options	Variable	Options for security, loose source routing, record route, and timestamp.
Padding	Variable	Added to ensure that the header ends in a 32-bit boundary.

Table 7-27 compares DSCP and IP precedence values used to assign priority and apply policies to IP packets.

Table 7-27 *DSCP and IP Precedence Values*

IP Precedence			**DSCP**		
Service Type	**Decimal**	**Binary**	**Class**	**Decimal**	**Binary**
Routine	0	000	Best effort	0	000 to 000
Priority	1	001	Assured Forwarding (AF) Class 1	8	001 to 000
Immediate	2	010	AF Class 2	16	010 to 000
Flash	3	011	AF Class 3	24	011 to 000
Flash override	4	100	AF Class 4	32	100 to 000
Critical	5	101	Express Forwarding (EF)	40	101 to 000
Internetwork control	6	110	Control	48	110 to 000
Network control	7	111	Control	56	111 to 000

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. List the RFC 1918 private address space.
2. What is the difference between VLSM and CIDR?
3. Fill in the blank: _____ maps FQDN to IP addresses.
4. True or false: You can use DHCP to specify the TFTP host's IP address to a client PC.
5. True or false: 255.255.255.248 and /28 are two representations of the same IP mask.
6. True or false: Upper-layer protocols are identified in the IP header's protocol field. TCP is protocol 6, and UDP is protocol 17.
7. Fill in the blank: Without any options, the IP header is _____ bytes in length.
8. The IP header's ToS field is redefined as the DS field. How many bits does DSCP use for packet classification, and how many levels of classification are possible?
9. True or false: NAT uses different IP addresses for translations. PAT uses different port numbers to identify translations.
10. True or false: The IP header's header checksum field performs the checksum of the IP header and data.
11. Calculate the subnet, the address range within the subnet, and the subnet broadcast of the address 172.56.5.245/22.
12. When packets are fragmented at the network layer, where are the fragments reassembled?
13. Which protocol can you use to configure a default gateway?
    a. ARP
    b. DHCP
    c. DNS
    d. RARP

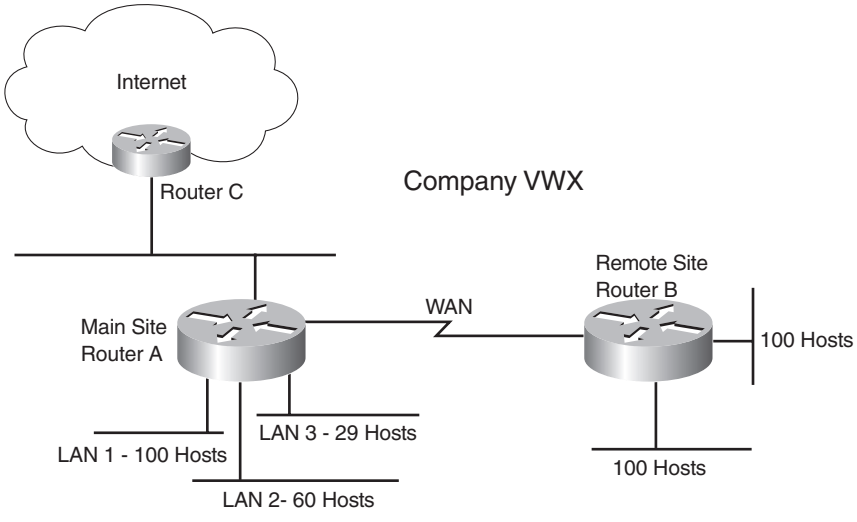
14. How many host addresses are available with a Class B network with the default mask?
    a. 63,998
    b. 64,000
    c. 65,534
    d. 65,536
15. Which of the following is a dotted-decimal representation of a /26 prefix mask?
    a. 255.255.255.128
    b. 255.255.255.192
    c. 255.255.255.224
    d. 255.255.255.252
16. Which network and mask summarize both the 192.170.20.16/30 and 192.170.20.20/30 networks?
    a. 192.170.20.0/24
    b. 192.170.20.20/28
    c. 192.170.20.16/29
    d. 192.170.20.0/30
17. Which AF class is backward-compatible with IP precedence bits' flash traffic?
    a. AF2
    b. AF3
    c. AF4
    d. EF
18. Which of the following is true about fragmentation?
    a. Routers between source and destination hosts can fragment IPv4 packets.
    b. Only the first router in the network can fragment IPv4 packets.
    c. IPv4 packets cannot be fragmented.
    d. IPv4 packets are fragmented and reassembled at each link through the network.
19. A packet sent to a multicast address reaches what destination(s)?
    a. The nearest destination in a set of hosts.
    b. All destinations in a set of hosts.
    c. Broadcasts to all hosts.
    d. Reserved global destinations.

20. What are three types of IPv4 addresses?

Answer the following questions based on the given scenario and figure.

Company VWX has the network shown in Figure 7-8. The main site has three LANs with 100, 29, and 60 hosts. The remote site has two LANs, each with 100 hosts. The network uses private addresses. The Internet service provider assigned the company the network 210.200.200.8/26.

Figure 7-8 *Scenario Diagram*



21. The remote site uses the network prefix 192.168.10.0/24. What subnets and masks can you use for the LANs at the remote site and conserve address space?

- **a.** 192.168.10.64/26 and 192.168.10.192/26
- **b.** 192.168.10.0/25 and 192.168.10.128/25
- **c.** 192.168.10.32/28 and 192.168.10.64/28
- **d.** 192.168.10.0/30 and 192.168.10.128/30

22. The main site uses the network prefix 192.168.15.0/24. What subnets and masks can you use to provide sufficient addresses for LANs at the main site and conserve address space?

- **a.** 192.168.15.0/25 for LAN 1, 192.168.15.128/26 for LAN 2, and 172.15.192.0/27 for LAN 3
- **b.** 192.168.15.0/27 for LAN 1, 192.168.15.128/26 for LAN 2, and 172.15.192.0/25 for LAN 3

c. 192.168.15.0/100 for LAN 1, 192.168.15.128/60 for LAN 2, and 172.15.192.0/29 for LAN 3

d. 192.168.15.0/26 for LAN 1, 192.168.15.128/26 for LAN 2, and 172.15.192.0/29 for LAN 3

23. Which network and mask would you use for the WAN link to save the most address space?

a. 192.168.11.240/27

b. 192.168.11.240/28

c. 192.168.11.240/29

d. 192.168.11.240/30

24. What networks does Router C announce to the Internet service provider's Internet router?

a. 210.200.200.8/26

b. 192.168.10.0/24 and 192.168.11.0/24

c. 192.168.10.0/25 summary address

d. 201.200.200.8/29 and 192.168.10.0/25

25. What technology does Router C use to convert private addresses to public addresses?

a. DNS

b. NAT

c. ARP

d. VLSM

26. What mechanism supports the ability to divide a given subnet into smaller subnets based on need?

a. DNS

b. NAT

c. ARP

d. VLSM

This chapter covers the following subjects:

- Introduction to IPv6
- IPv6 header
- IPv6 address representation
- IPv6 address types and address allocations
- IPv6 mechanisms
- IPv6 routing protocols
- IPv4 to IPv6 transition strategies and deployments
- IPv6 comparison with IPv4

CHAPTER 8

Internet Protocol Version 6

This chapter reviews Internet Protocol Version 6 (IPv6) address structures, address assignments, representations, and mechanisms used to deploy IPv6. Expect plenty of questions about IPv6 on the exam. The CCDA must understand how an IPv6 address is represented and the different types of IPv6 addresses. This chapter also covers the benefits of IPv6 over IPv4 and compares the protocols.

As IPv6 matures, different deployment models will be used to implement the new protocol with existing IPv4 networks. This chapter covers these models at a high level. This chapter does not discuss the configuration of IPv6 because it is not a requirement for CCDA certification.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 8-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 8-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
IPv6 Header	1, 2
IPv6 Address Representation	5, 8, 9
IPv6 Address Types and Address Allocations	3, 4, 7
IPv6 Mechanisms	10
IPv4 to IPv6 Transition Strategies and Deployments	6

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. IPv6 uses how many more bits for addresses than IPv4?
   a. 32
   b. 64
   c. 96
   d. 128
2. What is the length of the IPv6 header?
   a. 20 bytes
   b. 30 bytes
   c. 40 bytes
   d. Same size as the IPv4 header
3. What address type is the IPv6 address FE80::300:34BC:123F:1010?
   a. Aggregatable global
   b. Site-local
   c. Link-local
   d. Multicast
4. What are three types of IPv6 addresses?
   a. Unicast, multicast, broadcast
   b. Unicast, anycast, broadcast
   c. Unicast, multicast, endcast
   d. Unicast, anycast, multicast
5. What is a compact representation of the address 3f00:0000:0000:a7fb:0000:0000:b100:0023?
   a. 3f::a7fb::b100:0023
   b. 3f00::a7fb:0000:0000:b100:23
   c. 3f::a7fb::b1:23
   d. 3f00:0000:0000:a7fb::b1:23

6. What is NAT-PT?
   a. Network address translation-port translation. Translates RFC 1918 addresses to public IPv4 addresses.
   b. Network addressable transparent-port translation. Translates network addresses to ports.
   c. Network address translation-protocol translation. Translates between IPv4 and IPv6 addresses.
   d. Next address translation–port translation
7. What IPv6 address type replaces the IPv4 broadcast address?
   a. Unicast
   b. Multicast
   c. Broadcast
   d. Anycast
8. What is the IPv6 equivalent to 127.0.0.1?
   a. 0:0:0:0:0:0:0:0
   b. 0:0:0:0:0:0:0:1
   c. 127:0:0:0:0:0:0:1
   d. FF::1
9. Which of the following is an "IPv4-compatible" IPv6 address?
   a. ::180.10.1.1
   b. f000:0:0:0:0:0:180.10.1.1
   c. 180.10.1.1::
   d. 2010::180.10.1.1
10. Which protocol maps names to IPv6 addresses?
    a. Address Resolution Protocol (ARP)
    b. Network discovery (ND)
    c. Domain Name System (DNS)
    d. DNSv2

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

The following sections cover topics that you need to master for the CCDA exam. The section "IPv6 Header" covers each field of the IPv6 header, which helps you understand the protocol. The section "IPv6 Address Representation" covers the hexadecimal representation of IPv6 addresses and the compressed representation. The section "IPv6 Address Types" covers unicast, multicast, and anycast IPv6 addresses and the current allocations of IPv6 addresses.

The section "IPv6 Mechanisms" covers Internet Control Message Protocol Version 6 (ICMPv6), ND, address assignment and resolution, and IPv6 routing protocols. The section "IPv4 to IPv6 Transition Strategies and Deployments" covers dual-stack backbones, IPv6 over IPv4 tunnels, dual-stack hosts, and network address translation-protocol translation (NAT-PT).

Introduction to IPv6

You should become familiar at a high level with IPv6 specifications, addressing, and design. The driving motivation for the adoption of a new version of IP is the limitation imposed by the 32-bit address field in IPv4. In the 1990s, there was concern that the IP address space would be depleted soon. Although classless interdomain routing (CIDR) and NAT have slowed down the deployment of IPv6, its standards and deployments are becoming mature. IPv6 is playing a significant role in the deployment of IP services for wireless phones. Some countries such as Japan directed IPv6 compatibility back in 2005. Several IPv6 test beds include the 6bone and the 6ren. The 6bone was an IPv6 test bed that focused on testing standards, implementations, and transition and operational procedures. The 6bone has served its purpose and ceased to operate in 2006. The 6ren is an IPv6 network that serves research and educational institutions. Furthermore, the U.S. Federal government has mandated all agencies to support IPv6 by mid 2008.

The IPv6 specification provides 128 bits for addressing, a significant increase from 32 bits. The overall specification of IPv6 is in RFC 2460. Other RFCs describing IPv6 specifications are 3513, 3587, 3879, 2373, 2374, 2461, 1886, and 1981.

IPv6 includes the following enhancements over IPv4:

- **Expanded address space**—IPv6 uses 128-bit addresses instead of the 32-bit addresses in IPv4.
- **Globally unique IP addresses**—The additional address spaces allow each node to have a unique address and eliminate the need for NAT.
- **Fixed header length**—The IPv6 header length is fixed, allowing vendors to improve switching efficiency.
- **Improved option mechanism**—IPv6 options are placed in separate optional headers that are located between the IPv6 header and the transport layer header. The option headers are not required.

- **Address autoconfiguration**—This capability provides for dynamic assignment of IPv6 addresses. IPv6 hosts can automatically configure themselves, with or without a Dynamic Host Configuration Protocol (DHCP) server.
- **Support for labeling traffic flows**—Instead of the type-of-service field in IPv4, IPv6 enables the labeling of packets belonging to a particular traffic class for which the sender requests special handling. This support aids specialized traffic, such as real-time video.
- **Security capabilities**—IPv6 includes features that support authentication and privacy.
- **Maximum transmission unit (MTU) path discovery**—IPv6 eliminates the need to fragment packets by implementing MTU path discovery before sending packets to a destination.
- **Site multihoming**—IPv6 allows multihoming of hosts and networks to have multiple IPv6 prefixes, which facilitates connection to multiple ISPs.

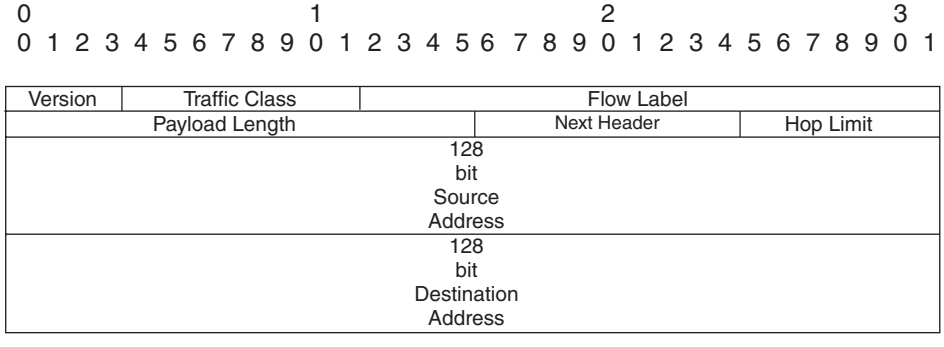
IPv6 Header

This section covers each field of the IPv6 header. The IPv6 header is simpler than the IPv4 header. Some IPv4 fields have been eliminated or changed to optional fields. The fragment offset fields and flags in IPv4 have been eliminated from the header. IPv6 adds a flow label field for quality-of-service (QoS) mechanisms to use.

The use of 128 bits for source and destination addresses provides a significant improvement over IPv4. With 128 bits, there are 3.4 * 10^{38} or 34 billion billion billion billion IPv6 addresses, compared to only 4.3 billion IPv4 addresses.

IPv6 improves over IPv4 by using a fixed-length header. The IPv6 header appears in Figure 8-1.

Figure 8-1 *IPv6 Header Format*



The following is a description of each field in the IP header:

- **Version**—This field is 4 bits long. It indicates the format, based on the version number, of the IP header. These bits are set to 0110 for IPv6 packets.
- **Traffic class**—This field is 8 bits in length. It describes the class or priority of the IPv6 packet and provides functionality similar to the IPv4 type-of-service field.
- **Flow label**—This field is 20 bits in length. It indicates a specific sequence of packets between a source and destination that requires special handling, such as real-time data (voice and video).
- **Payload length**—This field is 16 bits in length. It indicates the payload's size in bytes. Its length includes any extension headers.
- **Next header**—This field is 8 bits in length. It indicates the type of header that follows this IPv6 header. In other words, it identifies the upper-layer protocol. It uses values defined by the Internet Assigned Numbers Authority (IANA).
- **Hop limit**—This field is 8 bits in length. It is decremented by 1 by each router that forwards the packets. If this field is 0, the packet is discarded.
- **Source address**—This field is 128 bits in length. It indicates the sender's IPv6 address.
- **Destination address**—This field is 128 bits in length. It indicates the destination host's IPv6 address.

Notice that although the IPv6 address is four times the length of an IPv4 address, the IPv6 header is only twice the length (40 bytes). Optional network layer information is not included in the IPv6 header; instead, it is included in separate extended headers.

Two important extended headers are the Authentication Header (AH) and the Encapsulating Security Payload (ESP) header. These headers are covered later in the chapter.

IPv6 Address Representation

RFC 2373 specifies the IPv6 addressing architecture. IPv6 addresses are 128 bits in length. For display, the IPv6 addresses have eight 16-bit groups. The hexadecimal value is *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*, where each *x* represents four hexadecimal digits (16 bits).

An example of a full IPv6 address is 1111111000011010 0100001010111001 0000000000011011 0000000000000000 0000000000000000 0001001011010000 0000000001011011 0000011010110000.

The hexadecimal representation of the preceding IPv6 binary number is

FE1A:42B9:001B:0000:0000:12D0:005B:06B0

Groups with a value of 0 can be represented with a single 0. For example, you can also represent the preceding number as

FE1A:42B9:001B:0:0:12D0:005B:06B0

You can represent multiple groups of 16-bit 0s with ::, which might appear only once in the number. Also, you do not need to represent leading 0s in a 16-bit piece. The preceding IPv6 address can be further shortened to

FE1A:42B9:1B::12D0:5B:6B0

TIP Remember that the fully expanded address has eight blocks and that the double colon represents only 0s. You can use the double colon only once.

You expand a compressed address following the same rules used earlier. For example, the IPv6 address 2001:4C::50:0:0:741 expands as follows:

2001:004C::0050:0000:0000:0741

Because there should be eight blocks of addresses and you have six, you can expand the double colon to two blocks as follows:

2001:004C:0000:0000:0050:0000:0000:0741

IPv4-Compatible IPv6 Addresses

In a mixed IPv6/IPv4 environment, the IPv4 portion of the address requires the last two 16-bit blocks, or 32 bits of the address, which is represented in IPv4 dotted-decimal notation. The remaining portion of the IPv6 address is all 0s. Six hexadecimal 16-bit blocks are concatenated with the dotted-decimal format. The first 96 bits are 0, and the last 32 bits are used for the IPv4 address. This form is *x*:*x*:*x*:*x*:*x*:*x*:*d*.*d*.*d*.*d*, where each *x* represents the hexadecimal digits and *d*.*d*.*d*.*d* is the dotted-decimal representation.

An example of a mixed full address is 0000:0000:0000:0000:0000:0000:100.1.1.1; this example can be shortened to 0:0:0:0:0:0:100.1.1.1 or ::100.1.1.1.

IPv6 Prefix Representation

IPv6 prefixes are represented similar to IPv4, with the following format:

IPv6-address/prefix

The *IPv6-address* portion is a valid IPv6 address. The *prefix* portion is the number of contiguous bits that represent the prefix. You use the double colon only once in the representation. An example of an IPv6 prefix is 200C:001b:1100:0:0:0:0:0/40 or 200C:1b:1100::/40.

For another example, look at the representations of the 60-bit prefix 2001000000000ab0:

2001:0000:0000:0ab0:0000:0000:0000:0000/60
2001:0000:0000:0ab0:0:0:0:0/60
2001:0000:0000:ab0::/60
2001:0:0:ab0::/60

The rules for address representation are still valid when using a prefix. The following is not a valid representation of the preceding prefix:

2001:0:0:ab0/60

The preceding representation is missing the trailing double colon:

2001::ab0/60

The preceding representation expands to 2001:0:0:0:0:0:0:0ab0, which is not the prefix 2001:0000:0000:0ab0::/60.

When representing an IPv6 host address with its subnet prefix, you combine the two. For example, the IPv6 address 2001:0000:0000:0ab0:001c:1bc0:08ba:1c9a in subnet prefix 2001:0000:0000:0ab0::/60 is represented as the following:

2001:0000:0000:0ab0:001c:1bc0:08ba:1c9a/60

IPv6 Address Types and Address Allocations

This section covers the major types of IPv6 addresses. IPv4 addresses are unicast, multicast, or broadcast. IPv6 maintains each of these address functions, except that the IPv6 address types are defined a little differently. A special "all-nodes" IPv6 multicast address handles the broadcast function. IPv6 also introduces the anycast address type.

Also important to understand are the IPv6 address allocations. Sections of the IPv6 address space are reserved for particular functions, each of which is covered in this section. To provide you with a full understanding of address types, the following sections describe each type.

As mentioned earlier, there are three types of IPv6 addresses:

- Unicast
- Anycast
- Multicast

IPv6 Unicast Address

The IPv6 *unicast* (one-to-one) address is the logical identifier of a single-host interface. It is similar to IPv4 unicast classful (Class A, Class B, and Class C) addresses. Unicast addresses are divided into global and link-local addresses. A third type, site-local, has been deprecated in RFC 3879. These unicast address types are explained in the following sections.

IPv6 Anycast Address

The IPv6 *anycast* (one-to-nearest) address identifies a set of devices. An anycast address is allocated from a set of unicast addresses. These destination devices should share common characteristics and are explicitly configured for anycast.

You can use the anycast address to identify a set of routers or servers within an area. When a packet is sent to the anycast address, it is delivered to the nearest device as determined by the routing protocol. An example of the use of anycast addresses is to assign an anycast address to a set of servers—one in North America, and the other in Europe. Users in North America would be routed to the North American server, and those in Europe to the European server.

IPv6 Multicast Address

The IPv6 *multicast* (one-to-many) address identifies a set of hosts. The packet is delivered to all the hosts identified by that address. This type is similar to IPv4 multicast (Class D) addresses. IPv6 multicast addresses also supersede the broadcast function of IPv4 broadcasts. You use an "all-nodes" multicast address instead.

Some IPv6 multicast addresses are

FF01:0:0:0:0:0:0:1—Indicates all-nodes address for interface-local scope.
FF02:0:0:0:0:0:0:2—All-routers address for link-local.

IPv6 Address Allocations

The leading bits of an IPv6 address can define the IPv6 address type or other reservations. These leading bits are of variable length and are called the format prefix (FP). Table 8-2 shows the allocation of address prefixes. The IPv6 address space was delegated to IANA. You can find

current IPv6 allocations at http://www.iana.org/assignments/ipv6-address-space. Many prefixes are still unassigned.

Table 8-2 *IPv6 Prefix Allocation*

Binary Prefix	Hexadecimal/Prefix	Allocation
0000 0000	0000::/8	Unspecified, loopback, IPv4-compatible
0000 0001	0100::/8	Unassigned
0000 001	0200:/7	Unassigned
0000 010	0400::/7	Reserved for Internetwork Packet Exchange (IPX) allocation
0000 1	0800::/5	Unassigned
0001	1000::/4	Unassigned
001	2000::/3	Global unicast address
010	4000::/3	Unassigned
011	6000::/3	Unassigned
100	8000::/3	Reserved for geographic-based unicast addresses
101	A000::/3	Unassigned
110	C000::/3	Unassigned
1110	E000::/3	Unassigned
1111 0	F000::/5	Unassigned
1111 10	F800::/6	Unassigned
1111 110	FC00::/7	Unassigned
1111 1110 0	FE00::/9	Unassigned
1111 1110 10	FE80:/10	Link-local unicast addresses
1111 1110 11	FEC0::/10	Unassigned; was site-local unicast addresses (deprecated)
1111 1111	FF00::/8	Multicast addresses

Unspecified Address

An unspecified address is all 0s: 0:0:0:0:0:0:0:0. It signifies that an IPv6 address is not specified for the interface. Unspecified addresses are not forwarded by an IPv6 router.

Loopback Address

The IPv6 loopback address is 0:0:0:0:0:0:0:1. This address is similar to the IPv4 loopback address of 127.0.0.1.

IPv4-Compatible IPv6 Address

IPv4-compatible IPv6 addresses begin with 96 binary 0s (six 16-bit groups) followed by the 32-bit IPv4 address, as in 0:0:0:0:0:0:130.100.50.1 or just ::130.100.50.1.

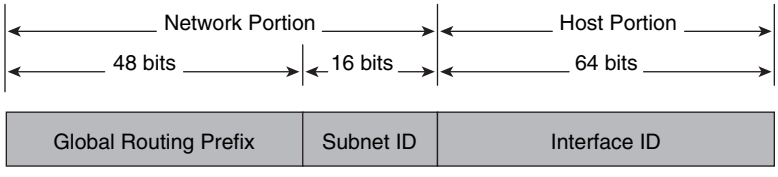
Global Unicast Addresses

IPv6 global addresses connect to the public network. These unicast addresses are globally unique and routable. This address format is initially defined in RFC 2374. RFC 3587 provides updates to the format.

The original specification defined the address format with a three-layer hierarchy: public topology, site topology, and interface identifier. The *public topology* consisted of service providers that provided transit services and exchanges of routing information. It used a Top-Level Aggregator (TLA) identifier and a next-level identifier. A site-level aggregator (SLA) was used for site topology. The *site topology* is local to the company or site and does not provide transit services. The TLA, NLA, and SLA identifiers are deprecated by RFC 3587. RFC 3587 simplifies these identifiers with a global routing prefix and subnet identifier for the network portion of the address.

Figure 8-2 shows the format of the standard IPv6 global unicast address. The global routing prefix is generally 48 bits in length, and the subnet ID is 16 bits. The interface ID is 64 bits in length and uniquely identifies the interface on the link.

Figure 8-2 *IPv6 Global Unicast Address Format*

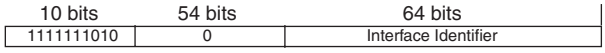


Link-Local Addresses

IPv6 link-local addresses are significant only to nodes on a single link. Routers do not forward packets with a link-local source or destination address beyond the local link. Link-local addresses are identified by leading FE8 hexadecimal numbers. Link-local addresses are configured automatically or manually.

As shown in Figure 8-3, the format of the link-local address is an FP of 1111111010, followed by 54 0s and a 64-bit interface identifier (ID). The interface ID is obtained automatically through communication with other nodes in the link. The interface ID is then concatenated with the link-local address prefix of FE80::/64 to obtain the interface link-local address.

Figure 8-3 *IPv6 Link-Local Address Format*



Site-Local Addresses

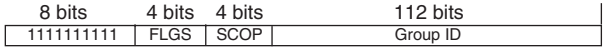
Site-local addresses were recently removed from IPv6 specifications. They are included here in case you encounter them in other references. IPv6 site-local addresses were meant to be analogous to IPv4 private addresses (RFC 1918). Site-local addresses were meant to be used within an organization and are not globally unique. Site-local addresses are not routable across a public network such as the Internet.

Multicast Addresses

IPv6 multicast addresses perform the same function as IPv4 multicast addresses. Multicast addresses send packets to all hosts in a group. IPv6 multicast addresses are identified by the leading FF hexadecimal numbers (an FP value of 11111111). One additional function of IPv6 multicast is to provide the IPv4 broadcast equivalent with the all-nodes multicast group.

RFC 2373 specifies the format of IPv6 multicast addresses. As shown in Figure 8-4, the fields of the IPv6 multicast address are the FP, a value of 0xFF, followed by a 4-bit flags field, a 4-bit scope field, and 112 bits for the group identifier (ID).

Figure 8-4 *Multicast Address Format*



The FLGS (flags) field consists of three leading 0s followed by a T bit: 000T. If T = 0, the address is a well-known multicast address assigned by the global IANA. If T = 1, the address is not a permanently assigned address.

The SCOP (scope) field limits the scope of the multicast group. Table 8-3 shows the assigned scope values.

Table 8-3 *Multicast Scope Assignments*

SCOP (Binary)	SCOP (Hexadecimal)	Assignment
0000	0	Reserved
0001	1	Node-local scope
0010	2	Link-local scope
0011	3	Unassigned

Table 8-3 *Multicast Scope Assignments (Continued)*

SCOP (Binary)	SCOP (Hexadecimal)	Assignment
0100	4	Admin-local scope
0101	5	Site-local scope
0110	6	Unassigned
0111	7	Unassigned
1000	8	Organization-local scope
1001	9	Unassigned
1010	A	Unassigned
1011	B	Unassigned
1100	C	Unassigned
1101	D	Unassigned
1110	E	Global scope
1111	F	Reserved

The group ID identifies the multicast group within the given scope. The group ID is independent of the scope. A group ID of 0:0:0:0:0:0:1 identifies nodes, whereas a group ID of 0:0:0:0:0:0:2 identifies routers. Some well-known multicast addresses appear in Table 8-4 associated with a variety of scope values.

Table 8-4 *Well-Known Multicast Addresses*

Multicast Address	Multicast Group
FF01::1	All nodes (node-local)
FF02::1	All nodes (link-local)
FF01::2	All routers (node-local)
FF02::2	All routers (link-local)
FF02::5	Open Shortest Path First version 3 (OSPFv3)
FF02::6	OSPFv3 designated routers
FF02::9	Routing Information Protocol (RIPng)
FF02::A	EIGRP routers
FF02::B	Mobile agents
FF02::C	DHCP servers/relay agents
FF02::D	All Protocol Independent Multicast (PIM) routers

IPv6 Mechanisms

The changes to the 128-bit address length and IPv6 header format modified the underlying protocols that support IP. This section covers ICMPv6, IPv6 ND, address resolution, address assignment, and IPv6 routing protocols. These protocols must now support 128-bit addresses. For example, DNS adds a new record locator for resolving fully qualified domain names (FQDN) to IPv6 addresses. IPv6 also replaces ARP with the IPv6 ND protocol. IPv6 ND uses ICMPv6.

ICMPv6

ICMP needed some modifications to support IPv6. RFC 2463 describes the use of ICMPv6 for IPv6 networks. All IPv6 nodes must implement ICMPv6 to perform network layer functions. ICMPv6 performs diagnostics (ping), reports errors, and provides reachability information. Although IPv4 ICMP uses IP protocol 1, IPv6 uses a Next Header number of 58.

Informational messages are

- Echo request
- Echo reply

Some error messages are

- Destination unreachable
- Packet too big
- Time exceeded
- Parameter problem

The destination-unreachable messages also provide further details:

- No route to destination
- Destination administratively prohibited
- Address unreachable
- Port unreachable

Other IPv6 mechanisms use ICMPv6 to determine neighbor availability, path MTU, destination address, or port reachability.

IPv6 Network Discovery (ND) Protocol

IPv6 does not implement the ARP that is used in IPv4. Instead, IPv6 implements the ND protocol described in RFC 2461. Hosts use ND to implement plug-and-play functions that discover all other nodes in the same link, check for duplicate addresses, and find routers in the link. The protocol also searches for alternative routers if the primary fails.

The IPv6 ND protocol performs the following functions:

- **Address autoconfiguration**—The host can determine its full IPv6 address without the use of DHCP.
- **Duplicate address detection**—The host can determine whether the address it will use is already in use on the network.
- **Prefix discovery**—The host finds out the link's IPv6 prefix.
- **Parameter discovery**—The host finds out the link's MTU and hop count.
- **Address resolution**—The host can determine the MAC address of other nodes without the use of ARP.
- **Router discovery**—The host finds local routers without the use of DHCP.
- **Next-hop determination**—The host can determine a destination's next hop.
- **Neighbor unreachability detection**—The host can determine whether a neighbor is no longer reachable.
- **Redirect**—The host can tell another host if a preferred next hop exists to reach a particular destination.

IPv6 ND uses ICMPv6 to implement some of its functions. These ICMPv6 messages are

- **Router Advertisement (RA)**—Sent by routers to advertise their presence and link-specific parameters.
- **Router Solicitation (RS)**—Sent by hosts to request RA from local routers.
- **Neighbor Solicitation (NS)**—Sent by hosts to request link layer addresses of other hosts. Also used for duplicate address detection.
- **Neighbor Advertisement (NA)**—Sent by hosts in response to an NS.
- **Redirect**—Sent to a host to notify it of a better next hop to a destination.

The link address resolution process uses Neighbor Solicitation (NS) messages to obtain a neighbor's link layer address. Nodes respond with a Neighbor Advertisement (NA) message that contains the link layer address.

IPv6 Name Resolution

IPv4 uses A records to provide FQDN name-to-IPv4 address resolution. DNS adds a resource record (RR) to support name-to-IPv6-address resolution. RFC 3596 describes the addition of a new DNS resource record type to support transition to IPv6 name resolution. The new record type is AAAA, commonly known as "quad-A." Given a domain name, the AAAA record returns an IPv6 address to the requesting host.

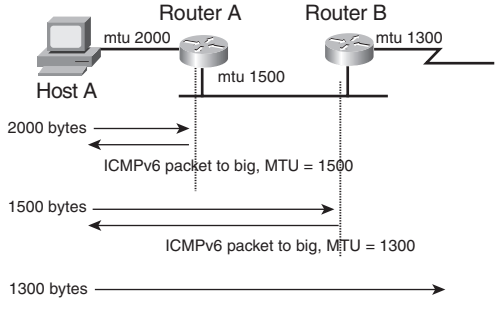
RFC 2874 specifies another DNS record for IPv6; it defines the A6 resource record. The A6 record provides additional features and is intended as a replacement for the AAAA RR. Current DNS implementations need to be able to support A (for IPv4), A6, and AAAA resource records, with type A having the highest priority and AAAA the lowest.

Path MTU Discovery

IPv6 does not allow packet fragmentation throughout the internetwork. Only sending hosts are allowed to fragment. Routers are not allowed to fragment packets. RFC 2460 specifies that the MTU of every link in an IPv6 must be 1280 bytes or greater. RFC 1981 recommends that nodes should implement IPv6 path MTU discovery to determine whether any paths are greater than 1280 bytes. ICMPv6 packet-too-big error messages determine the path MTU. Nodes along the path send the ICMPv6 packet-too-big message to the sending host if the packet is larger than the outgoing interface MTU.

Figure 8-5 shows a host sending a 2000-byte packet. Because the outgoing interface MTU is 1500 bytes, Router A sends an ICMPv6 packet-too-big error message back to Host A. The sending host then sends a 1500-byte packet. The outgoing interface MTU at Router B is 1300 bytes. Router B sends an ICMPv6 packet-too-big error message to Host A. Host A then sends the packet with 1300 bytes.

Figure 8-5 *ICMPv6 Packet-Too-Big Message*



IPv6 Address-Assignment Strategies

An IPv6 host can obtain its address through autoconfiguration or from the DHCP. DHCP is a stateful method of address assignment. IPv6 nodes might or might not use DHCPv6 to acquire IP address information.

Autoconfiguration of Link-Local Address

IPv6 hosts can use a stateless autoconfiguration method, without DHCP, to acquire their own IP address information. Hosts obtain their link-local addresses automatically as an interface is initialized. First, the host performs a duplicate address-detection process. The host joins the all-nodes multicast group to receive neighbor advertisements from other nodes. The neighbor advertisements include the subnet or prefix associated with the link. The host then sends a neighbor-solicitation message with the tentative IP address (interface identifier) as the target. If a host is already using the tentative IP address, that host replies with a neighbor advertisement. If the host receives no neighbor advertisement, the target IP address becomes the link-local address of the originating host.

DHCPv6

DHCPv6 is the updated version of DHCP that provides dynamic IP address assignment for IPv6 hosts. DHCPv6 is described in RFC 3315. It provides the same functions as DHCP, with more control than stateless autoconfiguration, and it supports renumbering without routers. DHCPv6 assignment is stateful, whereas IPv6 link-local autoconfiguration is not.

IPv6 Security

IPv6 has two integrated mechanisms to provide security for communications. It natively supports IP Security (IPSec). IPSec is mandated at the operating-system level for all IPSec hosts. RFC 2401 describes IPSec. Extension headers carry the IPSec AH and ESP header. The AH provides authentication and integrity. The ESP header provides confidentiality by encrypting the payload. For IPv6, the AH defaults to message digest algorithm 5 (MD5), and the ESP encryption defaults to data encryption standard-cipher block chaining (DES-CBC).

A description of the IPSec mechanisms appears in Chapter 13, “Security Solutions.” More information also appears in RFC 2402, *IP Authentication Header*, and in RFC 2406, *IP Encapsulating Security Payload (ESP)*.

IPv6 Routing Protocols

New routing protocols have been developed to support IPv6, such as RIPng, Integrated Intermediate System-to-Intermediate System (i/IS-IS), EIGRP for IPv6, and OSPFv3. Border Gateway Protocol (BGP) also includes changes that support IPv6. Enhanced Interior Gateway Routing Protocol (EIGRP) also now supports IPv6.

RIPng for IPv6

RFC 2080 describes changes to RIP to support IPv6 networks, called RIP next generation (RIPng). RIP mechanisms remain the same. RIPng still has a 15-hop limit, counting to infinity, and split horizon with poison reverse. Instead of User Datagram Protocol (UDP) Port 520 for RIPv2, RIPng uses UDP Port 521. RIPng supports IPv6 addresses and prefixes. Cisco IOS Software currently supports RIPng. RIPng uses multicast group FF02::9 for RIP updates to all RIP routers.

EIGRP for IPv6

Cisco has developed EIGRP support for IPv6 networks to route IPv6 prefixes. EIGRP for IPv6 is configured and managed separately from EIGRP for IPv4; no network statements are used. EIGRP for IPv6 retains all the characteristics (network discovery, DUAL, modules) and functions of EIGRP for IPv4. EIGRP uses multicast group FF02::A for EIGRP updates.

OSPFv3 for IPv6

RFC 2740 describes OSPF Version 3 to support IPv6 networks. OSPF algorithms and mechanisms (flooding, designated router [DR] election, areas, shortest path first [SPF] calculations) remain the same. Changes are made for OSPF to support IPv6 addresses, address hierarchy, and IPv6 for transport. Cisco IOS Software currently supports OSPFv3.

OSPFv3 uses multicast group FF02::5 for all OSPF routers and FF02::6 for all designated routers.

IS-IS for IPv6

Specifications for routing IPv6 with integrated IS-IS are currently an Internet draft of the IETF. The draft specifies new type, length, and value (TLV) objects, reachability TLVs, and an interface address TLV to forward IPv6 information in the network. IOS supports IS-IS for IPv6 as currently described in the draft standard.

BGP4 Multiprotocol Extensions for IPv6

RFC 2545 specifies the use of BGP attributes for passing on IPv6 route information. The MP_REACH_NLRI (multiprotocol-reachable) attribute describes reachable destinations. It includes the next-hop address and a list of Network Layer Reachability Information (NLRI) prefixes of reachable networks. The MP_UNREACH_NLRI (multiprotocol-unreachable) attribute conveys unreachable networks. IOS currently supports these BGP4 multiprotocol attributes to communicate reachability information for IPv6 networks.

IPv4 to IPv6 Transition Strategies and Deployments

Several deployment models exist to migrate from an IPv4 network to IPv6. During a transition time, both protocols can coexist in the network. The deployment models are

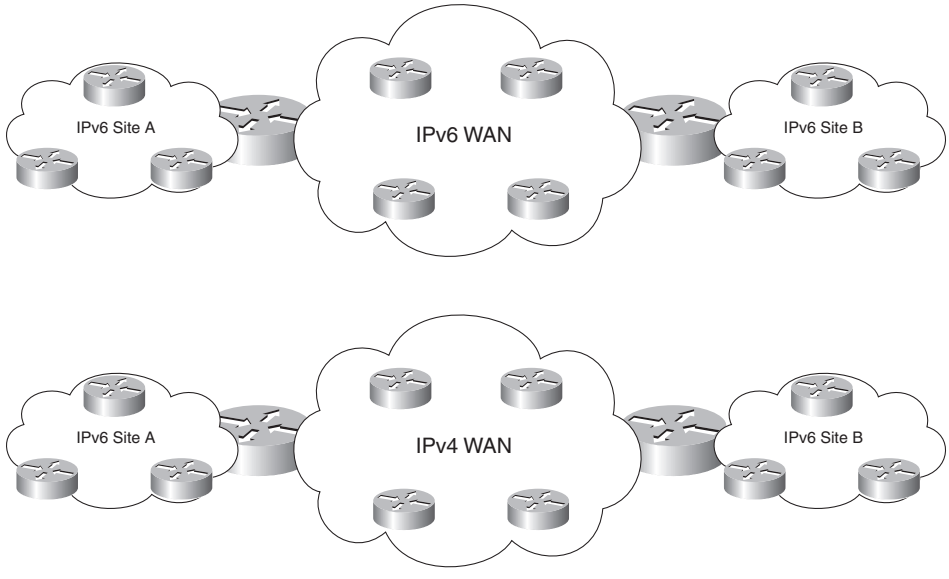
- IPv6 over dedicated WAN links
- IPv6 over IPv4 tunnels
- IPv6 using dual-stack backbones
- Protocol translation

Each model provides several advantages and disadvantages with which you should become familiar. The following sections describe each model.

IPv6 over Dedicated WAN Links

In this deployment model, all nodes and links use IPv6 hierarchy, addressing, and protocols. It is not a transition model, but a new, separate deployment of IPv6. The WAN in this model uses IPv6. The disadvantage of this model is that additional costs are incurred when separate links are used for IPv6 WAN circuits during the transition to using IPv6 exclusively. As shown in Figure 8-6, a company needs both IPv6 and IPv4 networks in sites A and B during the IPv6 deployment and transition. The networks are connected using separate WANs.

Figure 8-6 *Dedicated IPv6 WAN*



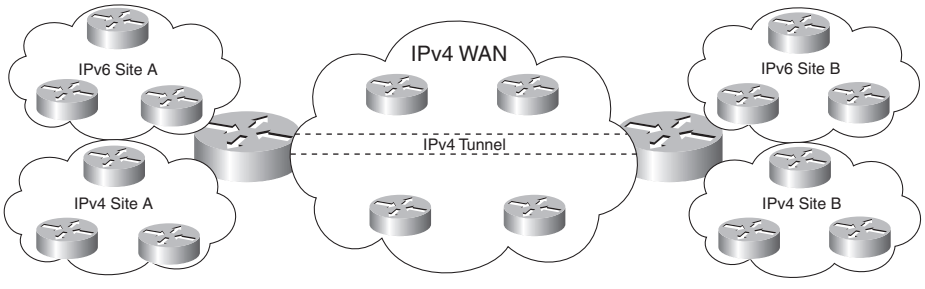
IPv6 over IPv4 Tunnels

In this deployment model, pockets of IPv6-only networks are connected using IPv4 tunnels. With tunneling, IPv6 traffic is encapsulated within IPv4 packets so that they are sent over the IPv4 WAN. The advantage of this method is that you do not need separate circuits to connect the IPv6 networks. A disadvantage of this method is the increased protocol overhead of the encapsulated IPv6 headers. Tunnels are created manually, semiautomatedly, or automatically using 6to4.

RFC 3056 specifies the 6to4 method for transition by assigning an interim unique IPv6 prefix. 2002::/16 is the assigned range for 6to4. Each 6to4 site uses a /48 prefix that is concatenated with 2002.

Figure 8-7 shows a network using IPv4 tunnels. Site A and Site B both have IPv4 and IPv6 networks. The IPv6 networks are connected using an IPv4 tunnel in the WAN.

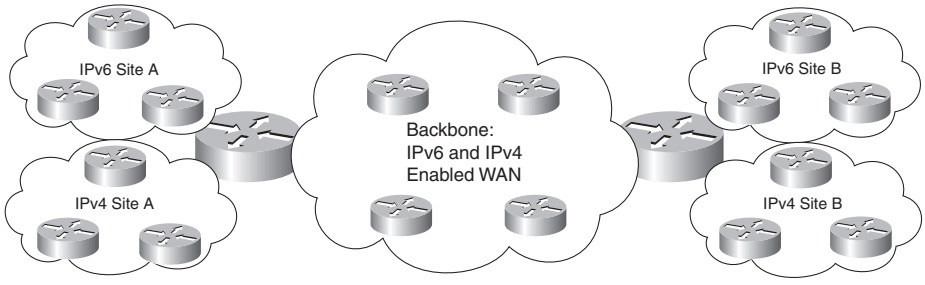
Figure 8-7 *IPv6 over IPv4 Tunnels*



Dual-Stack Backbones

In this model, all routers in the backbone are dual-stack, capable of routing both IPv4 and IPv6 packets. The IPv4 protocol stack is used between IPv4 hosts, and the IPv6 protocol stack is used between IPv6 hosts. This deployment model works for organizations with a mixture of IPv4 and IPv6 applications. Figure 8-8 shows a network with a dual-stack backbone. All the WAN routers run both IPv4 and IPv6 routing protocols. The disadvantages are that the WAN routers require dual addressing, run two routing protocols, and might require additional CPU and memory resources. Another disadvantage is that IPv4-only and IPv6-only hosts cannot communicate with each other directly; dual-stack hosts or network translation is required (covered next) for IPv4 and IPv6 hosts to communicate.

Figure 8-8 *Dual-Stack Backbone*



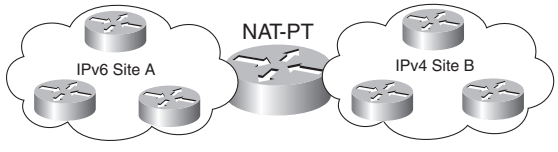
Dual-Stack Hosts

Hosts require dual stacks (IPv4 and IPv6) to communicate with both IPv4 and IPv6 hosts. In this environment, host applications can communicate with both IPv4 and IPv6 stacks. When using dual stacks, a host uses DNS to determine which stack to use to reach a destination. If DNS returns an IPv6 (A6 record) address to the host, the host uses the IPv6 stack. If DNS returns an IPv4 (A record) address to the host, the host uses the IPv4 stack. Using dual stacks is the method recommended for campus and access networks during a transition to IPv6.

Protocol Translation Mechanisms

One of the mechanisms for an IPv6-only host to communicate with an IPv4-only host without using dual stacks is protocol translation. RFC 2766 describes NAT-PT, which provides translation between IPv6 and IPv4 hosts. NAT-PT operates similarly to the NAT mechanisms to translate IPv4 private addresses to public address space. NAT-PT binds addresses in the IPv6 network to addresses in the IPv4 network and vice versa. Figure 8-9 shows a network using NAT-PT.

Figure 8-9 *Network Address Translation-Protocol Translation*



IPv6 Comparison with IPv4

This section provides a summary comparison of IPv6 to IPv4. Become knowledgeable about the characteristics summarized in Table 8-5. The use of 128 bits over 32 bits is an obvious change.

The upper-layer protocol is identified with the next header field in IPv6, which was the protocol type field used in IPv4. ARP is replaced by IPv6 ND.

Table 8-5 *IPv6 and IPv4 Characteristics*

Characteristic	IPv6	IPv4
Address length	128 bits	32 bits
Address representation	Hexadecimal	Dotted-decimal
Header length	Fixed (40 bytes)	Variable
Upper-layer protocols	Next header field	Protocol type field
Link address resolution	ND	ARP
Address configuration	Stateless autoconfiguration or stateful DHCP	Stateful DHCP
DNS (name-to-address resolution)	A6 records	A records
Interior routing protocols	EIGRPv6, OSPFv3, RIPng, IS-IS for IPv6	EIGRP, OSPFv2, RIPv2, IS-IS
Classification and marking	Traffic class and flow label fields, Differentiated Services Code Point (DSCP)	IP precedence bits, type-of-service field, DSCP
Private addresses	Site-local addresses	RFC 1918 private address space
Fragmentation	Sending host only	Sending host and intermediate routers
Loopback address	0:0:0:0:0:0:0:1	127.0.0.1
Address types	Unicast, anycast, multicast	Unicast, multicast, broadcast

References and Recommended Readings

Carpenter, B. and K. Moore. RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*. Available from http://www.ietf.org/rfc.

Coltun, R., D. Ferguson, and J. Moy. RFC 2740, *OSPF for IPv6*. Available from http://www.ietf.org/rfc.

Conta, A. and S. Deering. RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. Available from http://www.ietf.org/rfc.

Crawford, M. and C. Huitema. RFC 2874, *DNS Extensions to Support IPv6 Address Aggregation and Renumbering*. Available from http://www.ietf.org/rfc.

Deering, S. and R. Hinden. RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*. Available from http://www.ietf.org/rfc.

Doyle, J. and J. Carroll. *Routing TCP/IP*, Volume I, Second Edition. Indianapolis: Cisco Press, 2005.

Doyle, J. and J. Carroll. *Routing TCP/IP*, Volume II. Indianapolis: Cisco Press, 2001.

Droms, R., editor, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. Available from http://www.ietf.org/rfc.

Hinden, R. and S. Deering. RFC 2373, *IP Version 6 Addressing Architecture*. Available from http://www.ietf.org/rfc.

Hinden, R. and S. Deering. RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*. Available from http://www.ietf.org/rfc.

Hinden, R., S. Deering, and E. Nordmark. RFC 3587, *IPv6 Global Unicast Address Format*. Available from http://www.ietf.org/rfc.

Hinden R., M. O'Dell, and S. Deering. RFC 2374, *An IPv6 Aggregatable Global Unicast Address Format*. Available from http://www.ietf.org/rfc.

Hopps, C. *Routing IPv6 for IS-IS* (draft). Available from http://www.simpleweb.org/ietf/internetdrafts/complete/draft-ietf-isis-ipv6-03.txt.

Huitema, C. and B. Carpenter. RFC 3879, *Deprecating Site Local Addresses*. Available from http://www.ietf.org/rfc.

"Implementing IPv6 Networks Training." http://www.cisco.com/application/pdf/en/us/guest/tech/tk373/c1482/ccmigration_09186a008019d70b.pdf.

Kent, S. and R. Atkinson. RFC 2401, *Security Architecture for the Internet Protocol*. Available from http://www.ietf.org/rfc.

Kent, S. and R. Atkinson. RFC 2402, *IP Authentication Header*. Available from http://www.ietf.org/rfc.

Kent, S. and R. Atkinson. RFC 2406, *IP Encapsulating Security Payload (ESP)*. Available from http://www.ietf.org/rfc.

Malkin, G. and R. Minnear. RFC 2080, *RIPng for IPv6*. Available from http://www.ietf.org/rfc.

Marques, P. and F. Dupont. RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*. Available from http://www.ietf.org/rfc.

McCann, J., S. Deering, and J. Mogul. RFC 1981, *Path MTU Discovery for IP version 6*. Available from http://www.ietf.org/rfc.

Narten, T., E. Nordmark, and W. Simpson. RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*. Available from http://www.ietf.org/rfc.

Thomson, S. and C. Huitema. RFC 1886, *DNS Extensions to Support IP Version 6*. Available from http://www.ietf.org/rfc.

Tsirtsis, G. and P. Srisuresh. RFC 2766, *Network Address Translation – Protocol Translation (NAT-PT)*. Available from http://www.ietf.org/rfc.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the three types of IPv6 addresses:

- **Unicast**—The logical identifier of a single host. Unicast addresses are global unicast or link-local unicast.
- **Anycast**—Identifies a set of devices. The packet is delivered to the nearest device as determined by the routing protocol.
- **Multicast**—Identifies a set of hosts. The packet is delivered to all the hosts.

Table 8-6 provides a quick look at the current IPv6 allocations. Be able to identify the allocation based on the leading binary or hexadecimal numbers.

Table 8-6 *IPv6 Prefix Allocations*

Binary Prefix	Hexadecimal/Prefix	Allocation
0000 0000	0000::/8	Unspecified, loopback, IPv4-compatible
0000 0001	0100::/8	Unassigned
0000 001	0200:/7	Unassigned
0000 010	0400::/7	Reserved for Internetwork Packet Exchange (IPX) allocation
0000 1	0800::/5	Unassigned
0001	1000::/4	Unassigned
001	2000::/3	Global unicast address
010	4000::/3	Unassigned
011	6000::/3	Unassigned
100	8000::/3	Reserved for geographic-based unicast addresses
101	A000::/3	Unassigned
110	C000::/3	Unassigned
1110	E000::/3	Unassigned

continues

Table 8-6 *IPv6 Prefix Allocations (Continued)*

Binary Prefix	Hexadecimal/Prefix	Allocation
1111 0	F000::/5	Unassigned
1111 10	F800::/6	Unassigned
1111 110	FC00::/7	Unassigned
1111 1110 0	FE00::/9	Unassigned
1111 1110 10	FE80:/10	Link-local unicast addresses
1111 1110 11	FEC0::/10	Unassigned; was site-local unicast addresses (deprecated)
1111 1111	FF00::/8	Multicast addresses

Table 8-7 is actually a review of Table 8-5. It is presented again in this section because it is essential for the exam. It provides a quick summary of IPv6 characteristics compared to IPv4. Study this table in detail.

Table 8-7 *IPv6 and IPv4 Characteristics*

Characteristic	IPv6	IPv4
Address length	128 bits	32 bits
Address representation	Hexadecimal	Dotted-decimal
Header length	Fixed (40 bytes)	Variable
Upper-layer protocols	Next header field	Protocol type field
Link address resolution	ND	ARP
Address configuration	Stateless autoconfiguration or stateful DHCP	Stateful DHCP
DNS (name-to-address resolution)	A6 records	A records
Interior routing protocols	EIGRP for IPv6, OSPFv3, RIPng, IS-IS for IPv6	EIGRP, OSPFv2, RIPv2, IS-IS
Classification and marking	Traffic class and flow label fields, DSCP	IP precedence bits, type-of-service field, DSCP
Fragmentation	Sending host only	Sending host and intermediate routers
Loopback address	0:0:0:0:0:0:0:1	127.0.0.1
Address types	Unicast, anycast, multicast	Unicast, multicast, broadcast

Table 8-8 describes each field in the 40-byte IP header.

Table 8-8 *IPv6 Header Fields*

IPv6 Header Field	Description
Version	This field is 4 bits in length. It indicates the format, based on the version number, of the IP header. These bits are set to 0110 for IPv6 packets.
Traffic class	This field is 8 bits in length. It describes the IPv6 packet's class or priority and provides similar functionality to the IPv4 type-of-service field.
Flow label	This field is 20 bits in length. It indicates a specific sequence of packets between a source and destination that requires special handling, such as real-time data (voice and video).
Payload length	This field is 16 bits in length. It indicates the payload's size in bytes. Its length includes any extension headers.
Next header	This field is 8 bits in length. It indicates the type of header that follows this IPv6 header.
Hop limit	This field is 8 bits in length. It is decremented by 1 by each router that forwards the packets. If this field is 0, the packet is discarded.
Source address	This field is 128 bits in length. It indicates the sender's IPv6 address.
Destination address	This field is 128 bits in length. It indicates the destination host's IPv6 address.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: OSPFv2 supports IPv6.
2. True or false: DNS A6 records are used in IPv6 networks for name-to-IPv6-address resolution.
3. Fill in the blank: IPv6 ND is similar to what _____ does for IPv4 networks.
4. How many bits are there between the colons of IPv6 addresses?
5. The first field of the IPv6 header is 4 bits in length. What binary number is it always set to?
6. True or false: DHCP is required for dynamic allocation of IPv6 addresses.
7. IPv6 multicast addresses begin with what hexadecimal numbers?
8. IPv6 link-local addresses begin with what hexadecimal prefix?
9. True or false: 6to4 allows tunneling of IPv6 through IPv4 networks.
10. List the eight fields of the IPv6 header.
11. Which of the following is not an IPv6 address type?
    a. Unicast
    b. Broadcast
    c. Anycast
    d. Multicast
12. True or false: The IPv6 address 2001:0:0:1234:0:0:0:abcd can be represented as 2001::1234:0:0:0:abcd and 2001:0:0:1234::abcd.
13. What is the subnet prefix of 2001:1:0:ab0:34:ab1:0:1/64?
14. The IPv6 address has 128 bits. How many hexadecimal numbers does an IPv6 address have?
15. What type of IPv6 address is the following?

    FF01:0:0:0:0:0:0:2

16. What is the compact format of the address 2102:0010:0000:0000:0000:fc23:0100:00ab?

    a. 2102:10::fc23:01:ab

    b. 2102:001::fc23:01:ab

    c. 2102:10::fc23:100:ab

    d. 2102:0010::fc23:01:ab

17. When using the dual-stack backbone, which of the following statements is correct?

    a. The backbone routers have IPv4/IPv6 dual stacks, and end hosts do not.

    b. The end hosts have IPv4/IPv6 dual stacks, and backbone routers do not.

    c. Both the backbone routers and end hosts have IPv4/IPv6 dual stacks.

    d. Neither the backbone routers nor end hosts have IPv4/IPv6 dual stacks.

18. How does a dual-stack host know which stack to use to reach a destination?

    a. It performs an ND, which returns the destination host type.

    b. It performs a DNS request that returns the IP address. If the returned address is IPv4, the host uses the IPv4 stack. If the returned address is IPv6, the host uses the IPv6 stack.

    c. The IPv6 stack makes a determination. If the destination is IPv4, the packet is sent to the IPv4 stack.

    d. The IPv4 stack makes a determination. If the destination is IPv6, the packet is sent to the IPv6 stack.

19. Name at least two transition methods or technologies used to migrate from IPv4 to IPv6.

20. Which of the following describe(s) the IPv6 header?

    a. It is 40 bytes in length.

    b. It is of variable length.

    c. The Protocol Number field describes the upper-layer protocol.

    d. The Next Header field describes the upper-layer protocol.

21. Which of the following is true about fragmentation?

    a. Routers between source and destination hosts can fragment IPv4 and IPv6 packets.

    b. Routers between source and destination hosts cannot fragment IPv4 and IPv6 packets.

    c. Routers between source and destination hosts can fragment IPv6 packets only. IPv4 packets cannot be fragmented.

    d. Routers between source and destination hosts can fragment IPv4 packets only. IPv6 packets cannot be fragmented.

22. A packet sent to an anycast address reaches what?

    a. The nearest destination in a set of hosts

    b. All destinations in a set of hosts

    c. Broadcasts to all hosts

    d. Global unicast destinations

23. Which of the following is/are true about IPv6 and IPv4 headers?

    a. The IPv6 header is of fixed length, and the Next Header field describes the upper-layer protocol.

    b. The IPv4 header is of variable length, and the Protocol field describes the upper-layer protocol.

    c. The IPv6 header is of fixed length, and the Protocol field describes the upper-layer protocol.

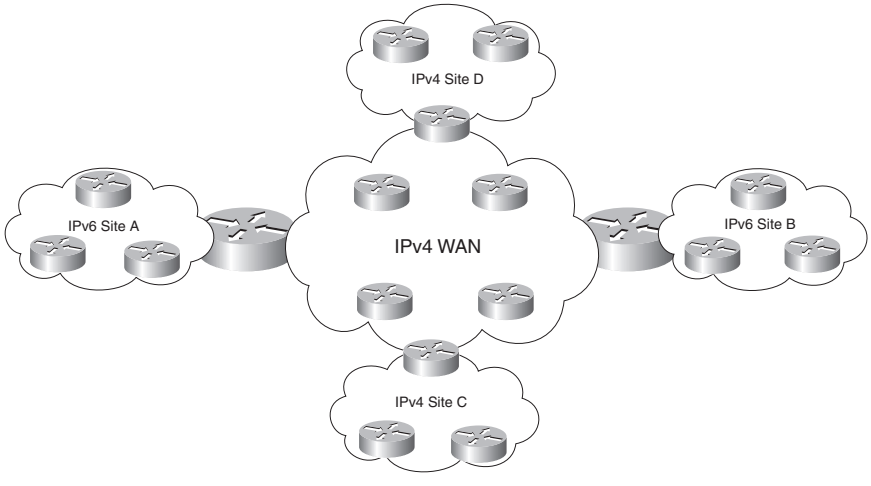
    d. A and B.

    e. B and C.

Answer the following questions based on the scenario and figure.

A company has an existing WAN that uses IPv4. Sites C and D use IPv4. As shown in Figure 8-10, the company plans to add two new locations (Sites A and B). The new sites will implement IPv6. The company does not want to lease more WAN circuits.

Figure 8-10 *Company Adds Sites A and B*



Answer the following questions.

24. What options does the company have to connect Site A to Site B?

25. What mechanism needs to be implemented so that IPv6 hosts can communicate with IPv4 hosts and vice versa?

26. If a dual-stack backbone is implemented, do all WAN routers and all hosts need an IPv6-IPv4 dual stack?

27. If an IPv4 tunnel is implemented between Sites A and B, do all WAN routers require an IPv6-IPv4 dual stack?

This chapter covers the following subjects:

- Routing protocol characteristics
- Routing protocol metrics and loop prevention
- ODR

CHAPTER 9

Routing Protocol Selection Criteria

This chapter covers the metrics used and other characteristics of routing protocols. Routing protocols can be categorized as distance-vector or link-state and as hierarchical or flat. The CCDA must understand how each routing protocol is categorized to select the one that meets the customer's requirements. This chapter covers the routing protocols at a high level. The following chapters dive into more detail on the operations and algorithms used in each routing protocol.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 9-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 9-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Routing Protocol Characteristics	1, 2, 3, 4, 7, 8
Routing Protocol Metrics and Loop Prevention	6
On-Demand Routing	5

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following routing protocols are classful?
   a. Routing Information Protocol Version 1 (RIPv1) and RIPv2
   b. Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF)
   c. Intermediate System-to-Intermediate System (IS-IS) and OSPF
   d. RIPv1 only
2. Which type of routing protocol would you use when connecting to an Internet service provider?
   a. Classless routing protocol
   b. Interior gateway protocol
   c. Exterior gateway protocol
   d. Classful routing protocol
3. Which routing protocol is distance-vector and classless?
   a. RIPv2
   b. EIGRP
   c. OSPF
   d. IS-IS
4. Which type of routing protocol sends periodic routing updates?
   a. Static
   b. Distance-vector
   c. Link-state
   d. Hierarchical
5. Which distance-vector routing protocol is used for IPv6 networks?
   a. OSPFv2
   b. RIPng
   c. OSPFv3
   d. BGPv3
6. Which of the following is true regarding routing metrics?
   a. If the metric is bandwidth, the path with the lowest bandwidth is selected.
   b. If the metric is bandwidth, the path with the highest bandwidth is selected.
   c. If the metric is bandwidth, the highest sum of the bandwidth is used to calculate the highest cost.
   d. If the metric is cost, the path with the highest cost is selected.

7. Both OSPF and EIGRP are enabled on a router with default values. Both protocols have a route to a destination network in their databases. Which route is entered into the routing table?

   a. The OSPF route.

   b. The EIGRP route.

   c. Both routes are entered with load balancing.

   d. Neither route is entered; an error has occurred.

8. Which of the following are classless routing protocols?

   a. RIPv1 and RIPv2

   b. EIGRP and RIPv2

   c. IS-IS and OSPF

   d. Answers B and C

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers the high-level characteristics of routing protocols and their metrics. You should become familiar with the different categories of routing protocols and their characteristics for the test. Understand how each metric is used and, based on the metric, which path is preferred. For example, you need to know that a path with the highest bandwidth is preferred over a path with lower bandwidth. This chapter also covers on-demand routing (ODR).

Routing Protocol Characteristics

This section discusses the different types and characteristics of routing protocols.

Characteristics of routing-protocol design are

- **Distance-vector, link-state, or hybrid**—How routes are learned
- **Interior or exterior**—For use in private networks or the public Internet
- **Classless (classless interdomain routing [CIDR] support) or classful**—CIDR enables aggregation of network advertisements (supernetting) between routers
- **Fixed-length or variable-length subnet masks (VLSM)**—Conserve addresses within a network
- **Flat or potentially hierarchical**—Addresses scalability in large internetworks
- **IPv4 or IPv6**—Newer routing protocols are used for IPv6 networks

This section also covers the default administrative distance assigned to routes learned from each routing protocol or from static assignment. Routes are categorized as statically (manually) configured or dynamically learned from a routing protocol. The following sections cover all these characteristics.

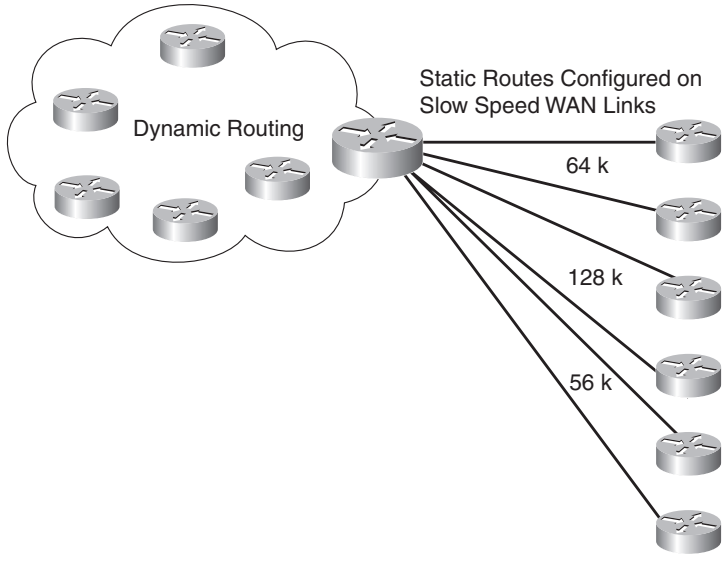
Static Versus Dynamic Route Assignment

Static routes are manually configured on a router. They do not react to network outages. The one exception is when the static route specifies the outbound interface: If the interface goes down, the static route is removed from the routing table. Because static routes are unidirectional, they must be configured for each outgoing interface the router will use. The size of today's networks makes it impossible to manually configure and maintain all the routes in all the routers in a timely manner. Human configuration can involve many mistakes, which is why routing protocols exist. They use algorithms to advertise and learn about changes in the network topology.

The main benefit of static routing is that a router generates no routing protocol overhead. Because no routing protocol is enabled, no bandwidth is consumed by route advertisements between network devices. Another benefit of static routing protocols is that they are easier to configure and troubleshoot than dynamic routing protocols. Static routing is recommended for hub-and-spoke topologies with a low-speed remote connection. A default static route is configured at each remote site because the hub is the only route used to reach all other sites. Static routers are also used at network boundaries (Internet or partners) where routing information is not exchanged. These static routes are then redistributed into the internal dynamic routing protocol used.

Figure 9-1 shows a hub-and-spoke WAN where static routes are defined in the remote WAN routers because no routing protocols are configured. This setup eliminates routing protocol traffic on the low-bandwidth WAN circuits.

Figure 9-1 *Static Routes in a Hub-and-Spoke Network*



Routing protocols dynamically determine the best route to a destination. When the network topology changes, the routing protocol adjusts the routes without administrative intervention. Routing protocols use a metric to determine the best path toward a destination network. Some use a single measured value such as hop count. Others compute a metric value using one or more parameters. Routing metrics are discussed later in this chapter. The following is a list of dynamic routing protocols:

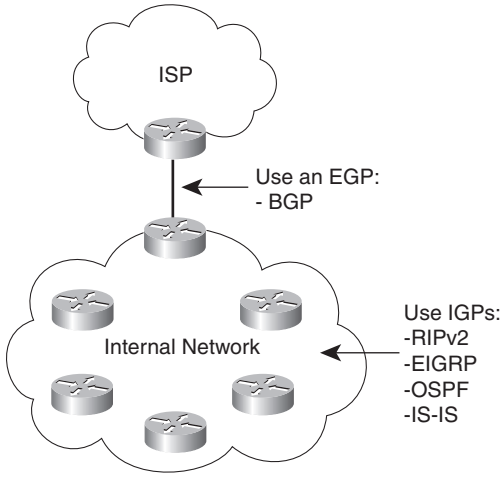
- RIPv1
- RIPv2

- IGRP
- EIGRP
- OSPF
- IS-IS
- RIPng
- OSPFv3
- EIGRP for IPv6
- Border Gateway Protocol (BGP)

Interior Versus Exterior Routing Protocols

Routing protocols can be categorized as interior gateway protocols (IGP) or exterior gateway protocols (EGP). IGPs are meant for routing within an organization's administrative domain—in other words, the organization's internal network. EGPs are routing protocols used to communicate with exterior domains. Figure 9-2 shows where an internetwork uses IGPs and EGPs with multiple autonomous administrative domains. BGP exchanges routing information between the internal network and an ISP. IGPs appear in the internal private network.

Figure 9-2 *Interior and Exterior Routing Protocols*



One of the first EGPs was called exactly that—Exterior Gateway Protocol. Today, BGP is the de facto (and the only available) exterior gateway protocol.

Potential IGPs for an IPv4 network are

- RIPv2
- OSPF
- IS-IS
- EIGRP

Potential IGPs for an IPv6 network are

- RIPng
- OSPFv3
- EIGRP for IPv6

RIPv1 is no longer recommended because RIPv2 is the most recent version of RIP. IGRP is an earlier version of EIGRP. IGRP is no longer a CCDA exam topic.

Distance-Vector Routing Protocols

The first IGP routing protocols introduced were distance-vector routing protocols. They used the Bellman-Ford algorithm to build the routing tables. With distance-vector routing protocols, routes are advertised as vectors of distance and direction. The distance metric is usually router hop count. The direction is the next-hop router (IP address) toward which to forward the packet. For RIP, the maximum number of hops is 15, which can be a serious limitation, especially in large nonhierarchical internetworks.

Distance-vector algorithms call for each router to send its entire routing table to only its immediate neighbors. The table is sent periodically (30 seconds for RIP and 90 seconds for IGRP). In the period between advertisements, each router builds a new table to send to its neighbors at the end of the period. Because each router relies on its neighbors for route information, it is commonly said that distance-vector protocols "route by rumor."

Having to wait half a minute for a new routing table with new routes is too long for today's networks. This is why distance-vector routing protocols have slow convergence.

RIPv2 and IGRP can send triggered updates—full routing table updates sent before the update timer has expired. A router can receive a routing table with 500 routes with only one route change, which creates serious overhead on the network—another drawback. Furthermore, RFC 2091 updates RIP with triggered extensions to allow triggered updates with only route changes. Cisco routers support this on fixed point-to-point interfaces.

The following is a list of IP distance-vector routing protocols:

- RIPv1 and RIPv2
- IGRP
- EIGRP (which could be considered a hybrid)
- RIPng

EIGRP

EIGRP is a hybrid routing protocol. It is a distance-vector protocol that implements some link-state routing protocol characteristics. Although EIGRP uses distance-vector metrics, it sends partial updates and maintains neighbor state information just as link-state protocols do. EIGRP does not send periodic updates as other distance-vector routing protocols do. The important thing to consider for the test is that EIGRP could be presented as a hybrid protocol. EIGRP metrics and mechanisms are discussed in Chapter 10, "RIP and EIGRP Characteristics and Design."

Link-State Routing Protocols

Link-state routing protocols address some of the limitations of distance-vector protocols. When running a link-state routing protocol, routers originate information about themselves (IP addresses), their connected links (the number and types of links), and the state of those links (up or down). The information is flooded to all routers in the network as changes in the link state occur. Each router makes a copy of the information received and forwards it without change. Each router independently calculates the best paths to each destination network, using a shortest path tree with itself as the root, and maintains a map of the network.

After the initial exchange of information, link-state updates are not sent unless a change in the topology occurs. Routers do send small Hello messages between neighbors to maintain neighbor relationships. If no updates have been sent, the routing table is refreshed after 30 minutes.

The following is a list of link-state routing protocols (including non-IP routing protocols):

- OSPF
- IS-IS
- OSPFv3
- IPX NetWare Link-Services Protocol (NLSP)

OSPF and IS-IS are covered in Chapter 11, "OSPF and IS-IS."

Distance-Vector Routing Protocols Versus Link-State Protocols

When choosing a routing protocol, consider that distance-vector routing protocols use more network bandwidth than link-state protocols. Distance-vector protocols generate more bandwidth overhead because of the large periodic routing updates. Link-state routing protocols do not generate significant routing update overhead but do use more router CPU and memory resources than distance-vector protocols. Generally, WAN bandwidth is a more expensive resource than router CPU and memory in modern devices.

Table 9-2 compares distance-vector to link-state routing protocols.

Table 9-2 *Distance-Vector Versus Link-State Routing Protocols*

Characteristic	Distance-Vector	Link-State
Scalability	Limited	Good
Convergence	Slow	Fast
Routing overhead	More traffic	Less traffic
Implementation	Easy	More complex
Protocols	RIPv1, RIPv2, IGRP, RIPng	OSPF, IS-IS, OSPFv3

EIGRP is a distance-vector protocol with link-state characteristics (hybrid) that give it high scalability, fast convergence, less routing overhead, and relatively easy configuration.

Hierarchical Versus Flat Routing Protocols

Some routing protocols require a network topology that must have a backbone network defined. This network contains some, or all, of the routers in the internetwork. When the internetwork is defined hierarchically, the backbone consists of only some devices. Backbone routers service and coordinate the routes and traffic to or from routers not in the local internetwork. The supported hierarchy is relatively shallow. Two levels of hierarchy are generally sufficient to provide scalability. Selected routers forward routes into the backbone. OSPF and IS-IS are hierarchical routing protocols.

Flat routing protocols do not allow a hierarchical network organization. They propagate all routing information throughout the network without dividing or summarizing large networks into smaller areas. Carefully designing network addressing to naturally support aggregation within routing-protocol advertisements can provide many of the benefits offered by hierarchical routing protocols. Every router is a peer of every other router in flat routing protocols; no router has a special role in the internetwork. RIPv1, IGRP, and RIPv2 are flat routing protocols. By default, EIGRP is a flat routing protocol, but it can be configured with manual summarization to support hierarchical designs.

Classless Versus Classful Routing Protocols

Routing protocols can be classified based on their support of VLSM and CIDR. Classful routing protocols do not advertise subnet masks in their routing updates; therefore, the configured subnet mask for the IP network must be the same throughout the entire internetwork. Furthermore, the subnets must, for all practical purposes, be contiguous within the larger internetwork. For example, if you use a classful routing protocol for network 130.170.0.0, you must use the chosen mask (such as 255.255.255.0) on all router interfaces using the 130.170.0.0 network. You must configure serial links with only two hosts and LANs with tens or hundreds of devices with the same mask of 255.255.255.0. The big disadvantage of classful routing protocols is that the network designer cannot take advantage of address summarization across networks (CIDR) or allocation of smaller or larger subnets within an IP network (VLSM). For example, with a classful routing protocol that uses a default mask of /25 for the entire network, you cannot assign a /30 subnet to a serial point-to-point circuit. Classful routing protocols are

- RIPv1
- IGRP

Classless routing protocols advertise the subnet mask with each route. You can configure subnetworks of a given IP network number with different subnet masks (VLSM). You can configure large LANs with a smaller subnet mask and configure serial links with a larger subnet mask, thereby conserving IP address space. Classless routing protocols also allow flexible route summarization and supernetting (CIDR). You create supernets by aggregating classful IP networks. For example, 200.100.100.0/23 is a supernet of 200.100.100.0/24 and 200.100.101.0/24. Classless routing protocols are

- RIPv2
- OSPF
- EIGRP
- IS-IS
- RIPng
- OSPFv3
- EIGRP for IPv6
- BGP

IPv4 Versus IPv6 Routing Protocols

With the increasing use of the IPv6 protocol, the CCDA must be prepared to design networks using IPv6 routing protocols. As IPv6 was defined, routing protocols needed to be updated to support the new IP address structure. None of the IPv4 routing protocols support IPv6 networks, and none of the IPv6 routing protocols are backward-compatible with IPv4 networks. But both protocols can coexist on the same network, each with their own routing protocol. Devices with dual stacks recognize which protocol is being used by the IP version field in the IP header.

RIPng is the IPv6-compatible RIP routing protocol. EIGRP for IPv6 is the new version of EIGRP that supports IPv6 networks. OSPFv3 was developed for IPv6, and OSPFv2 remains for IPv4. Internet drafts were written to provide IPv6 routing using IS-IS. Multiprotocol Extensions for BGP provide IPv6 support for BGP. Table 9-3 summarizes IPv4 versus IPv6 routing protocols.

Table 9-3 *IPv4 and IPv6 Routing Protocols*

IPv4 Routing Protocols	IPv6 Routing Protocols
RIPv1, RIPv2	RIPng
EIGRP	EIGRP for IPv6
OSPFv2	OSPFv3
IS-IS	IS-IS for IPv6
BGP	Multiprotocol Extensions for BGP

Administrative Distance

On Cisco routers running more than one routing protocol, it is possible for two different routing protocols to have a route to the same destination. Cisco routers assign each routing protocol an administrative distance. When multiple routes exist for a destination, the router selects the longest match. For example, if to reach a destination of 170.20.10.1 OSPF has a route prefix of 170.20.10.0/24 and EIGRP has a route prefix of 170.20.0.0/16, the OSPF route is preferred because the /24 prefix is longer than the /16 prefix. It is more specific.

In the event that two or more routing protocols offer the same route (with same prefix length) for inclusion in the routing table, the Cisco IOS router selects the route with the lowest administrative distance.

The administrative distance is a rating of the trustworthiness of a routing information source. Table 9-4 shows the default administrative distance for configured (static) or learned routes. In the table, you can see that static routes are trusted over dynamically learned routes. Within IGP routing protocols, EIGRP internal routes are trusted over OSPF, IS-IS, and RIP routes.

Table 9-4 *Default Administrative Distances for IP Routes*

IP Route	Administrative Distance
Connected interface	0
Static route directed to a connected interface	0
Static route directed to an IP address	1
EIGRP summary route	5
External BGP route	20
Internal EIGRP route	90
IGRP route	100
OSPF route	110
IS-IS route	115
RIP route	120
EGP route	140
External EIGRP route	170
Internal BGP route	200
Route of unknown origin	255

The administrative distance establishes the precedence used among routing algorithms. Suppose a router has an EIGRP route to network 172.20.10.0/24 with the best path out Ethernet 0 and an OSPF route for the same network out Ethernet 1. Because EIGRP has an administrative distance of 90 and OSPF has an administrative distance of 110, the router enters the EIGRP route in the routing table and sends packets with destinations of 172.20.10.0/24 out Ethernet 0.

Static routes have a default administrative distance of 1. There is one exception. If the static route points to a connected interface, it inherits the administrative distance of connected interfaces, which is 0. You can configure static routes with a different distance by appending the distance value to the end of the command.

Routing Protocol Metrics and Loop Prevention

Routing protocols use a metric to determine best routes to a destination. Some routing protocols use a combination of metrics to build a composite metric for best path selection. This section describes metrics and also covers routing loop-prevention techniques. You must understand each metric for the CCDA.

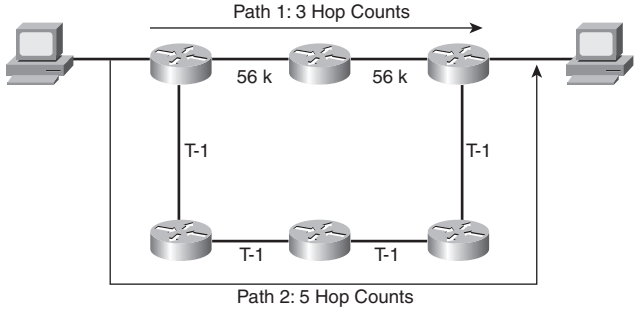
Some routing metric parameters are

- Hop count
- Bandwidth
- Cost
- Load
- Delay
- Reliability
- Maximum transmission unit (MTU)

Hop Count

The hop count parameter counts the number of links between routers the packet must traverse to reach a destination. The RIP routing protocol uses hop count as the metric for route selection. If all links were the same bandwidth, this metric would work well. The problem with routing protocols that use only this metric is that the shortest hop count is not always the most appropriate path. For example, between two paths to a destination network—one with two 56-kbps links and another with four T1 links—the router chooses the first path because of the lower number of hops (see Figure 9-3). However, this is not necessarily the best path. You would prefer to transfer a 20-MB file via the T1 links instead of the 56-kbps links.

Figure 9-3 *Hop Count Metric*

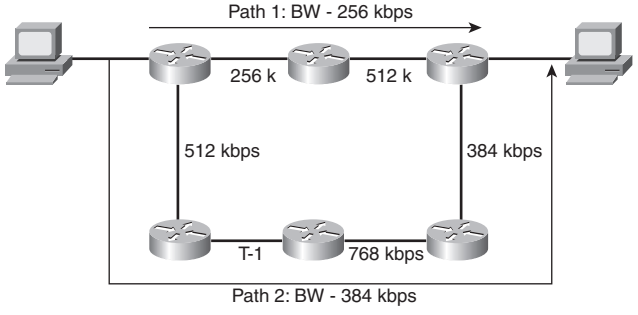


Bandwidth

The bandwidth parameter uses the interface bandwidth to determine a best path to a destination network. When bandwidth is the metric, the router prefers the path with the highest bandwidth to a destination. For example, a Fast Ethernet (100 Mbps) is preferred over a DS-3 (45 Mbps). As shown in Figure 9-3, a router using bandwidth to determine a path would select Path 2 because of the larger bandwidth, 1.5 Mbps over 56 kbps.

If a routing protocol uses only bandwidth as the metric and the path has several different speeds, the protocol can use the lowest speed in the path to determine the bandwidth for the path. EIGRP and IGRP use the minimum path bandwidth, inverted and scaled, as one part of the metric calculation. In Figure 9-4, Path 1 has two segments, with 256 kbps and 512 kbps of bandwidth. Because the smaller speed is 256 kbps, this speed is used as Path 1's bandwidth. The smallest bandwidth in Path 2 is 384 kbps. When the router has to choose between Path 1 and Path 2, it selects Path 2 because 384 kbps is larger than 256 kbps.

Figure 9-4 *Bandwidth Metric Example*



Cost

Cost is the name of the metric used by OSPF and IS-IS. In OSPF on a Cisco router, a link's default cost is derived from the interface's bandwidth.

Cisco's implementation of IS-IS assigns a default cost of 10 to all interfaces.

The formula to calculate cost in OSPF is

$$10^8/BW$$

where BW is the interface's default or configured bandwidth.

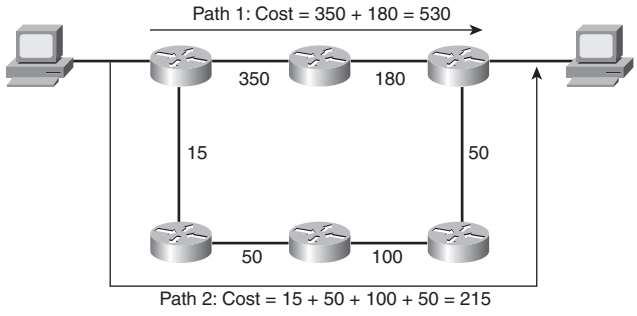
For 10-Mbps Ethernet, cost is calculated as follows:

$$BW = 10 \text{ Mbps} = 10 * 10^6 = 10{,}000{,}000 = 10^7$$
$$\text{cost (Ethernet)} = 10^8 / 10^7 = 10$$

The sum of all the costs to reach a destination is the metric for that route. The lowest cost is the preferred path.

Figure 9-5 shows an example of how the path costs are calculated. The path cost is the sum of all costs in the path. The cost for Path 1 is 350 + 180 = 530. The cost for Path 2 is 15 + 50 + 100 + 50 = 215.

Figure 9-5 *Cost Metric Example*



Because the cost of Path 2 is less than that of Path 1, Path 2 is selected as the best route to the destination.

Load

The load parameter refers to the degree to which the interface link is busy. The router keeps track of interface utilization; routing protocols can use this metric when calculating the best route. Load is one of the five parameters included in the definition of the IGRP and EIGRP metric. By default, it is not used to calculate the composite metric. If you have 512-kbps and 256-kbps links to reach a destination, but the 512-kbps circuit is 99 percent busy and the 256-kbps is only 5 percent busy, the 256 kbps link is the preferred path. On Cisco routers, the percentage of load is shown as a fraction over 255. Utilization at 100 percent is shown as 255/255, and utilization at 0 percent is shown as 0/255. Example 9-1 shows the load of a serial interface at 5/255 (1.9 percent).

Example 9-1 *Interface Load*

```
router3>show interface serial 1
Serial1 is up, line protocol is up
  Hardware is PQUICC Serial
  Internet address is 10.100.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 5/255
```

Delay

The delay parameter refers to how long it takes to move a packet to the destination. Delay depends on many factors, such as link bandwidth, utilization, port queues, and physical distance traveled. Total delay is one of the five parameters included in the definition of the IGRP and EIGRP composite metric. By default, it is used to calculate the composite metric. You can configure an interface's delay with the **delay** *tens-of-microseconds* command, where *tens-of-microseconds*

specifies the delay in tens of microseconds for an interface or network segment. As shown in Example 9-2, the interface's delay is 20,000 microseconds.

Example 9-2 *Interface Delay*

```
router3>show interface serial 1
Serial1 is up, line protocol is up
  Hardware is PQUICC Serial
  Internet address is 10.100.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

Reliability

The reliability parameter is the dependability of a network link. Some WAN links tend to go up and down throughout the day. These links get a small reliability rating. Reliability is measured by factors such as a link's expected received keepalives and the number of packet drops and interface resets. If the ratio is high, the line is reliable. The best rating is 255/255, which is 100 percent reliability. Reliability is one of the five parameters included in the definition of the IGRP and EIGRP metric. By default, it is not used to calculate the composite metric. As shown in Example 9-3, you can verify an interface's reliability using the **show interface** command.

Example 9-3 *Interface Reliability*

```
router4#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

Maximum Transmission Unit (MTU)

The MTU parameter is simply the maximum size of bytes a unit can have on an interface. If the outgoing packet is larger than the MTU, the IP protocol might need to fragment it. If a packet larger than the MTU has the "do not fragment" flag set, the packet is dropped. As shown in Example 9-4, you can verify an interface's MTU using the **show interface** command.

Example 9-4 *Interface MTU*

```
router4#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is PQUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

Routing Loop-Prevention Schemes

Some routing protocols employ schemes to prevent the creation of routing loops in the network. These schemes are

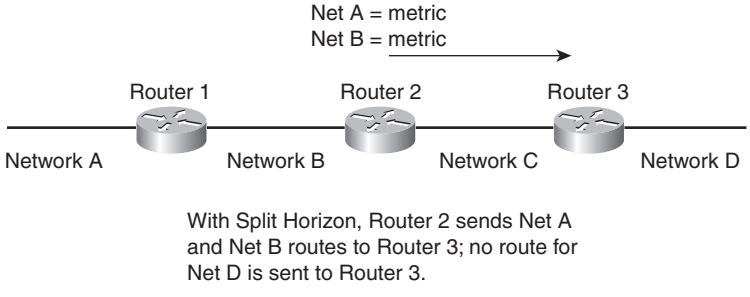
- Split horizon
- Split horizon with poison reverse
- Counting to infinity

Split Horizon

Split horizon is a technique used by distance-vector routing protocols to prevent routing loops. Routes that are learned from a neighboring router are not sent back to that neighboring router, thus suppressing the route. If the neighbor is already closer to the destination, it already has a better path.

In Figure 9-6, Routers 1, 2, and 3 learn about Networks A, B, C, and D. Router 2 learns about Network A from Router 1 and also has Networks B and C in its routing table. Router 3 advertises Network D to Router 2. Now, Router 2 knows about all networks. Router 2 sends its routing table to Router 3 without the route for Network D because it learned that route from Router 3.

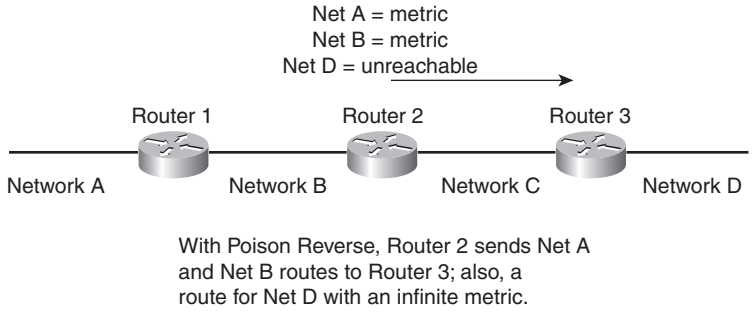
Figure 9-6 *Simple Split-Horizon Example*



Split Horizon with Poison Reverse

Split horizon with poison reverse is a route update sent out an interface with an infinite metric for routes learned (received) from the same interface. Poison reverse simply indicates that the learned route is unreachable. It is more reliable than split horizon alone. Examine Figure 9-7. Instead of suppressing the route for Network D, Router 2 sends that route in the routing table marked as unreachable. In RIP, the poison-reverse route is marked with a metric of 16 (infinite) to prevent that path from being used.

Figure 9-7 *Split Horizon with Poison Reverse*



Counting to Infinity

Some routing protocols keep track of router hops as the packet travels through the network. In large networks where a routing loop might be present because of a network outage, routers might forward a packet without its reaching its destination.

Counting to infinity is a loop-prevention technique in which the router discards a packet when it reaches a maximum limit. It assumes that the network diameter is smaller than the maximum allowed hops. The router uses the Time-to-Live (TTL) field to count to infinity. The TTL starts at a set number and is decremented at each router hop. When the TTL equals 0, the packet is discarded. For IGRP and EIGRP, the TTL of routing updates is 100 by default.

Triggered Updates

Another loop-prevention and fast-convergence technique used by routing protocols is triggered updates. When a router interface changes state (up or down), the router is required to send an update message, even if it is not time for the periodic update message. Immediate notification about a network outage is key to maintaining valid routing entries within all routers in the network. Some distance-vector protocols, including RIP, specify a small time delay to avoid having triggered updates generate excessive network traffic. The time delay is variable for each router.

Summarization

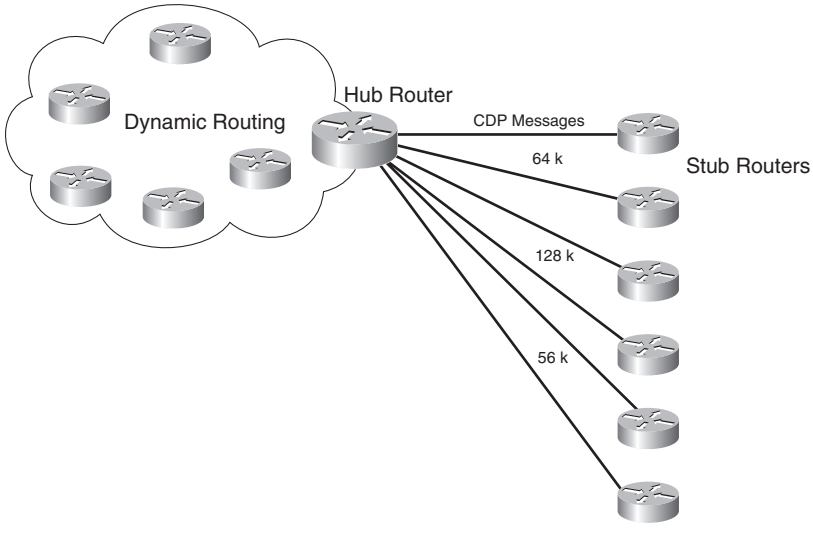
Another characteristic of routing protocols is the ability to summarize routes. Protocols that support CIDR can perform summarization outside of IP class boundaries. By summarizing, the routing protocol can reduce the size of the routing table, and fewer routing updates on the network occur.

ODR

On-demand routing (ODR) is a mechanism for reducing the overhead with routing. Only Cisco routers can use ODR. With ODR, there is no need to configure dynamic routing protocols or static routes at a hub router. ODR eliminates the need to manage static route configuration at the hub router.

Figure 9-8 shows a hub-and-spoke network where you can configure ODR. The stub router is the spoke router in the hub-and-spoke network. The stub network consists of small LAN segments connected to the stub router and a WAN connection to the hub. Because all outgoing traffic travels via the WAN, no external routing information is necessary.

Figure 9-8 *ODR Hub-and-Spoke Network*



ODR simplifies the configuration of IP with stub networks in which the hub routers dynamically maintain routes to the stub networks. With ODR, the stub router advertises the IP prefixes of its connected networks to the hub router. It does so without requiring the configuration of an IP routing protocol at the stub routers.

ODR uses Cisco Discovery Protocol (CDP) for communication between hub and stub routers. CDP must be enabled for ODR to work. CDP updates every 60 seconds. Because ODR route prefixes are carried in CDP messages, a change is not reported until the CDP message is sent.

The hub router receives the prefix routes from its stub routers. You can configure the hub router to redistribute these prefixes into a dynamic routing protocol to propagate those routes to the rest of the internetwork. Stub routers are configured with a static default route to the hub router.

The benefits of ODR are as follows:

- Less routing overhead than dynamic routing protocols
- No configuration or management of static routes on the hub router
- Reduced circuit utilization

References and Recommended Readings

Bruno, A. *CCIE Routing and Switching Exam Certification Guide*. Indianapolis: Cisco Press, 2002.

Hedrick, C. RFC 1058, *Routing Information Protocol*. Available from http://www.ietf.org/rfc.

Malkin, G. RFC 2453, *RIP Version 2*. Available from http://www.ietf.org/rfc.

Moy, J. RFC 2328, *OSPF Version 2*. Available from http://www.ietf.org/rfc.

Oran, D. RFC 1142, *OSI IS-IS Intra-domain Routing Protocol*. Available from http://www.ietf.org/rfc.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics that were covered in this chapter:

- **Routing protocol characteristics**—Characteristics such as static, dynamic, distance-vector, link-state, and interior and exterior protocols
- **Routing protocol metrics**—The metrics used by routing protocols and loop-prevention schemes
- **On-demand routing**—Where to use ODR

Table 9-5 compares distance-vector versus link-state routing protocols.

Table 9-5 *Distance-Vector Versus Link-State Routing Protocols*

Characteristic	Distance-Vector	Link-State
Scalability	Limited	Good
Convergence	Slow	Fast
Routing overhead	More traffic	Less traffic
Implementation	Easy	More complex

Ensure that you know and understand default administrative distances for IP routes. For your convenience, Table 9-6 lists the default administrative distances for IP routes.

Table 9-6 *Default Administrative Distances for IP Routes*

IP Route	Administrative Distance
Connected interface	0
Static route directed to a connected interface	0
Static route directed to the next-hop IP address	1
EIGRP summary route	5
External BGP route	20

continues

Table 9-6 *Default Administrative Distances for IP Routes (Continued)*

IP Route	Administrative Distance
Internal EIGRP route	90
IGRP route	100
OSPF route	110
IS-IS route	115
RIP route	120
EGP route	140
External EIGRP route	170
Internal BGP route	200
Route of unknown origin	255

Table 9-7 summarizes routing protocol characteristics.

Table 9-7 *Routing Protocol Characteristics*

Routing Protocol	Distance-Vector or Link-State	Interior or Exterior	Classful or Classless	Administrative Distance
RIPv1	DV	Interior	Classful	120
RIPv2	DV	Interior	Classless	120
IGRP	DV	Interior	Classful	100
EIGRP	DV (hybrid)	Interior	Classless	90
OSPF	LS	Interior	Classless	110
IS-IS	LS	Interior	Classless	115
BGP	—	Both	Classless	20

The CCDA must know the new routing protocols for IPv6, as listed in Table 9-8.

Table 9-8 *IPv4 and IPv6 Routing Protocols*

IPv4 Routing Protocols	IPv6 Routing Protocols
RIPv1, RIPv2	RIPng
EIGRP	EIGRP for IPv6
OSPFv2	OSPFv3
IS-IS	IS-IS for IPv6
BGP	Multiprotocol Extensions for BGP

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What two routing protocols do not carry mask information in the route updates?
2. True or false: Link-state routing protocols send periodic routing updates.
3. True or false: RIPv2 was created to support IPv6.
4. True or false: The path with the lowest cost is preferred.
5. True or false: A link with a reliability of 200/255 is preferred over a link with a reliability of 10/255.
6. True or false: A link with a load of 200/255 is preferred over a link with a load of 10/255.
7. On a router, both EIGRP and OSPF have a route to 198.168.10.0/24. Which route is injected into the routing table?
8. On a router, both RIPv2 and IS-IS have a route to 198.168.10.0/24. Which route is injected into the routing table?
9. On a router, EIGRP has a route to the destination with a prefix of /28, and OSPF has a route to the destination with a prefix of /30. Which is used to reach the destination?
10. Which of the following is the best measurement of an interface's reliability and load?
    a. Reliability 255/255, load 1/255
    b. Reliability 255/255, load 255/255
    c. Reliability 1/255, load 1/255
    d. Reliability 1/255, load 255/255
11. Which routing protocols permit an explicit hierarchical topology?
    a. BGP
    b. EIGRP
    c. IS-IS
    d. RIP
    e. OSPF
    f. B and D
    g. C and E

12. What routing protocol parameter is concerned with how long a packet takes to travel from one end to another in the internetwork?

13. For what routing protocol metric is the value of a Fast Ethernet interface calculated as $10^8 / 10^8 = 1$?

14. What is the Cisco default OSPF metric for a Fast Ethernet interface?

15. Match the loop-prevention technique (numerals) with its description (letters):

    i. Split horizon

    ii. Split horizon with poison reverse

    iii. Triggered updates

    iv. Counting to infinity

    a. Sends an infinite metric from which the route was learned

    b. Drops a packet when the hop count limit is reached

    c. Suppresses a route announcement from which the route was learned

    d. Sends a route update when a route changes

16. True or false: Link-state routing protocols are more CPU- and memory-intensive than distance-vector routing protocols.

17. Which routing protocols would you select if you needed to take advantage of VLSMs? (Select all that apply.)

    a. RIPv1
    b. RIPv2
    c. IGRP
    d. EIGRP
    e. OSPF
    f. IS-IS

18. Which standards-based protocol would you select in a large IPv6 network?

    a. RIPng
    b. OSPFv3
    c. EIGRP for IPv6
    d. RIPv2

19. Which routing protocol is typically deployed by Internet service providers?

    a. EIGRP
    b. OSPFv2

c. IS-IS

d. RIPv2

20. Which of the following routing protocols are fast in converging when a change in the network occurs? (Select three.)

a. RIPv1

b. RIPv2

c. EIGRP

d. OSPF

e. IS-IS

f. BGP

21. If you are designing a large corporate network that cannot be designed in a hierarchy, which routing protocol would you recommend?

a. RIPv1

b. RIPv2

c. EIGRP

d. OSPF

e. IS-IS

f. BGP

22. Which routing protocols support VLSMs? (Select all that apply.)

a. RIPv1

b. RIPv2

c. EIGRP

d. OSPF

e. IS-IS

f. All of the above

23. You are connecting your network to an ISP. Which routing protocol would you use to exchange routes?

a. RIPv1

b. RIPv2

c. EIGRP

d. OSPF

e. IS-IS

f. BGP

g. All of the above

24. Which routing protocol requires only Cisco routers on the network?

- **a.** RIPv1
- **b.** RIPv2
- **c.** EIGRP
- **d.** OSPF
- **e.** IS-IS
- **f.** BGP
- **g.** All of the above

25. Which routing protocol would be supported on an IPv6 network with multiple vendor routers?

- **a.** RIPv2
- **b.** EIGRP for IPv6
- **c.** BGPv6
- **d.** OSPFv3
- **e.** RIPv3
- **f.** All of the above
- **g.** B and D

26. What additional protocol is required for ODR to work?

27. For what network design is ODR preferred?

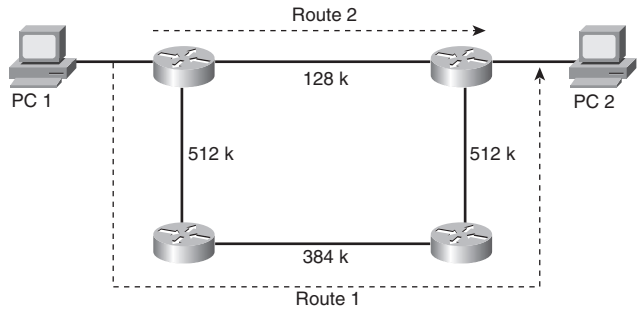
- **a.** Mesh topology
- **b.** Multipoint WAN
- **c.** Hub-and-spoke topology
- **d.** All of the above

28. Which routing protocol represents each column of the following table?

Characteristic	A	B	C	D	E
Supports VLSM	Yes	Yes	Yes	Yes	Yes
Convergence	Fast	Fast	Slow	Fast	Fast
Scalability	High	High	Low	High	High
Supports IPv6	Yes	No	No	No	Yes
Proprietary	Yes	No	No	Yes	No

Answer the following questions based on Figure 9-9.

Figure 9-9 *Scenario Diagram*



29. A user performs a Telnet from PC 1 to PC 2. If the metric used by the configured routing protocol is the bandwidth parameter, which route will the packets take?

- **a.** Route 1
- **b.** Route 2
- **c.** Neither. The information is insufficient.
- **d.** One packet will take Route 1, the following packet will take Route 2, and so on.

30. A user performs a Telnet from PC 1 to PC 2. If the metric used by the configured routing protocol is hop count, which route will the packets take?

- **a.** Route 1
- **b.** Route 2
- **c.** Neither. The information is insufficient.
- **d.** One packet will take Route 1, the following packet will take Route 2, and so on.

31. A user performs a Telnet from PC 1 to PC 2. If the metric used by the configured routing protocol is OSPF cost, which route will the packets take?

- **a.** Route 1.
- **b.** Route 2.
- **c.** Neither. The information is insufficient.
- **d.** One packet will take Route 1, the following packet will take Route 2, and so on.

This chapter covers the following subjects:

- RIPv1
- RIPv2
- RIPng
- IGRP
- EIGRP for IPv4 Networks
- EIGRP for IPv6 Networks

CHAPTER 10

RIP and EIGRP Characteristics and Design

This chapter reviews distance-vector routing protocols. It covers both versions of the Routing Information Protocol (RIP). Although RIPv1 is no longer a test subject, it is included for reference and because it is still seen on some enterprise networks. This chapter also covers Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco's IGRP is also included although it is no longer a test subject. This chapter also covers the routing protocols for IPv6: RIPng and EIGRP for IPv6. The CCDA should understand the capabilities and constraints of each routing protocol.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 10-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 10-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
RIPv2	2, 3, 7
RIPng	5
EIGRP for IPv4 Networks	1, 4, 6, 7, 8
EIGRP for IPv6 Networks	5

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. Which protocol should you select if the network diameter is more than 17 hops?
   a. RIPv1
   b. RIPv2
   c. EIGRP
   d. Answers A and B
   e. Answers B and C
   f. Answers A, B, and C
2. How often does a RIPv2 router broadcast its routing table by default?
   a. Every 30 seconds
   b. Every 60 seconds
   c. Every 90 seconds
   d. RIPv1 does not broadcast periodically.
3. RIPv2 improves on RIPv1 with which of the following capabilities?
   a. Multicast updates, authentication, hop count
   b. Multicast updates, authentication, variable-length subnet mask (VLSM)
   c. Authentication, VLSM, hop count
   d. Multicast updates, hop count
4. Which protocol(s) maintain(s) neighbor adjacencies?
   a. RIPv2 and EIGRP
   b. IGRP and EIGRP
   c. RIPv2
   d. EIGRP
5. Which pair of distance-vector routing protocols supports IPv6 networks?
   a. EIGRP and OSPF
   b. RIPng and EIGRP
   c. RIPv2 and EIGRP
   d. OSPFv2 and EIGRP for IPv6
6. Which parameters are included in the computation of the EIGRP composite metric use by default?
   a. Bandwidth and load
   b. Bandwidth and delay

c. Bandwidth and reliability

d. Bandwidth and maximum transmission unit (MTU)

7. Which protocols support VLSMs?

a. RIPv1 and RIPv2

b. EIGRP and IGRP

c. RIPv1 and IGRP

d. RIPv2 and EIGRP

8. Which routing protocol implements the diffusing update algorithm (DUAL)?

a. IS-IS

b. IGRP

c. EIGRP

d. OSPF

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers the characteristics of the distance-vector routing protocols that a CCDA can choose from in a network design. *RIPv1* is a routing protocol developed in the late 1980s; it was the only interior gateway protocol (IGP) at that time. *RIPv2* provides enhancements to RIP, such as support for VLSMs.

IGRP is an IGP developed by Cisco in the early 1980s that was not limited to the 15-router-hop constraint in RIP. EIGRP is a hybrid routing protocol that uses distance-vector metrics and link-state routing protocol characteristics. RIPng is the IPv6 implementation of RIP. EIGRP for IPv6 is Cisco's implementation of EIGRP for IPv6 networks.

RIPv1

RFC 1058 from June 1988 defines RIPv1. RIP is a distance-vector routing protocol that uses router hop count as the metric. RIPv1 is a classful routing protocol that does not support VLSMs or classless interdomain routing (CIDR). RIPv1 is no longer a topic on the CCDA test. But reading this section will help you understand the evolution of this routing protocol and help you compare it to the later versions.

There is no method for authenticating route updates with RIPv1. A RIP router sends a copy of its routing table to its neighbors every 30 seconds. RIP uses split horizon with poison reverse; therefore, route updates are sent out an interface with an infinite metric for routes learned (received) from the same interface.

The RIP standard was based on the popular **routed** program used in UNIX systems since the 1980s. The Cisco implementation of RIP adds support for load balancing. RIP load-balances traffic if several paths have the same metric (equal-cost load balancing) to a destination. Also, RIP sends triggered updates when a route's metric changes. Triggered updates can help the network converge faster rather than wait for the periodic update. RIP has an administrative distance of 120. Chapter 9, "Routing Protocol Selection Criteria," covers administrative distance.

RIPv1 summarizes to IP network values at network boundaries. A network boundary occurs at a router that has one or more interfaces that do not participate in the specified IP network. The IP address assigned to the interface determines participation. IP class determines the network value. For example, an IP network that uses 24-bit subnetworks from 180.100.50.0/24 to 180.100.120.0/24 is summarized to 180.100.0.0/16 at a network boundary.

RIPv1 Forwarding Information Base

The RIPv1 protocol keeps the following information about each destination:

- **IP address**—IP address of the destination host or network
- **Gateway**—The first gateway along the path to the destination
- **Interface**—The physical network that must be used to reach the destination
- **Metric**—The number of hops to the destination
- **Timer**—The amount of time since the entry was last updated

The database is updated with the route updates received from neighboring routers. As shown in Example 10-1, the **show ip rip database** command shows a router's RIP private database.

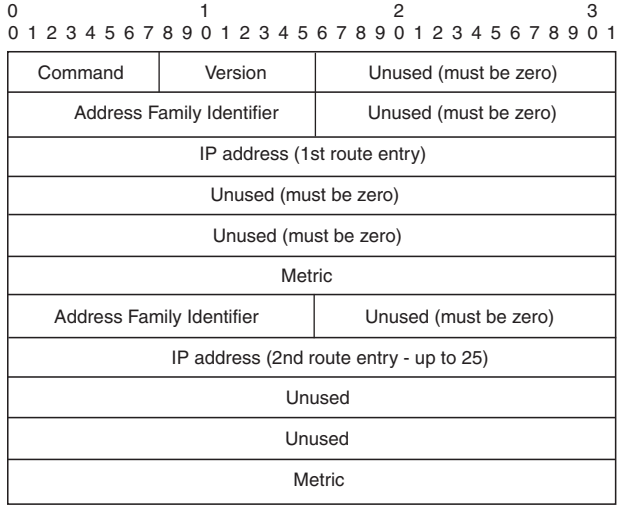
Example 10-1 **show ip rip database** *Command*

```
router9#  show ip rip database
172.16.0.0/16    auto-summary
172.16.1.0/24    directly connected, Ethernet0
172.16.2.0/24
    [1] via 172.16.4.2, 00:00:06, Serial0
172.16.3.0/24
    [1] via 172.16.1.2, 00:00:02, Ethernet0
172.16.4.0/24    directly connected, Serial0
```

RIPv1 Message Format

The RIPv1 message format is described in RFC 1058 and is shown in Figure 10-1. The RIP messages are encapsulated using User Datagram Protocol (UDP). RIP uses the well-known UDP port 520.

Figure 10-1 *RIPv1 Message Format*



The following describes each field:

- **Command**—Describes the packet's purpose. The RFC describes five commands, two of which are obsolete and one of which is reserved. The two used commands are
  - **Request**—Requests all or part of the responding router's routing table.
  - **Response**—Contains all or part of the sender's routing table. This message might be a response to a request, or it might be an update message generated by the sender.
- **Version**—Set to a value of 1 for RIPv1.
- **Address Family Identifier (AFI)**—Set to a value of 2 for IP.
- **IP address**—The destination route. It might be a network address, subnet, or host route. Special route 0.0.0.0 is used for the default route.
- **Metric**—A field that is 32 bits in length. It contains a value between 1 and 15 inclusive, specifying the current metric for the destination. The metric is set to 16 to indicate that a destination is unreachable.

Because RIP has a maximum hop count, it implements counting to infinity. For RIP, infinity is 16 hops. Notice that the RIP message has no subnet masks accompanying each route. Five 32-bit words are repeated for each route entry: AFI (16 bits); unused, which is 0 (16 bits); IP address; two more 32-bit unused fields; and the 32-bit metric. Five 32-bit words equals 20 bytes for each route entry. Up to 25 routes are allowed in each RIP message. The maximum datagram size is limited to 512 bytes, not including the IP header. Calculating 25 routes by 20 bytes each, plus the RIP header (4 bytes), plus an 8-byte UDP header, you get 512 bytes.

RIPv1 Timers

The Cisco implementation of RIPv1 uses four timers:

- Update
- Invalid
- Flush
- Holddown

RIPv1 sends its full routing table out all configured interfaces. The table is sent periodically as a broadcast (255.255.255.255) to all hosts.

Update Timer

The update timer specifies the frequency of the periodic broadcasts. By default, the update timer is set to 30 seconds. Each route has a timeout value associated with it. The timeout gets reset every time the router receives a routing update containing the route.

Invalid Timer

When the timeout value expires, the route is marked as unreachable because it is marked invalid. The router marks the route invalid by setting the metric to 16. The route is retained in the routing table. By default, the invalid timer is 180 seconds, or six update periods (30 * 6 = 180).

Flush Timer

A route entry marked as invalid is retained in the routing table until the flush timer expires. By default, the flush timer is 240 seconds, which is 60 seconds longer than the invalid timer.

Holddown Timer

Cisco implements an additional timer for RIP, the holddown timer. The holddown timer stabilizes routes by setting an allowed time for which routing information about different paths is suppressed. After the metric for a route entry changes, the router accepts no updates for the route until the holddown timer expires. By default, the holddown timer is 180 seconds.

The output of the **show ip protocol** command, as shown in Example 10-2, shows the timers for RIP, unchanged from the defaults.

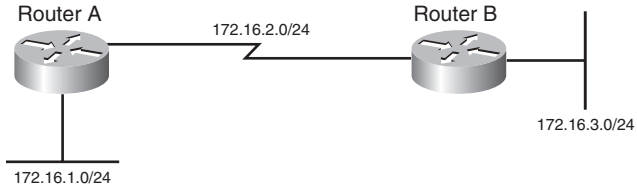
Example 10-2 *RIP Timers Verified with* **show ip protocol**

```
router9>  show ip protocol
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 3 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    Ethernet0             1     1 2
    Serial0               1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.4.2           120      00:00:00
    172.16.1.2           120      00:00:07
  Distance: (default is 120)
```

RIPv1 Design

New networks should not be designed using RIPv1. It does not support VLSMs and CIDR. The IP addressing scheme with RIPv1 requires the same subnet mask for the entire IP network, a flat IP network. As shown in Figure 10-2, when you use RIPv1, all segments must have the same subnet mask.

Figure 10-2 *RIPv1 Design*



RIPv1 has low scalability. It is limited to 15 hops; therefore, the network diameter cannot exceed this limit. RIPv1 also broadcasts its routing table every 30 seconds. RIP's slow convergence time prevents it from being used as an IGP when time-sensitive data, such as voice and video, is being transmitted across the network. RIPv1 is usually limited to access networks where it can interoperate with servers running **routed** or with non-Cisco routers.

RIPv1 Summary

The characteristics of RIPv1 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classful protocol (no support for VLSM or CIDR).
- Metric is router hop count.
- Low scalability: maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast every 30 seconds.
- 25 routes per RIPv1 message.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks.

RIPv2

RIPv2 was first described in RFC 1388 and RFC 1723 (1994); the current RFC is 2453, written in November 1998. Although current environments use advanced routing protocols such as OSPF

and EIGRP, some networks still use RIP. The need to use VLSMs and other requirements prompted the definition of RIPv2.

RIPv2 improves on RIPv1 with the ability to use VLSM, with support for route authentication, and with multicasting of route updates. RIPv2 supports CIDR. It still sends updates every 30 seconds and retains the 15-hop limit; it also uses triggered updates. RIPv2 still uses UDP port 520; the RIP process is responsible for checking the version number. It retains the loop-prevention strategies of poison reverse and counting to infinity. On Cisco routers, RIPv2 has the same administrative distance as RIPv1, which is 120. Finally, RIPv2 uses the IP address 224.0.0.9 when multicasting route updates to other RIP routers. As in RIPv1, RIPv2 by default summarizes IP networks at network boundaries. You can disable autosummarization if required.

You can use RIPv2 in small networks where VLSM is required. It also works at the edge of larger networks.

Authentication

Authentication can prevent communication with any RIP routers that are not intended to be part of the network, such as UNIX stations running **routed**. Only RIP updates with the authentication password are accepted. RFC 1723 defines simple plain-text authentication for RIPv2.

MD5 Authentication

In addition to plain-text passwords, the Cisco implementation provides the ability to use Message Digest 5 (MD5) authentication, which is defined in RFC 1321. Its algorithm takes as input a message of arbitrary length and produces as output a 128-bit fingerprint or message digest of the input, making it much more secure than plain-text passwords.

RIPv2 Forwarding Information Base

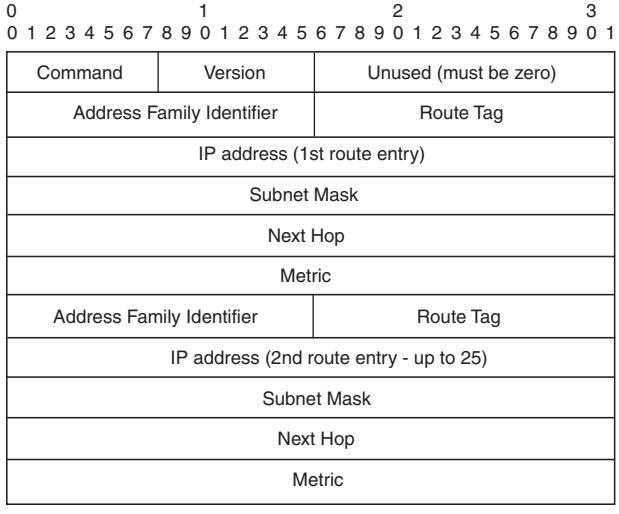
RIPv2 maintains a routing table database as in Version 1. The difference is that it also keeps the subnet mask information. The following list repeats the table information of RIPv1:

- **IP address**—The IP address of the destination host or network, with subnet mask
- **Gateway**—The first gateway along the path to the destination
- **Interface**—The physical network that must be used to reach the destination
- **Metric**—A number indicating the number of hops to the destination
- **Timer**—The amount of time since the route entry was last updated

RIPv2 Message Format

The RIPv2 message format takes advantage of the unused fields in the RIPv1 message format by adding subnet masks and other information. Figure 10-3 shows the RIPv2 message format.

Figure 10-3 *RIPv2 Message Format*



The following describes each field:

- **Command**—Indicates whether the packet is a request or response message. The request message asks that a router send all or a part of its routing table. Response messages contain route entries. The router sends the response periodically or as a reply to a request.
- **Version**—Specifies the RIP version used. It is set to 2 for RIPv2 and to 1 for RIPv1.
- **AFI**—Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an AFI to indicate the type of address specified. The AFI for IP is 2. The AFI is set to 0xFFF for the first entry to indicate that the remainder of the entry contains authentication information.
- **Route tag**—Provides a method for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols). You can add this optional attribute during the redistribution of routing protocols.
- **IP address**—Specifies the IP address (network) of the destination.
- **Subnet mask**—Contains the subnet mask for the destination. If this field is 0, no subnet mask has been specified for the entry.

- **Next hop**—Indicates the IP address of the next hop where packets are sent to reach the destination.
- **Metric**—Indicates how many router hops to reach the destination. The metric is between 1 and 15 for a valid route or 16 for an unreachable or infinite route.

Again, as in Version 1, the router permits up to 25 occurrences of the last five 32-bit words (20 bytes) for up to 25 routes per RIP message. If the AFI specifies an authenticated message, the router can specify only 24 routing table entries. The updates are sent to the multicast address of 224.0.0.9.

RIPv2 Timers

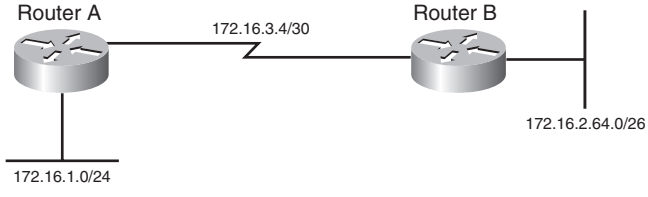
RIPv2 timers are the same as in Version 1. They send periodic updates every 30 seconds. The default invalid timer is 180 seconds, the holddown timer is 180 seconds, and the flush timer is 240 seconds. You can write this list as 30/180/180/240, representing the U/I/H/F timers.

RIPv2 Design

Things to remember in designing a network with RIPv2 include that it supports VLSM within networks and CIDR for network summarization across adjacent networks. RIPv2 allows for the summarization of routes in a hierarchical network. RIPv2 is still limited to 16 hops; therefore, the network diameter cannot exceed this limit. RIPv2 multicasts its routing table every 30 seconds to the multicast IP address 224.0.0.9. RIPv2 is usually limited to accessing networks where it can interoperate with servers running **routed** or with non-Cisco routers. RIPv2 also appears at the edge of larger internetworks. RIPv2 further provides for route authentication.

As shown in Figure 10-4, when you use RIPv2, all segments can have different subnet masks.

Figure 10-4 *RIPv2 Design*



RIPv2 Summary

The characteristics of RIPv2 follow:

- Distance-vector protocol.
- Uses UDP port 520.

- Classless protocol (support for CIDR).
- Supports VLSMs.
- Metric is router hop count.
- Low scalability: maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates are sent every 30 seconds to multicast address 224.0.0.9.
- 25 routes per RIP message (24 if you use authentication).
- Supports authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Subnet mask included in route entry.
- Administrative distance for RIPv2 is 120.
- Not scalable. Used in small, flat networks or at the edge of larger networks.

RIPng

RIPng (RIP next generation) is the version of RIP that can be used in IPv6 networks. It is described in RFC 2080. Most of the RIP mechanisms from RIPv2 remain the same. RIPng still has a 15-hop limit, counting to infinity, and split horizon with poison reverse. A hop count of 16 still indicates an unreachable route.

Instead of using UDP port 520 as in RIPv2, RIPng uses UDP port 521. RIPng supports IPv6 addresses and prefixes. RIPng uses multicast group FF02::9 for RIPng updates to all RIPng routers.

RIPng Timers

RIPng timers are similar to RIPv2. Periodic updates are sent every 30 seconds. The default invalid timeout for routes to expire is 180 seconds, the default holddown timer is 180 seconds, and the default garbage-collection timer is 120 seconds.

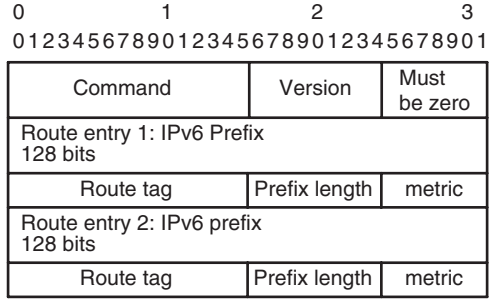
Authentication

RIPng does not implement authentication methods in its protocol as RIPv2 does. RIPng relies on built-in IPv6 authentication functions.

RIPng Message Format

Figure 10-5 shows the RIPng routing message. Each route table entry (RTE) consists of the IPv6 prefix, route tag, prefix length, and metric.

Figure 10-5 *RIPng Update Message Format*

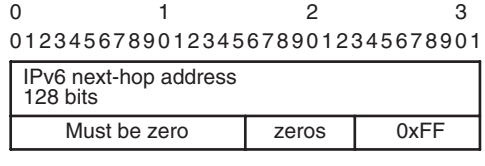


The following describes each field:

- **Command**—Indicates whether the packet is a request or response message. This field is set to 1 for a request and to 2 for a response.
- **Version**—Set to 1, the first version of RIPng.
- **IPv6 prefix**—The destination 128-bit IPv6 prefix.
- **Route tag**—As with RIPv2, this is a method that distinguishes internal routes (learned by RIP) from external routes (learned by external protocols). Tagged during redistribution.
- **Prefix length**—Indicates the significant part of the prefix.
- **Metric**—This 8-bit field contains the router hop metric.

RIPv2 has a Next Hop field for each of its route entries. An RTE with a metric of 0xFF indicates the next-hop address to reduce the number of route entries in RIPng. It groups all RTEs after it to summarize all destinations to that particular next-hop address. Figure 10-6 shows the format of the special RTE indicating the next-hop entry.

Figure 10-6 *RIPng Next-Hop Route Table Entry*



RIPng Design

RIPng has low scalability. As with RIPv2, it is limited to 15 hops; therefore, the network diameter cannot exceed this limit. RIPng also broadcasts its routing table every 30 seconds, which causes network overhead. RIPng can be used only in small networks.

RIPng Summary

The characteristics of RIPng are as follows:

- Distance-vector protocol for IPv6 networks only.
- Uses UDP port 521.
- Metric is router hop count.
- Maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates are sent every 30 seconds to multicast address FF02::9.
- Uses IPv6 functions for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Prefix length included in route entry.
- Administrative distance for RIPv2 is 120.
- Not scalable. Used in small networks.

IGRP

Cisco Systems developed IGRP to overcome the limitations of RIPv1. IGRP is a distance-vector routing protocol that considers a composite metric that, by default, uses bandwidth and delay as parameters instead of hop count. IGRP is not limited to RIP's 15-hop limit. IGRP has a maximum hop limit of 100 by default and can be configured to support a network diameter of 255.

NOTE IGRP is no longer a CCDA test topic. EIGRP is the enhanced version of IGRP. However, reading this section will provide a good foundation for learning EIGRP in the section that follows.

With IGRP, routers usually select paths with a larger minimum-link bandwidth over paths with a smaller hop count. Links do not have a hop count. They are exactly one hop.

IGRP is a classful protocol and cannot implement VLSM or CIDR. IGRP summarizes at network boundaries. As in RIP, IGRP implements split horizon with poison reverse, triggered updates, and holddown timers for stability and loop prevention. Another benefit of IGRP is that it can load-balance over unequal-cost links. As a routing protocol developed by Cisco, IGRP is available only on Cisco routers.

By default, IGRP load-balances traffic if several paths have equal cost to the destination. IGRP does unequal-cost load balancing if configured with the **variance** command.

IGRP Timers

IGRP sends its routing table to its neighbors every 90 seconds. IGRP's default update period of 90 seconds is a benefit compared to RIP, which can consume excessive bandwidth when sending updates every 30 seconds. IGRP uses an invalid timer to mark a route as invalid after 270 seconds (3 times the update timer). As with RIP, IGRP uses a flush timer to remove a route from the routing table; the default flush timer is set to 630 seconds (7 times the update period and more than 10 minutes).

If a network goes down or the metric for the network increases, the route is placed in holddown. The router accepts no new changes for the route until the holddown timer expires. This setup prevents routing loops in the network. The default holddown timer is 280 seconds (3 times the update timer plus 10 seconds). Table 10-2 summarizes the default settings for IGRP timers.

Table 10-2 *IGRP Timers*

IGRP Timer	Default Time
Update	90 seconds
Invalid	270 seconds
Holddown	280 seconds
Flush	630 seconds

IGRP Metrics

IGRP uses a composite metric based on bandwidth, delay, load, and reliability. Chapter 9 discusses these metrics. By default, IGRP uses bandwidth and delay to calculate the composite metric, as follows:

$$IGRP_{metric} = \{k1 * BW + [(k2 * BW)/(256 - load)] + k3 * delay\} * \{k5/(reliability + k4)\}$$

In this formula, BW is the lowest interface bandwidth in the path, and delay is the sum of all outbound interface delays in the path. The router dynamically measures reliability and load. The

values of reliability and load used in the metric computation range from 1 to 255. Cisco IOS routers display 100 percent reliability as 255/255. They also display load as a fraction of 255. They display an interface with no load as 1/255. By default, k1 and k3 are set to 1, and k2, k4, and k5 are set to 0. With the default values, the metric becomes

$$IGRP_{metric} = \{1 * BW + [(0 * BW)/(256 - load)] + 1 * delay\} * \{0/(reliability + 0)\}$$
$$IGRP_{metric} = BW + delay$$

The BW is 10,000,000 divided by the smallest of all the bandwidths (in kbps) from outgoing interfaces to the destination. To find delay, add all the delays (in microseconds) from the outgoing interfaces to the destination, and divide this number by 10. (The delay is in 10s of microseconds.)

Example 10-3 shows the output interfaces of two routers. For a source host to reach network 172.16.2.0, a path takes the serial link and then the Ethernet interface. The bandwidths are 10,000 and 1544; the slowest bandwidth is 1544. The sum of delays is 20000 + 1000 = 21000.

Example 10-3 ***show interface***

```
RouterA>  show interface serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 172.16.4.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255

RouterB>  show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0010.7b80.bad5 (bia 0010.7b80.bad5)
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

The IGRP metric is calculated as follows:

$$IGRP_{metric} = (10{,}000{,}000/1544) + (20000 + 1000)/10$$
$$IGRP_{metric} = 6476 + 2100 = 8576$$

You can change the default metrics using the **metric weight** *tos k1 k2 k3 k4 k5* subcommand under **router igrp**. Cisco once intended to implement the tos field as a specialized service in IGRP. However, it was never implemented, so the value of *tos* is always 0. The *k* arguments are the k

values used to build the composite metric. For example, if you want to use all metrics, the command is as follows:

```
router igrp n
 metric weight 0 1 1 1 1 1
```

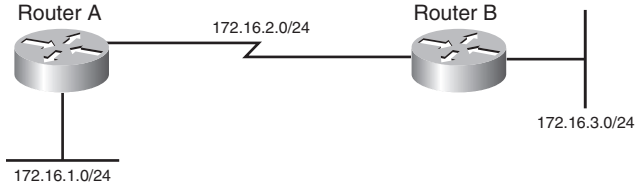
IGRP Design

IGRP should not be used in the design of new networks because it does not support VLSMs. The IP addressing scheme with IGRP requires the same subnet mask for the entire IP network, a flat IP network. IGRP does not support CIDR and network summarization within the major network boundary. IGRP is not limited to a maximum of 15 hops as RIP is; therefore, the network diameter can be larger than that of networks using RIP. IGRP also broadcasts its routing table every 90 seconds, which produces less network overhead than RIP. IGRP is limited to Cisco-only networks.

Drawbacks of IGRP are that it lacks VLSM support and that it broadcasts its entire table every 90 seconds. Its slow convergence makes it too slow for time-sensitive applications. EIGRP is recommended over IGRP.

As shown in Figure 10-7, when you use IGRP, all segments must have the same subnet mask.

Figure 10-7 *IGRP Design*



IGRP Summary

The characteristics of IGRP follow:

- Distance-vector protocol.
- Uses IP protocol number 9.
- Classful protocol (no support for CIDR).
- No support for VLSMs.
- Composite metric using bandwidth and delay by default.
- You can include load and reliability in the metric.

- Route updates are sent every 90 seconds.
- 104 routes per IGRP message.
- Hop count is limited to 100 by default and is configurable up to 255.
- No support for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 100.
- Previously used in large networks; now replaced by EIGRP.

EIGRP for IPv4 Networks

Cisco Systems released EIGRP in the early 1990s as an evolution of IGRP toward a more scalable routing protocol for large internetworks. EIGRP is a classless protocol that permits the use of VLSMs and that supports CIDR for the scalable allocation of IP addresses. EIGRP does not send routing updates periodically, as does IGRP. EIGRP allows for authentication with MD5. EIGRP autosummarizes networks at network borders and can load-balance over unequal-cost paths. Packets using EIGRP use IP 88. Only Cisco routers can use EIGRP.

EIGRP is an advanced distance-vector protocol that implements some characteristics similar to those of link-state protocols. Some Cisco documentation refers to EIGRP as a hybrid protocol. EIGRP advertises its routing table to its neighbors as distance-vector protocols do, but it uses hellos and forms neighbor relationships as link-state protocols do. EIGRP sends partial updates when a metric or the topology changes on the network. It does not send full routing-table updates in periodic fashion as do distance-vector protocols. EIGRP uses DUAL to determine loop-free paths to destinations. This section discusses DUAL.

By default, EIGRP load-balances traffic if several paths have equal cost to the destination. EIGRP performs unequal-cost load balancing if you configure it with the **variance** *n* command. EIGRP includes routes that are equal to or less than *n* times the minimum metric route to a destination. As in RIP and IGRP, EIGRP also summarizes IP networks at network boundaries.

EIGRP internal routes have an administrative distance of 90. EIGRP summary routes have an administrative distance of 5, and EIGRP external routes (from redistribution) have an administrative distance of 170.

EIGRP Components

EIGRP has four components that characterize it:

- Protocol-dependent modules
- Neighbor discovery and recovery
- Reliable Transport Protocol (RTP)
- DUAL

You should know the role of the EIGRP components, which are described in the following sections.

Protocol-Dependent Modules

EIGRP uses different modules that independently support IP, Internetwork Packet Exchange (IPX), and AppleTalk routed protocols. These modules are the logical interface between DUAL and routing protocols such as IPX RIP, AppleTalk Routing Table Maintenance Protocol (RTMP), and IGRP. The EIGRP module sends and receives packets but passes received information to DUAL, which makes routing decisions.

EIGRP automatically redistributes with IGRP if you configure both protocols with the same autonomous system number. When configured to support IPX, EIGRP communicates with the IPX RIP and forwards the route information to DUAL to select the best paths. AppleTalk EIGRP automatically redistributes routes with AppleTalk RTMP to support AppleTalk networks. AppleTalk is not a CCDA objective and is not covered in this book.

Neighbor Discovery and Recovery

EIGRP discovers and maintains information about its neighbors. It multicasts hello packets (224.0.0.10) every 5 seconds on most interfaces. The router builds a table with EIGRP neighbor information. The holdtime to maintain a neighbor is 3 times the hello time: 15 seconds. If the router does not receive a hello in 15 seconds, it removes the neighbor from the table. EIGRP multicasts hellos every 60 seconds on multipoint WAN interfaces (X.25, Frame Relay, ATM) with speeds less than a T-1 (1.544 Mbps), inclusive. The neighbor holdtime is 180 seconds on these types of interfaces. To summarize, hello/holdtime timers are 5/15 seconds for high-speed links and 60/180 seconds for low-speed links.

Example 10-4 shows an EIGRP neighbor database. The table lists the neighbor's IP address, the interface to reach it, the neighbor holdtime timer, and the uptime.

Example 10-4 *EIGRP Neighbor Database*

```
Router#  show ip eigrp neighbor
IP-EIGRP neighbors for process 100
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
1   172.17.1.1              Se0           11 00:11:27   16   200  0  2
0   172.17.2.1              Et0           12 00:16:11   22   200  0  3
```

RTP

EIGRP uses RTP to manage EIGRP packets. RTP ensures the reliable delivery of route updates and also uses sequence numbers to ensure ordered delivery. It sends update packets using multicast address 224.0.0.10. It acknowledges updates using unicast hello packets with no data.

DUAL

EIGRP implements DUAL to select paths and guarantee freedom from routing loops. J.J. Garcia Luna-Aceves developed DUAL. It is mathematically proven to result in a loop-free topology, providing no need for periodic updates or route-holddown mechanisms that make convergence slower.

DUAL selects a best path and a second-best path to reach a destination. The best path selected by DUAL is the *successor*, and the second-best path (if available) is the *feasible successor*. The feasible distance is the lowest calculated metric of a path to reach the destination. The topology table in Example 10-5 shows the feasible distance. The example also shows two paths (Ethernet 0 and Ethernet 1) to reach 172.16.4.0/30. Because the paths have different metrics, DUAL chooses only one successor.

Example 10-5 *Feasible Distance as Shown in the EIGRP Topology Table*

```
Router8#  show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(172.16.3.1)


Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status


P 172.16.4.0/30, 1 successors, FD is 2195456
         via 172.16.1.1 (2195456/2169856), Ethernet0
         via 172.16.5.1 (2376193/2348271), Ethernet1
P 172.16.1.0/24, 1 successors, FD is 281600
         via Connected, Ethernet0
```

The route entries in Example 10-5 are marked with a P for the passive state. A destination is in passive state when the router is not performing any recomputations for the entry. If the successor goes down and the route entry has feasible successors, the router does not need to perform any recomputations and does not go into active state.

DUAL places the route entry for a destination into active state if the successor goes down and there are no feasible successors. EIGRP routers send query packets to neighboring routers to find a feasible successor to the destination. A neighboring router can send a reply packet that indicates it has a feasible successor or a query packet. The query packet indicates that the neighboring router does not have a feasible successor and will participate in the recomputation. A route does not return to passive state until it has received a reply packet from each neighboring router. If the router does not receive all the replies before the "active-time" timer expires, DUAL declares the route as stuck in active (SIA). The default active timer is 3 minutes.

EIGRP Timers

EIGRP sets updates only when necessary and sends them only to neighboring routers. There is no periodic update timer.

EIGRP uses hello packets to learn of neighboring routers. On high-speed networks, the default hello packet interval is 5 seconds. On multipoint networks with link speeds of T1 and slower, hello packets are unicast every 60 seconds.

The holdtime to maintain a neighbor adjacency is 3 times the hello time: 15 seconds. If a router does not receive a hello within the holdtime, it removes the neighbor from the table. Hellos are multicast every 60 seconds on multipoint WAN interfaces (X.25, Frame Relay, ATM) with speeds less than 1.544 Mbps, inclusive. The neighbor holdtime is 180 seconds on these types of interfaces. To summarize, hello/holdtime timers are 5/15 seconds for high-speed links and 60/180 seconds for multipoint WAN links less than 1.544 Mbps, inclusive.

NOTE EIGRP does not send updates using a broadcast address; instead, it sends them to the multicast address 224.0.0.10 (all EIGRP routers).

EIGRP Metrics

EIGRP uses the same composite metric as IGRP, but the BW term is multiplied by 256 for finer granularity. The composite metric is based on bandwidth, delay, load, and reliability. MTU is not an attribute for calculating the composite metric.

EIGRP calculates the composite metric with the following formula:

$$EIGRP_{metric} = \{k1 * BW + [(k2 * BW)/(256 - load)] + k3 * delay\} * \{k5/(reliability + k4)\}$$

In this formula, BW is the lowest interface bandwidth in the path, and delay is the sum of all outbound interface delays in the path. The router dynamically measures reliability and load. It expresses 100 percent reliability as 255/255. It expresses load as a fraction of 255. An interface with no load is represented as 1/255.

Bandwidth is the inverse minimum bandwidth (in kbps) of the path in bits per second scaled by a factor of $256 * 10^7$. The formula for bandwidth is

$$(256 * 10^7)/BW_{min}$$

The delay is the sum of the outgoing interface delays (in microseconds) to the destination. A delay of all 1s (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable. The formula for delay is

$$[sum\ of\ delays] * 256$$

Reliability is a value between 1 and 255. Cisco IOS routers display reliability as a fraction of 255. That is, 255/255 is 100 percent reliability, or a perfectly stable link; a value of 229/255 represents a 90 percent reliable link.

Load is a value between 1 and 255. A load of 255/255 indicates a completely saturated link. A load of 127/255 represents a 50 percent saturated link.

By default, k1 = k3 = 1 and k2 = k4 = k5 = 0. EIGRP's default composite metric, adjusted for scaling factors, is

$$EIGRP_{metric} = 256 * \{ [10^7/BW_{min}] + [sum\_of\_delays] \}$$

BW_{min} is in kbps, and sum_of_delays is in 10s of microseconds. The bandwidth and delay for an Ethernet interface are 10 Mbps and 1 ms, respectively.

The calculated EIGRP BW metric is

$$256 * 10^7/BW = 256 * 10^7/10{,}000$$
$$= 256 * 10{,}000$$
$$= 256{,}000$$

The calculated EIGRP delay metric is

256 * sum of delay = 256 * 1 ms
= 256 * 100 * 10 microseconds
= 25,600 (in 10s of microseconds)

Table 10-3 shows some default values for bandwidth and delay.

Table 10-3 *Default EIGRP Values for Bandwidth and Delay*

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 Mbps)
Ethernet	25,600 (1 ms)	256,000 (10 Mbps)
T-1 (1.544 Mbps)	512,000 (20,000 ms)	1,657,856
64 kbps	512,000	40,000,000
56 kbps	512,000	45,714,176

As with IGRP, you use the **metric weights** subcommand to change EIGRP metric computation. You can change the k values in the EIGRP composite metric formula to select which EIGRP metrics to use. The command to change the k values is the **metric weights** *tos k1 k2 k3 k4 k5* subcommand under **router eigrp** *n*. The *tos* value is always 0. You set the other arguments to 1 or 0 to alter the composite metric. For example, if you want the EIGRP composite metric to use all the parameters, the command is as follows:

```
router eigrp n
 metric weights 0 1 1 1 1 1
```

EIGRP Packet Types

EIGRP uses five packet types:

- **Hello**—EIGRP uses hello packets in the discovery of neighbors. They are multicast to 224.0.0.10. By default, EIGRP sends hello packets every 5 seconds (60 seconds on WAN links with 1.544 Mbps speeds or less).
- **Acknowledgment**—An acknowledgment packet acknowledges the receipt of an update packet. It is a hello packet with no data. EIGRP sends acknowledgment packets to the unicast address of the sender of the update packet.

- **Update**—Update packets contain routing information for destinations. EIGRP unicasts update packets to newly discovered neighbors; otherwise, it multicasts update packets to 224.0.0.10 when a link or metric changes. Update packets are acknowledged to ensure reliable transmission.
- **Query**—EIGRP sends query packets to find feasible successors to a destination. Query packets are always multicast unless they are sent as a response; then they are unicast back to the originator.
- **Reply**—EIGRP sends reply packets to respond to query packets. Reply packets provide a feasible successor to the sender of the query. Reply packets are unicast to the sender of the query packet.

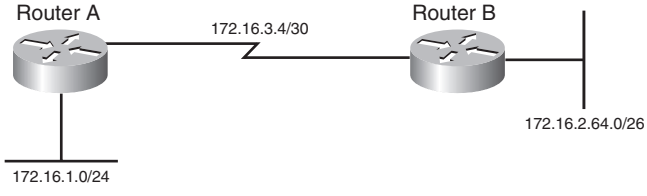
EIGRP Design

When designing a network with EIGRP, remember that it supports VLSMs, CIDR, and network summarization. EIGRP allows for the summarization of routes in a hierarchical network. EIGRP is not limited to 16 hops as RIP is; therefore, the network diameter can exceed this limit. In fact, the EIGRP diameter can be 225 hops. The default diameter is 100. EIGRP can be used in the site-to-site WAN and IPsec VPNs. In the enterprise campus, EIGRP can be used in data centers, server distribution, building distribution, and the network core.

EIGRP does not broadcast its routing table periodically, so there is no large network overhead. You can use EIGRP for large networks; it is a potential routing protocol for the core of a large network. EIGRP further provides for route authentication.

As shown in Figure 10-8, when you use EIGRP, all segments can have different subnet masks.

Figure 10-8 *EIGRP Design*



EIGRP Summary

The characteristics of EIGRP follow:

- Hybrid routing protocol (a distance-vector protocol that has link-state protocol characteristics).
- Uses IP protocol number 88.

- Classless protocol (supports VLSMs).
- Default composite metric uses bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends partial route updates only when there are changes.
- Supports MD5 authentication.
- Uses DUAL for loop prevention and fast convergence.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.
- High scalability; used in large networks.
- Does not require a hierarchical physical topology.

EIGRP for IPv6 Networks

Cisco has developed EIGRP support for IPv6 networks to route IPv6 prefixes. EIGRP for IPv6 is configured and managed separately from EIGRP for IPv4; no network statements are used. EIGRP for IPv6 retains all the same characteristics (network discovery, DUAL, modules) and functions as EIGRP for IPv4. The major themes with EIGRP for IPv6 are as follows:

- Implements the protocol-independent modules.
- Does EIGRP neighbor discovery and recovery.
- Uses reliable transport.
- Implements the DUAL algorithm for a loop-free topology.
- Uses the same metrics as EIGRP for IPv4 networks.
- Has the same timers as EIGRP for IPv4.
- Uses same concepts of feasible successors and feasible distance as EIGRP for IPv4.
- Uses the same packet types as EIGRP for IPv4.
- Managed and configured separately from EIGRP for IPv4.
- Requires a router ID before it can start running.
- Configured on interfaces. No network statements are used.

The difference is the use of IPv6 prefixes and the use of IPv6 multicast group FF02::A for EIGRP updates. Because EIGRP for IPv6 uses the same characteristics and functions as EIGRP for IPv4 covered in the previous section on EIGRP, they are not repeated here.

EIGRP for IPv6 Design

Use EIGRP for IPv6 in large geographic IPv6 networks. EIGRP's diameter can scale up to 255 hops, but this network diameter is not recommended. EIGRP authentication can be used instead of IPv6 authentication.

EIGRP for IPv6 can be used in the site-to-site WAN and IPsec VPNs. In the enterprise campus, EIGRP can be used in data centers, server distribution, building distribution, and the network core.

EIGRP's DUAL algorithm provides for fast convergence and routing loop prevention. EIGRP does not broadcast its routing table periodically, so there is no large network overhead. The only constraint is that EIGRP for IPv6 is restricted to Cisco routers.

EIGRP for IPv6 Summary

The characteristics of EIGRP for IPv6 are as follows:

- Uses the same characteristics and functions as EIGRP for IPv4.
- Hybrid routing protocol (a distance-vector protocol that has link-state protocol characteristics).
- Uses Next Header protocol 88.
- Routes IPv6 prefixes.
- Default composite metric uses bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends partial route updates only when there are changes.
- Supports EIGRP MD5 authentication.
- Uses DUAL for loop prevention and fast convergence.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.

- Uses IPv6 multicast FF02::A for EIGRP updates.
- High scalability; used in large networks.

References and Recommended Readings

Bruno, A. *CCIE Routing and Switching Exam Certification Guide*. Indianapolis: Cisco Press, 2002.

Doyle, J. *Routing TCP/IP*, Volume I. Indianapolis: Cisco Press, 1998.

"Enhanced IGRP." http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm.

"Enhanced Interior Gateway Routing Protocol." http://www.cisco.com/en/US/tech/tk365/tk207/technologies_white_paper09186a0080094cb7.shtml.

Hedrick, C. RFC 1058, Routing Information Protocol. Available from http://www.ietf.org/rfc.

"Implementing EIGRP for IPv6." http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00805fc867.html#wp1049317.

Malkin, G. RFC 1723, *RIP Version 2 - Carrying Additional Information*. Available from http://www.ietf.org/rfc.

Malkin, G. RFC 2453, *RIP Version 2*. Available from http://www.ietf.org/rfc.

Malkin, G. and R. Minnear. RFC 2080, *RIPng for IPv6*. Available from http://www.ietf.org/rfc.

Rivest, R. RFC 1321, *The MD5 Message-Digest Algorithm*. Available from http://www.ietf.org/rfc.

"Routing Information Protocol." http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm.

"Tech Notes: How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP?" http://www.cisco.com/warp/public/103/19.html.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

This chapter has covered the following topics you need to master for the CCDA exam:

- **RIPv2**—The enhancements in Version 2 of RIP to support network designs
- **RIPng**—New RIP for IPv6 networks
- **EIGRP for IPv4**—The enhanced version of IGRP and its uses in network design
- **EIGRP for IPv6**—The modified version of EIGRP that supports IPv6 networks

Table 10-4 compares the routing protocols covered in this chapter.

Table 10-4 *Routing Protocol Comparisons*

Characteristic	RIPv1	RIPv2	RIPng	EIGRP	EIGRP for IPv6
Distance vector	Yes	Yes	Yes	DV/Hybrid	DV/Hybrid
VLSMs	No	Yes	Yes	Yes	Yes
Authentication	No	Yes	No	Yes	Yes
Update timer (sec)	30	30	90	—	—
Invalid timer (sec)	180	180	180	—	—
Flush timer (sec)	240	240	240	—	—
Holddown timer (sec)	180	180	180	—	—
Protocol/port	UDP 520	UDP 520	UDP 521	IP 88	Next Header 88
Admin distance	120	120	120	90	90
IP version	IPv4	IPv4	IPv6	IPv4	IPv6

RIPv1 Summary

The characteristics of RIPv1 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classful protocol (no support for VLSMs or CIDR).
- Metric is router hop count.
- Low scalability: maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast (255.255.255.255) every 30 seconds.
- 25 routes per RIPv1 message.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks.

RIPv2 Summary

The characteristics of RIPv2 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classless protocol (support for CIDR).
- Supports VLSMs.
- Metric is router hop count.
- Low scalability: maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates are sent every 30 seconds to multicast address 224.0.0.9.
- 25 routes per RIP message (24 if authentication is used).
- Supports authentication.
- Implements split horizon with poison reverse.

- Implements triggered updates.
- Subnet mask included in route entry.
- Administrative distance for RIPv2 is 120.
- Not scalable. Used in small, flat networks or at the edge of larger networks.

RIPng Summary

The characteristics of RIPng are as follows:

- Distance-vector protocol for IPv6 networks only.
- Uses UDP port 521.
- Metric is router hop count.
- Maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates are sent every 30 seconds to multicast address FF02::9.
- Uses IPv6 functions for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Prefix length included in route entry.
- Administrative distance for RIPv2 is 120.
- Not scalable. Used in small networks.

EIGRP for IPv4 Summary

The characteristics of EIGRP follow:

- Hybrid routing protocol (a distance-vector protocol that has link-state protocol characteristics).
- Uses IP protocol number 88.
- Classless protocol (supports VLSMs).
- Default composite metric of bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends route updates to multicast address 224.0.0.10.

- Sends partial route updates only when there are changes.
- Support for MD5 authentication and fast convergence.
- Uses DUAL for fast convergence and loop prevention.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.
- High scalability; used in large networks.
- Does not require hierarchical physical topology.

EIGRP for IPv6 Summary

The characteristics of EIGRP for IPv6 are as follows:

- Uses the same characteristics and functions as EIGRP for IPv4.
- Hybrid routing protocol (a distance-vector protocol that has link-state protocol characteristics).
- Uses Next Header protocol number 88.
- Routes IPv6 prefixes.
- Default composite metric uses bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends partial route updates only when there are changes.
- Support for EIGRP MD5 authentication.
- Uses DUAL for loop prevention and fast convergence.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.
- Uses IPv6 multicast FF02::A for EIGRP updates.
- High scalability; used in large networks.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: RIPv2 broadcasts (255.255.255.255) its routing table every 30 seconds.
2. True or false: By default, EIGRP uses bandwidth, delay, reliability, and load to calculate the composite metric.
3. True or false: EIGRP routers maintain neighbor adjacencies.
4. True or false: EIGRP and RIPv2 support VLSMs and CIDR.
5. True or false: RIPv2 does not have the 15-hop limit of RIPv1.
6. RIP uses which port?
7. RIPng uses which port?
8. EIGRP uses which IP protocol number?
9. Between RIPv1, RIPv2, and EIGRP, which protocol would you recommend for use in a large network?
10. Between RIPv1, RIPv2, and EIGRP, which protocol would you use in a small network that has both Cisco and non-Cisco routers?
11. Which protocol uses the DUAL algorithm for fast convergence?
12. Match the protocol with the characteristic:

    i. EIGRP for IPv6

    ii. RIPv2

    iii. RIPng

    iv. EIGRP

    a. Uses multicast FF02::9

    b. Uses multicast 224.0.0.9

    c. Uses multicast 224.0.0.10

    d. Uses multicast FF02::

13. Why is EIGRP sometimes considered a hybrid protocol?

14. A small network is experiencing excessive broadcast traffic and slow response times. The current routing protocol is RIPv1. What design changes would you recommend?

    a. Migrate to RIPv2

    b. Migrate to RIPng

    c. Migrate to EIGRP for IPv4

    d. Migrate to EIGRP for IPv6

15. Which IPv6 routing protocol does not include authentication within the protocol?

16. Match the RIP routing table field with its description:

    i. IP address

    ii. Gateway

    iii. Interface

    iv. Metric

    v. Timer

    a. The number of hops to the destination

    b. Next router along the path to the destination

    c. Destination network or host, with subnet mask

    d. Used to access the physical network that must be used to reach the destination

    e. Time since the route entry was last updated

17. Match the EIGRP component with its description:

    i. RTP

    ii. DUAL

    iii. Protocol-dependent modules

    iv. Neighbor discovery

    a. An interface between DUAL and IPX RIP, IGRP, and AppleTalk

    b. Used to deliver EIGRP messages reliably

    c. Builds an adjacency table

    d. Guarantees a loop-free network

18. With Cisco routers, which protocols use only equal-cost load balancing?

19. With Cisco routers, which protocols allow unequal-cost load balancing?

20. You are designing a global network with more than 500 locations. The network topology is not hierarchical. What routing protocol would you recommend?

    a. RIPv2

    b. EIGRP

    c. OSPF

    d. IS-IS

21. Match each EIGRP parameter with its description:

    i. Feasible distance

    ii. Successor

    iii. Feasible successor

    iv. Active state

    a. The best path selected by DUAL

    b. The successor is down

    c. The lowest calculated metric of a path to reach the destination

    d. The second-best path

22. On an IPv6 network you have RIPng and EIGRP running. Both protocols have a route to destination 10.1.1.0/24. Which route gets injected into the routing table?

    a. The RIPng route

    b. The EIGRP route

    c. Both routes

    d. Neither route. There is a route conflict.

23. A network has a router diameter of 10. Both IPv4 and IPv6 are used. The company does not want to use proprietary routing protocols. Which routing protocol(s) can be used?

    a. RIPv2
    b. RIPng
    c. EIGRP
    d. EIGRP for IPv6
    e. OSPFv2
    f. OSPFv3
    g. Answers A and C
    h. Answers A, B, E, and F
    i. Answers C and D

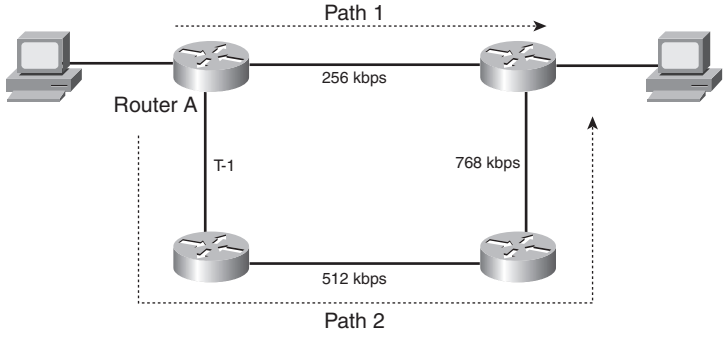
24. Complete Table 10-5 with the authentication, protocol/port, administrative distance, and IP version of each routing protocol.

Table 10-5 *Protocol Characteristics*

Characteristic	RIPv1	RIPv2	RIPng	EIGRP	EIGRP for IPv6
Authentication					
Protocol/port					
Administrative distance					
IP version					

Use Figure 10-9 to answer the remaining questions.

Figure 10-9 *Path Selection*



25. By default, if RIPv2 is enabled on all routers, what path is taken?
    a. Path 1
    b. Path 2
    c. Unequal load balancing with Path 1 and Path 2
    d. Equal load balancing with Path 1 and Path 2
26. By default, if RIPng is enabled on all routers, what path is taken?
    a. Path 1
    b. Path 2
    c. Unequal load balancing with Path 1 and Path 2
    d. Equal load balancing with Path 1 and Path 2
27. By default, if EIGRP is enabled on all routers, what path is taken?
    a. Path 1
    b. Path 2
    c. Unequal load balancing with Path 1 and Path 2
    d. Equal load balancing with Path 1 and Path 2
28. EIGRP is configured on the routers. If it is configured with the **variance** command, what path is taken?
    a. Path 1
    b. Path 2
    c. Unequal load balancing with Path 1 and Path 2
    d. Equal load balancing with Path 1 and Path 2
29. By default, if EIGRP for IPv6 is enabled on all routers, and this is an IPv6 network, what path is taken?
    a. Path 1
    b. Path 2
    c. Unequal load balancing with Path 1 and Path 2
    d. Equal load balancing with Path 1 and Path 2

This chapter covers the following subjects:

- OSPFv2
- OSPFv3
- IS-IS

CHAPTER 11

OSPF and IS-IS

This chapter reviews the characteristics and design issues of the Open Shortest Path First Version 2 (OSPFv2) and Intermediate System-to-Intermediate System (IS-IS) protocols. For IPv6 networks, OSPFv3 is also covered. OSPFv2, OSPFv3, and IS-IS are link-state routing protocols. They do not broadcast their route tables as distance-vector routing protocols do. Routers using link-state routing protocols send information about the status of their interfaces to all other routers in the area. Then they perform database computations to determine the shortest paths to each destination.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 11-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics..

Table 11-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
OSPFv2	1, 2, 4, 6, 7, 8
OSPFv3	10
IS-IS	3, 5, 9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which protocol defines an Area Border Router (ABR)?
   a. Enhanced Interior Gateway Routing Protocol (EIGRP)
   b. OSPF
   c. IS-IS
   d. On-Demand Routing (ODR)
2. Which routing protocols support variable-length subnet masks (VLSM)?
   a. EIGRP
   b. OSPF
   c. IS-IS
   d. A and B
   e. A and C
   f. B and C
   g. A, B, and C
3. Which IGP protocol is a common alternative to EIGRP and OSPF as a routing protocol in service provider networks?
   a. OSPFv2
   b. RIPv2
   c. IGRP
   d. IS-IS
4. What is an ASBR?
   a. Area Border Router
   b. Autonomous System Boundary Router
   c. Auxiliary System Border Router
   d. Area System Border Router
5. What is the default IS-IS metric for a T1 interface?
   a. 5
   b. 10
   c. 64
   d. 200
6. What is the OSPFv2 link-state advertisement (LSA) type for autonomous system (AS) external LSAs?
   a. Type 1
   b. Type 2

c. Type 3

d. Type 4

e. Type 5

7. What address do you use to multicast to the OSPFv2 designated router (DR)?

a. 224.0.0.1

b. 224.0.0.5

c. 224.0.0.6

d. 224.0.0.10

8. To where are OSPF Type 1 LSAs flooded?

a. The OSPF area

b. The OSPF domain

c. From the area to the OSPF backbone

d. Through the virtual link

9. In IS-IS networks, the backup designated router (BDR) forms adjacencies to what routers?

a. Only to the DR.

b. To all routers.

c. The BDR becomes adjacent only when the DR is down.

d. There is no BDR in IS-IS.

10. What OSPFv3 LSA carries address prefixes?

a. Network LSA

b. Summary LSA

c. Inter-Area-Router LSA

d. Intra-Area-Prefix LSA

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers the link-state routing protocols: OSPFv2, OSPFv3, and IS-IS. These three routing protocols are Interior Gateway Protocols (IGP) used within an autonomous system. OSPF is a popular standards-based protocol used in enterprises. IS-IS is commonly used by large Internet service providers (ISP) in their internal networks.

For the CCDA test, understand the characteristics and design constraints of these routing protocols. You should know the differences between OSPF, IS-IS, and the distance-vector routing protocols covered in Chapter 10, "RIP and EIGRP Characteristics and Design."

OSPFv2

RFC 2328 defines OSPFv2, a link-state routing protocol that uses Dijkstra's shortest path first (SPF) algorithm to calculate paths to destinations. OSPFv2 is used in IPv4 networks. OSPF was created for its use in large networks where RIP failed. OSPF improved the speed of convergence, provided for the use of VLSMs, and improved the path calculation.

In OSPF, each router sends link-state advertisements about itself and its links to all other routers in the area. Note that it does not send routing tables but link-state information about its interfaces. Then, each router individually calculates the best routes to the destination by running the SPF algorithm. Each OSPF router in an area maintains an identical database describing the area's topology. The routing table at each router is individually constructed using the local copy of this database to construct a shortest-path tree.

OSPFv2 is a classless routing protocol that permits the use of VLSMs and classless interdomain routing (CIDR). With Cisco routers, OSPF also supports equal-cost multipath load balancing and neighbor authentication. OSPF uses multicast addresses to communicate between routers. OSPF uses IP protocol 89.

OSPFv2 Concepts and Design

This section covers OSPF theory and design concepts. It discusses OSPF LSAs, area types, and router types. OSPF uses a two-layer hierarchy with a backbone area at the top and all other areas below. Routers send LSAs informing other routers of the status of their interfaces. The use of LSAs and the limitation of OSPF areas are important concepts to understand for the test.

OSPFv2 Metric

The metric that OSPFv2 uses is cost. It is an unsigned 16-bit integer in the range of 1 to 65,535. The default cost for interfaces is calculated based on the bandwidth in the formula 10^8/BW, where BW is the bandwidth of the interface expressed as a full integer of bps. If the result is smaller than 1, the cost is set to 1. A 10BASE-T (10 Mbps = 10^7 bps) interface has a cost of $10^8/10^7 = 10$. OSPF performs a summation of the costs to reach a destination; the lowest cost is the preferred path. Table 11-2 shows some sample interface metrics.

Table 11-2 *OSPF Interface Costs*

Interface Type	OSPF Cost
10 Gigabit Ethernet	.01 => 1
Gigabit Ethernet	.1 => 1
OC-3 (155 Mbps)	.64516 => 1
Fast Ethernet	$10^8/10^8 = 1$
DS-3 (45 Mbps)	2
Ethernet	$10^8/10^7 = 10$
T1	64
512 kbps	195
256 kbps	390

The default reference bandwidth used to calculate OSPF costs is 10^8 (cost = 10^8/BW). Notice that for technologies that support speeds greater than 100 Mbps, the default metric gets set to 1 without regard for the network's different capabilities (speed).

Because OSPF was developed prior to high-speed WAN and LAN technologies, the default metric for 100 Mbps was 1. Cisco provides a method to modify the default reference bandwidth. The cost metric can be modified on every interface.

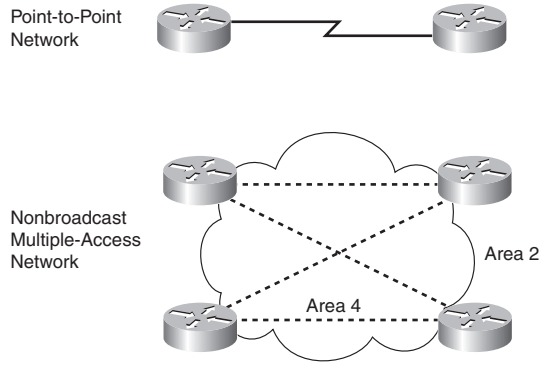
OSPFv2 Adjacencies and Hello Timers

OSPF uses Hello packets for neighbor discovery. The default Hello interval is 10 seconds (30 seconds for nonbroadcast multiaccess [NBMA] networks). Hellos are multicast to 224.0.0.5 (ALLSPFRouters). Hello packets include such information as the router ID, area ID, authentication, and router priority.

After two routers exchange Hello packets and set two-way communication, they establish adjacencies.

Figure 11-1 shows a point-to-point network and an NBMA network.

Figure 11-1 *OSPF Networks*



For point-to-point networks, valid neighbors always become adjacent and communicate using multicast address 224.0.0.5. For broadcast (Ethernet) and NBMA networks (Frame Relay), all routers become adjacent to the DR and BDR but not to each other. All routers reply to the DR and BDR using the multicast address 224.0.0.6. The later section "OSPF DRs" covers the DR concept.

On OSPF point-to-multipoint nonbroadcast networks, it might be necessary to configure the set of neighbors that are directly reachable over the point-to-multipoint network. Each neighbor is identified by its IP address on the point-to-multipoint network. Non-broadcast point-to-multipoint networks do not elect DRs, so the DR eligibility of configured neighbors is undefined. OSPF communication in point-to-point networks use unicast addresses .

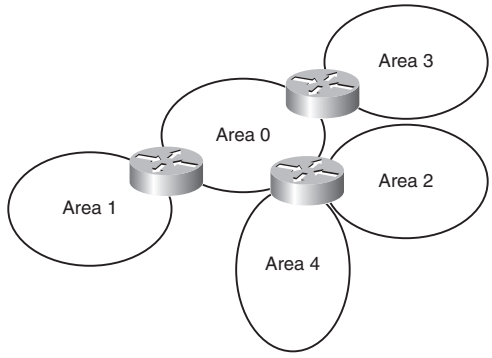
OSPF virtual links unicast OSPF packets. Later in this chapter, the section "Virtual Links" discusses virtual links.

OSPFv2 Areas

As a network grows, the initial flooding and database maintenance of LSAs can burden a router's CPU. OSPF uses areas to reduce these effects. An area is a logical grouping of routers and links that divides the network. Routers share link-state information with only the routers in their areas. This setup reduces the size of the database and the cost of computing the SPF tree at each router.

Each area is assigned a 32-bit integer number. Area 0 (or 0.0.0.0) is reserved for the backbone area. Every OSPF network should have a backbone area. The backbone area is responsible for distributing routing information between areas. It must exist in any internetwork using OSPF over multiple areas as a routing protocol. As you can see in Figure 11-2, communication between Area 1 and Area 2 must flow through Area 0. This communication can be internal to a single router that has interfaces directly connected to Areas 0, 1, and 2.

Figure 11-2 *OSPF Areas*

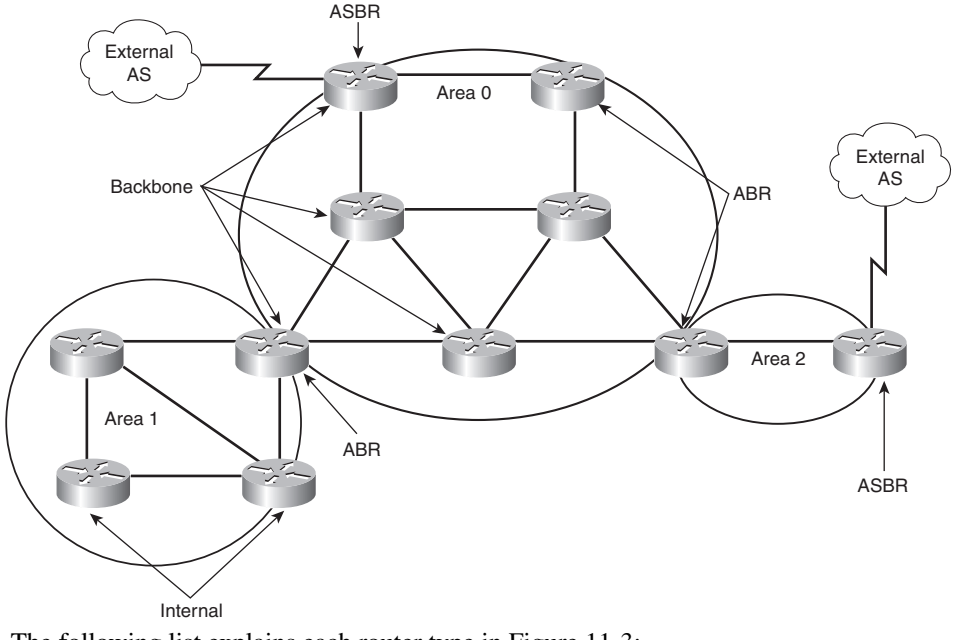


Intra-area traffic is packets passed between routers in a single area.

OSPF Router Types

OSPF classifies participating routers based on their place and function in the area architecture. Figure 11-3 shows OSPF router types.

Figure 11-3 *OSPF Router Types*



The following list explains each router type in Figure 11-3:

- **Internal router**—Any router whose interfaces all belong to the same OSPF area. These routers keep only one link-state database.

- **ABR**—Routers that are connected to more than one area. These routers maintain a link-state database for each area they belong to. These routers generate summary LSAs.
- **ASBR**—Routers that inject external LSAs into the OSPF database (redistribution). These external routes are learned via either other routing protocols or static routes.
- **Backbone router**—Routers with at least one interface attached to Area 0.

TIP An OSPF router can be an ABR, an ASBR, and a backbone router at the same time. The router is an ABR if it has an interface on Area 0 and another interface in another area. The router is a backbone router if it has one or more interfaces in Area 0. The router is an ASBR if it redistributes external routes into the OSPF network.

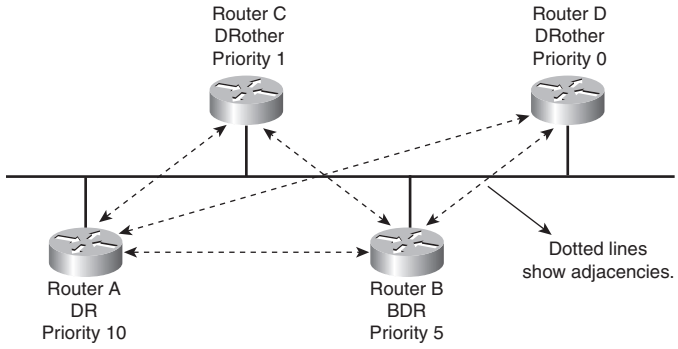
OSPF DRs

On multiaccess networks (such as Ethernet), some routers get selected as DRs. The purpose of the DR is to collect all LSAs for the multiaccess network and to forward the LSA to all non-DR routers; this arrangement reduces the amount of LSA traffic generated. A router can be the DR for one multiaccess network and not the DR in another attached multiaccess network.

The DR also floods the network LSAs to the rest of the area. OSPF also selects a BDR; it takes over the function of the DR if the DR fails. Both the DR and BDR become adjacent to all routers in the multiaccess network. All routers that are not DR and BDR are sometimes called DRothers. These routers are only adjacent to the DR and BDR. OSPF routers multicast LSAs only to adjacent routers. DRothers multicast packets to the DR and BDR using the multicast address 224.0.0.6 (ALLDRouters). The DR floods updates using ALLSPFRouters (224.0.0.5).

DR and BDR selection is based on an OSPF DR interface priority. The default value is 1, and the highest priority determines the DR. In a tie, OSPF uses the numerically highest router ID. The router ID is the IP address of the configured loopback interface. The router ID is the highest configured loopback address, or if the loopback is not configured then it's the highest physical address. Routers with a priority of 0 are not considered for DR/BDR selection. The dotted lines in Figure 11-4 show the adjacencies in the network.

Figure 11-4 *DRs*



In Figure 11-4, Router A is configured with a priority of 10, and Router B is configured with a priority of 5. Assuming that these routers are turned on simultaneously, Router A becomes the DR for the Ethernet network. Router C has a lower priority, becoming adjacent to Router A and Router B but not to Router D. Router D has a priority of 0 and thus is not a candidate to become a DR or BDR.

If you introduce a new router to the network with a higher priority than that of the current DR and BDR, it does not become the selected DR unless both the DR and BDR fail. If the DR fails, the current BDR becomes the DR.

LSA Types

OSPF routers generate LSAs that are flooded throughout an area or the entire autonomous system. OSPF defines different LSA types for participating routers, DRs, ABRs, and ASBRs. Understanding the LSA types can help you with other OSPF concepts. Table 11-3 describes the major LSA types. There are other LSA types that are not covered in this book.

Table 11-3 *Major LSA Types*

Type Code	Type	Description
1	Router LSA	Produced by every router. Includes all the router's links, interfaces, state of links, and cost. This LSA type is flooded within a single area.
2	Network LSA	Produced by every DR on every broadcast or NBMA network. It lists all the routers in the multiaccess network. This LSA type is contained within an area.
3	Summary LSA for ABRs	Produced by ABRs. It is sent into an area to advertise destinations outside the area.
4	Summary LSA for ASBRs	Originated by ABRs. Sent into an area by the ABR to advertise the ASBRs.

continues

Table 11-3 *Major LSA Types (Continued)*

Type Code	Type	Description
5	AS external LSA	Originated by ASBRs. Advertises destinations external to the OSPF AS, flooded throughout the whole OSPF AS.
7	Not-so-stubby area (NSSA) external LSA	Originated by ASBRs in an NSSA. It is not flooded throughout the OSPF autonomous system, only to the NSSA. Similar to the Type 5 LSA.

Type 1 and Type 2 LSAs are contained within each OSPF area. Routers in different areas pass interarea traffic. ABRs exchange Type 3 and Type 4 LSAs. Type 4 and Type 5 LSAs are flooded throughout all areas.

AS External Path Types

The two types of AS external paths are Type 1 (E1) and Type 2 (E2), and they are associated with Type 5 LSAs. ASBRs advertise external destinations whose cost can be just a redistribution metric (E2) or a redistribution metric plus the costs of each segment (E1) used to reach the ASBR.

By default, external routes are of Type 2, which is the metric (cost) used in the redistribution. Type 1 external routes have a metric that is the sum of the redistribution cost plus the cost of the path to reach the ASBR.

OSPF Stub Area Types

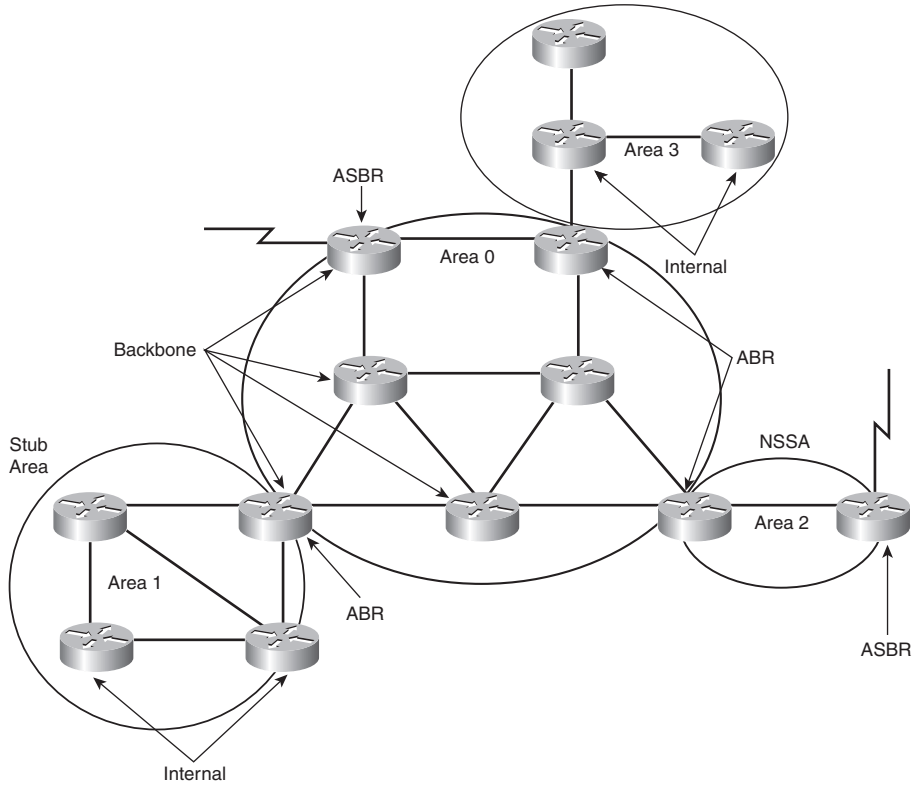
OSPF provides support for stub areas. The concept is to reduce the number of interarea or external LSAs that get flooded into a stub area. RFC 2328 defines OSPF stub areas. RFC 1587 defines support for NSSAs. Cisco routers use totally stubby areas, such as Area 2 as shown in Figure 11-5.

Stub Areas

Consider Area 1 in Figure 11-5. Its only path to the external networks is via the ABR through Area 0. All external routes are flooded to all areas in the OSPF AS. You can configure an area as a stub area to prevent OSPF external LSAs (Type 5) from being flooded into that area. A single default route is injected into the stub area instead. If multiple ABRs exist in a stub area, all inject the default route. Traffic originating within the stub area routes to the closest ABR.

Note that network summary LSAs (Type 3) from other areas are still flooded into the Stub Area 1.

Figure 11-5 *OSPF Stub Networks*



Totally Stubby Areas

Take the Area 1 in Figure 11-5 one step further. The only path for Area 1 to get to Area 0 and other areas is through the ABR. A totally stubby area does not flood network summary LSAs (Type 3). It stifles Type 4 LSAs as well. Like regular stub areas, totally stubby areas do not flood Type 5 LSAs. They send just a single LSA for the default route. If multiple ABRs exist in a totally stubby area, all ABRs inject the default route. Traffic originating within the totally stubby area routes to the closest ABR.

NSSAs

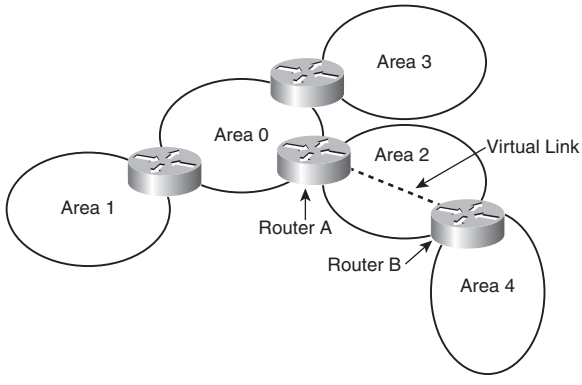
Notice that Area 2 in Figure 11-5 has an ASBR. If this area is configured as an NSSA, it generates the external LSAs (Type 7) into the OSPF system while retaining the characteristics of a stub area to the rest of the AS. There are two options for the ABR. First, the ABR for Area 2 can translate the NSSA external LSAs (Type 7) to AS external LSAs (Type 5) and flood the rest of the internetwork. Second, the ABR is not configured to convert the NSSA external LSAs to Type 5 external LSAs, thus the NSSA external LSAs remain within the NSSA.

Virtual Links

OSPF requires that all areas be connected to a backbone router. Sometimes, WAN link provisioning or failures can prevent an OSPF area from being directly connected to a backbone router. You can use virtual links to temporarily connect (virtually) the area to the backbone.

As shown in Figure 11-6, Area 4 is not directly connected to the backbone. A virtual link is configured between Router A and Router B. The flow of the virtual link is unidirectional and must be configured in each router of the link. Area 2 becomes the transit area through which the virtual link is configured. Traffic between Areas 2 and 4 does not flow directly to Router B. Instead, the traffic must flow to Router A to reach Area 0 and then pass through the virtual link.

Figure 11-6 *OSPF Virtual Link*



OSPFv2 Router Authentication

OSPFv2 supports the authentication of routes using 64-bit clear text or cryptographic Message Digest 5 (MD5) authentication. Plain-text authentication passwords do not need to be the same for the routers throughout the area, but they must be the same between neighbors.

MD5 authentication provides higher security than plain-text authentication. As with plain-text authentication, passwords don't have to be the same throughout an area, but they do need to be same between neighbors.

OSPFv2 Summary

OSPFv2 is used in large enterprise IPv4 networks. The network topology must be hierarchical. OSPF is used in the enterprise campus building access, distribution, and core layers. OSPF is also used in the enterprise data center, WAN/MAN, and branch offices.

The characteristics of OSPFv2 follow:

- Link-state routing protocol.
- Uses IP protocol 89.
- Classless protocol (supports VLSMs and CIDR).
- Metric is cost (based on interface bandwidth by default).
- Fast convergence. Uses link-state updates and SPF calculation.
- Reduced bandwidth use. Sends partial route updates only when changes occur.
- Routes are labeled as intra-area, interarea, external Type 1, or external Type 2.
- Support for authentication.
- Uses the Dijkstra algorithm to calculate the SPF tree.
- Default administrative distance is 110.
- Uses multicast address 224.0.0.5 (ALLSPFRouters).
- Uses multicast address 224.0.0.6 (ALLDRouters).
- Very good scalability. Recommended for large networks.

OSPFv3

RFC 2740 describes OSPF Version 3 for routing in IPv6 networks. Note that OSPFv3 is for IPv6 networks only and that it is not backward-compatible with OSPFv2 (used in IPv4). OSPF algorithms and mechanisms, such as flooding, router types, designated router election, areas, stub and NSSA, and shortest path first (SPF) calculations, remain the same. Changes are made for OSPF to support IPv6 addresses, address hierarchy, and IPv6 for transport. OSPFv3 uses multicast group FF02::5 for all OSPF routers and FF02::6 for all designated routers.

OSPFv3 Changes from OSPFv2

The following are the major changes for OSPFv3:

- **Version number is 3**—Obviously this is a newer version of OSPF, and it runs over IPv6 only.
- **Support for IPv6 addressing**—New LSAs created to carry IPv6 addresses and prefixes.
- **Per-link processing**—OSPFv2 uses per-subnet processing. With link processing, routers in the same link can belong to multiple subnets.

- **Address semantics removed**—Addresses are removed from the router and network LSAs. These LSAs now provide topology information.
- **No authentication in the OSPFv3 protocol**—OSPFv3 uses the authentication schemes inherited in IPv6.
- **New Link LSA**—For local-link flooding scope.
- **New Intra-Area-Prefix LSA**—Carries all the IPv6 prefix information. Similar to OSPFv2 router and network LSAs.
- **Identifying neighbors by router ID**—Neighbors are *always* identified by the router ID. This does not occur in OSPFv2 point-to-point and broadcast networks.

NOTE In OSPFv3, the router IDs, area IDs, and LSA link state IDs remain at the size of 32 bits. Larger IPv6 addresses cannot be used.

OSPFv3 Areas and Router Types

OSPFv3 retains the same structure and concepts as OSPFv2. The area topology, interfaces, neighbors, link-state database, and routing table remain the same. RFC 2740 does not define new area types or router types.

The OSPF areas shown in Figure 11-2 and the router types shown in Figure 11-3 remain the same. The router types in relation to the OSPF areas are

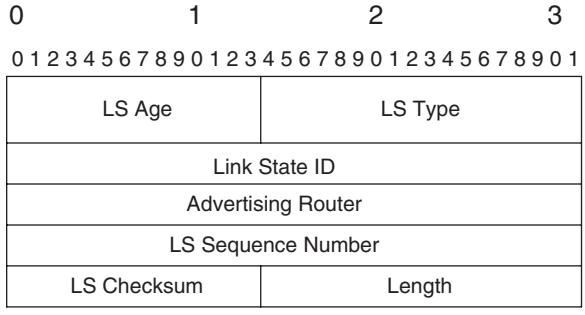
- **Internal router**—Any router whose interfaces all belong to the same OSPF area. These routers keep only one link-state database.
- **ABR**—Routers that are connected to more than one area, in which one area is Area 0. These routers maintain a link-state database for each area they belong to. These routers generate summary LSAs.
- **ASBR**—Routers that inject external LSAs into the OSPF database (redistribution). These external routes are learned via either other routing protocols or static routes.
- **Backbone router**—Routers with at least one interface attached to Area 0.

OSPFv3 Link State Advertisements

OSPFv3 retains the LSA types used by OSPFv2 with some modifications and introduces two new LSAs: Link LSA and Intra-Area-Prefix.

All LSAs use a common 20-byte header that indicates the LS type, the advertising router, and the sequence number. Figure 11-7 shows the format of the LSA header.

Figure 11-7 *LSA Header*



The LS age indicates the time in seconds since the LSA was generated.

The LS type indicates the function performed by this LSA. This field includes a U bit and S2 and S1 bits. When the U bit is set to 0, the LSA is only flooded locally. When the U bit is set to 1, the LSA is stored and flooded. The S1 and S2 bits have the functions indicated in Table 11-4.

Table 11-4 *LSA Header S2 S1 Bits*

S2 S1	Flooding Scope
00	Link-local scope
01	Flood to all routers within the area
10	Flood to all routers within the AS
11	Reserved

The Link State ID is used with the LS type and advertising router to identify the link-state database. The Advertising Router field contains the 32-bit router ID of the router that generated the LSA. The LS Sequence Number is used to detect old or duplicate LSAs. The LS Checksum is for error checking. The Length field indicates the length of the LSA, including the header.

Table 11-5 summarizes the nine LSAs that can be used in OSPF. Most LSAs retain the same function used in OSPFv2 for IPv4. Each OSPFv3 LSA is described in more detail following the table.

Table 11-5 *OSPFv3 LSA Types*

LSA Name	LS Type	Description
Router LSA	0x2001	State of router interfaces
Network LSA	0x2002	Generated by DR routers in broadcast or NBMA networks

continues

Table 11-5 *OSPFv3 LSA Types (Continued)*

LSA Name	LS Type	Description
Inter-Area-Prefix LSA	0x2003	Routes to prefixes in other areas
Inter-Area-Router LSA	0x2004	Routes to routers in other areas
AS-External LSA	0x4005	Routes to networks external to the AS
Group-Membership LSA	0x2006	Networks that contain multicast groups
NSSA Type 7 LSA	0x2007	Routers to networks external to the AS, injected into the NSSA
Link LSA	0x0008	Link-local addresses and list IPv6 prefixes associated with the link
Intra-Area-Prefix LSA	0x2009	IPv6 prefixes associated with a router, a stub network, or an associated transit network segment

Router LSAs describe the cost and state of all the originating router's interfaces. These LSAs are flooded within the area only. Router LSAs are LS type 0x2001. No IPv6 prefixes are contained in this LSA.

Network LSAs are originated by DRs in broadcast or NBMA networks. They describe all routers attached to the link that are adjacent to the DR. These LSAs are flooded within the area only. The LS type is 0x2002. No IPv6 prefixes are contained in this LSA.

Inter-Area-Prefix LSAs describe routes to IPv6 prefixes that belong to other areas. They are similar to OSPFv2 type 3 summary LSAs. The Inter-Area-Prefix LSA is originated by the ABR and has an LS type of 0x2003. It is also used to send the default route in stub areas. These LSAs are flooded within the area only.

Each Inter-Area-Router LSA describes a route to a router in another area. It is similar to OSPF type 4 summary LSAs. It is originated by the ABR and has an LS type of 0x2004. These LSAs are flooded within the area only.

AS-External LSAs describe networks that are external to the autonomous system (AS). These LSAs are originated by ASBRs, have an LS type of 0x4005, and thus are flooded to all routers in the AS.

The group-membership LSA describes the directly attached networks that contain members of a multicast group. This LSA is limited to the area and has an LS type of 0x2006. This LSA is described further in RFC 1584.

Type-7 LSAs describe networks that are external to the AS, but they are flooded to the NSSA area only. NSSAs are covered in RFC 1587. This LSA is generated by the NSSA ASBR and has a type of 0x2007.

Link LSAs describe the router's link-local address and a list of IPv6 prefixes associated with the link. This LSA is flooded to the local link only and has a type of 0x0008.

The Intra-Area-Prefix LSA is a new LSA type that is used to advertise IPv6 prefixes associated with a router, a stub network, or an associated transit network segment. This LSA contains information that used to be part of the router-LSAs and network-LSAs.

OSPFv3 Summary

OSPFv3 is used in large enterprise IPv6 networks. The network topology must be hierarchical. OSPF is used in the enterprise campus building access, distribution, and core layers. OSPF is also used in the enterprise data center, WAN/MAN, and branch offices.

The characteristics of OSPFv3 follow:

- Link-state routing protocol for IPv6.
- Uses IPv6 Next Header 89.
- Metric is cost (based on interface bandwidth by default).
- Sends partial route updates only when changes occur.
- Routes are labeled as intra-area, interarea, external Type 1, or external Type 2.
- Uses IPv6 for authentication.
- Uses the Dijkstra algorithm to calculate the SPF tree.
- Default administrative distance is 110.
- Uses multicast address FF02::5 (ALLSPFRouters).
- Uses multicast address FF02::6 (ALLDRouters).
- Recommended for large IPv6 networks.

IS-IS

IS-IS is an International Organization for Standardization (ISO) dynamic routing specification. IS-IS is described in ISO/IEC 10589, reprinted by the Internet Engineering Task Force (IETF) as RFC 1142. IS-IS is a link-state routing protocol that floods link-state information throughout the

network to build a picture of network topology. IS-IS was primarily intended to route OSI Connectionless Network Protocol (CLNP) packets but can also route IP packets. IP packet routing uses Integrated IS-IS, which provides the ability to route protocols such as IP. IS-IS is a common alternative to other powerful routing protocols such as OSPF and EIGRP in large networks. Although it isn't seen much in enterprise networks, IS-IS is commonly used for internal routing in large ISP networks.

IS-IS creates two levels of hierarchy, with Level 1 for intra-area and Level 2 for interarea routing. IS-IS distinguishes between Level 1 and Level 2 intermediate systems (IS). Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs (routers) are configured for L1/L2 areas, which route between Level 1 areas and form an intra-domain routing backbone. Hierarchical routing simplifies backbone design because Level 1 ISs only need to know how to get to the nearest Level 2 IS.

NOTE In IS-IS, a router is usually the IS, and PCs, workstations, and servers are end systems (ES). End System-to-Intermediate System links are Level 0.

IS-IS Metrics

IS-IS as originally defined uses a composite metric with a maximum path value of 1023. The required default metric is arbitrary and typically is assigned by a network administrator. By convention, it is intended to measure the circuit's capacity to handle traffic, such as its throughput in bits per second. Higher values indicate a lower capacity. Any single link can have a maximum value of 63. IS-IS calculates path values by summing link values. The standard sets the maximum metric values to provide the granularity to support various link types. It also ensures that the shortest-path algorithm used for route computation is reasonably efficient.

In Cisco routers, all interfaces have a default metric of 10. The administrator must configure the interface metric to get a different value. This small metric value range has proven insufficient for large networks. It also provides too little granularity for new features such as traffic engineering and other applications, especially with high-bandwidth links. Cisco IOS Software addresses this issue with the support of a 24-bit metric field, the so-called "wide metric." Wide metrics are also required for route leaking. Using the new metric style, link metrics now have a maximum value of 16,777,215 ($2^{24} - 1$), with a total path metric of 4,261,412,864 ($254 * 2^{24}$ or 2^{32}). Deploying IS-IS in the IP network with wide metrics is recommended for enabling finer granularity and supporting future applications such as traffic engineering.

IS-IS also defines three optional metrics (costs): delay, expense, and error. Cisco routers do not support the three optional metrics. The wide metric noted earlier uses the octets reserved for these metrics.

IS-IS Operation and Design

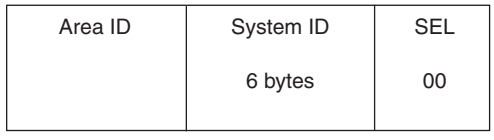
This subsection discusses IS-IS areas, designated routers, authentication, and the NET. IS-IS defines areas differently from OSPF; area boundaries are links and not routers. IS-IS has no BDRs. Because IS-IS is an OSI protocol, it uses a NET to identify each router.

NET

To configure the IS-IS routing protocol, you must configure a NET on every router. Although configuring NET is not a CCDA test requirement, this information is included for "extra credit."

Although you can configure IS-IS to route IP, the communication between routers uses OSI PDUs. The NET is the OSI address used for each router to communicate with OSI PDUs. A NET address ranges from 8 to 20 bytes. It consists of a domain, area ID, system ID, and selector (SEL), as shown in Figure 11-8.

Figure 11-8 *NET*



IS-IS routers use the area ID. The system ID must be the same length for all routers in an area. For Cisco routers, it must be 6 bytes in length. Usually, a router MAC address identifies each unique router. The SEL is configured as 00. You configure the NET with the **net** subcommand under the **router isis** command. In the following example, the domain authority and format identifier (AFI) is 49, the area is 0001, the system ID is 00aa.0101.0001, and the SEL is 00:

```
router isis
 net 49.0001.00aa.0101.0001.00
```

IS-IS DRs

As with OSPF, IS-IS selects DRs on multiaccess networks. It does not choose a backup DR as does OSPF. By default, the priority value is 64. You can change the priority value to a value from 0 to 127. If you set the priority to 0, the router is not eligible to become a DR for that network. IS-IS uses the highest system ID to select the DR if there is a tie with the priorities. On point-to-point networks, the priority is 0 because no DR is elected. In IS-IS, all routers in a multiaccess network establish adjacencies with all others in the subnetwork, and IS-IS neighbors become adjacent upon the discovery of one another. Both these characteristics are different from OSPF behavior.

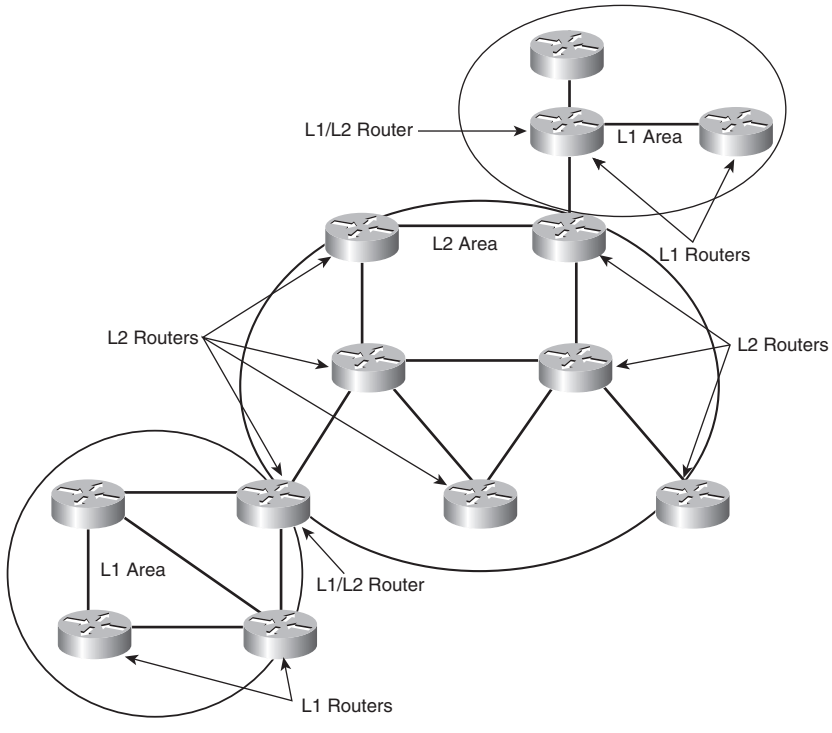
IS-IS Areas

IS-IS uses a two-level hierarchy similar to the OSPF area hierarchy developed later. Routers are configured to route Level 1 (L1), Level 2 (L2), or both Level 1 and Level 2 (L1/L2). Level 1 routers are like OSPF internal routers in a Cisco totally stubby area. An L2 router is similar to an OSPF backbone router. A router that has both Level 1 and Level 2 routes is similar to an OSPF ABR. IS-IS does not define a backbone area, but you can consider the backbone a continuous path of adjacencies among Level 2 ISs.

The L1/L2 routers maintain a separate link-state database for the L1 routes and L2 routes. Also, the L1/L2 routers do not advertise L2 routes to the L1 area. L1 routers do not have information about destinations outside the area and use L1 routes to their L1/L2 router to reach outside destinations.

As shown in Figure 11-9, IS-IS areas are bounded not by the L1/L2 routers but by the links between L1/L2 routers and L2 backbone routers.

Figure 11-9 *IS-IS Areas and Router Types*



IS-IS Authentication

IS-IS supports three types of clear-text authentication: link authentication, area authentication, and domain authentication. All these types support only clear-text password authentication. Recently, an RFC draft added support for an IS-IS MD5.

Routers in a common subnetwork (Ethernet, private line) use link authentication. The clear-text password must be common only between the routers in the link. Level 1 and Level 2 routes use separate passwords.

With area authentication, all routers in the area must use the same authentication mode and must have the same password.

Only L2 and L1/L2 routers use domain authentication. All L2 and L1/L2 routers must be configured for the same authentication mode and must use the same password.

IS-IS for IPv6

The specification for routing IPv6 with integrated IS-IS is currently an Internet draft (draft-ietf-isis-ipv6-06.txt) of the IETF. The draft specifies new type, length, and value (TLV) objects, reachability TLVs, and an interface address TLV to forward IPv6 information in the network. IOS currently supports IS-IS for IPv6, as described in the draft standard. Because IS-IS for IPv6 is not a focus area for the CCDA, refer to the IETF drafts for further information.

IS-IS Summary

The characteristics of IS-IS follow:

- Link-state protocol.
- Uses OSI CLNP to communicate with routers.
- Classless protocol (supports VLSMs and CIDR).
- Default metric is set to 10 for all interfaces.
- Single metric: single link max = 63, path max = 1023.
- Sends partial route updates only when changes occur.
- Authentication with clear-text passwords and MD5.
- Administrative distance is 115.
- Used in large service provider networks. Not recommended for enterprise networks. Sometimes attractive compared to OSPF and EIGRP.

- Described in ISO/IEC 10589; reprinted by the IETF as RFC 1142.
- IETF draft for routing IPv6 with IS-IS.

References and Recommended Readings

Bruno, A. *CCIE Routing and Switching Exam Certification Guide*. Indianapolis: Cisco Press, 2002.

Coltun, R., D. Ferguson, and J. Moy. RFC 2740, *OSPF for IPv6*. Available from http://www.ietf.org/rfc.

Coltun, R. and V. Fuller. RFC 1587, *The OSPF NSSA Option*. Available from http://www.ietf.org/rfc.

Doyle, J. and J. Carroll. *Routing TCP/IP*, Volume I, Second Edition. Indianapolis: Cisco Press, 2005.

Martey, A. *IS-IS Network Design Solutions*. Indianapolis: Cisco Press, 2002.

Moy, J. RFC 1584, *Multicast Extensions to OSPF*. Available from http://www.ietf.org/rfc.

Moy, J. RFC 2328, *OSPF Version 2*. Available from http://www.ietf.org/rfc.

Oran, D., editor. RFC 1142, *OSI IS-IS Intra-domain Routing Protocol*. Available from http://www.ietf.org/rfc.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics covered in this chapter:

- **OSPFv2**—The OSPF link-state routing protocol for IPv4
- **OSPFv3**—OSPF link-state routing protocol for IPv6
- **IS-IS**—The IS-IS link-state routing protocol

Table 11-6 summarizes the OSPF router types. Know how to identify these routers from a description or a diagram. These router types apply to both OSPFv2 and OSPFv3.

Table 11-6 *OSPF Router Types*

OSPF Router Type	Description
Internal router	Router whose interfaces belong to the same OSPF area.
ABR	Router connected to more than one area. It generates summary LSAs.
ASBR	Router that injects external routes into the OSPF protocol.
Backbone router	Routers with at least one interface connected to Area 0.

Table 11-7 summarizes OSPF stub network types. Remember which LSAs are not permitted in each stub type. These stub types apply for both OSPFv2 and OSPFv3.

Table 11-7 *OSPF Stub Network Types*

OSPF Area Stub Type	Description	LSA Types Not Permitted
Stub area	No OSPF external LSAs	Type 5
Totally stubby	No OSPF external and summary LSAs	Type 3, Type 4, and Type 5
NSSA	No OSPF external, Type 7 produced by NSSA	Type 5

Table 11-8 summarizes OSPFv2 LSA types. Understand which routers generate the LSA and what type of information each contains.

Table 11-8 *OSPFv2 Major LSA Types*

Type Code	Type	Description
1	Router LSA	Produced by every router. It includes all the router's links, interfaces, state of links, and cost. This LSA type is flooded within a single area.
2	Network LSA	Produced by every DR on every broadcast or NBMA network. It lists all the routers in the multiaccess network. This LSA type is contained within an area.
3	Summary LSA for ABRs	Produced by ABRs. It is sent into an area to advertise destinations outside the area.
4	Summary LSA for ASBRs	Originated by ABRs. Sent into an area by the ABR to advertise the ASBRs.
5	AS external LSA	Originated by ASBRs. Advertises destinations external to the OSPF AS, flooded throughout the whole OSPF AS.
7	NSSA external LSA	Originated by ASBRs in an NSSA. It is not flooded throughout the OSPF AS, only to the NSSA.

OSPFv2 Summary

Memorize the characteristics of OSPFv2, as listed here:

- Link-state routing protocol.
- Uses IP protocol 89.
- Classless protocol (supports VLSMs and CIDR).
- Metric is cost (based on interface bandwidth by default).
- Fast convergence. Uses link-state updates and SPF calculation.
- Reduced bandwidth use. Sends partial route updates only when changes occur.
- Routes are labeled as intra-area, interarea, external Type 1, or external Type 2.
- Support for authentication.
- Uses the Dijkstra algorithm to calculate the SPF tree.

- Default administrative distance is 110.
- Uses multicast address 224.0.0.5 (ALLSPFRouters).
- Uses multicast address 224.0.0.6 (ALLDRouters).
- Very good scalability. Recommended for large networks.

OSPFv3 Summary

The characteristics of OSPFv3 follow:

- Link-state routing protocol for IPv6.
- Uses IPv6 Next Header 89.
- Metric is cost (based on interface bandwidth by default).
- Sends partial route updates only when changes occur.
- Routes are labeled as intra-area, interarea, external Type 1, or external Type 2.
- Uses IPv6 for authentication.
- Uses the Dijkstra algorithm to calculate the SPF tree.
- Default administrative distance is 110.
- Uses multicast address FF02::5 (ALLSPFRouters).
- Uses multicast address FF02::6 (ALLDRouters).
- Recommended for large IPv6 networks.

Table 11-9 summarizes OSPFv3 LSA types.

Table 11-9 *OSPFv3 LSA Types*

LSA Name	LS Type	Description
Router LSA	0x2001	State of router interface
Network LSA	0x2002	Generated by DR routers in broadcast or NBMA networks
Inter-Area-Prefix LSA	0x2003	Routes to prefixes in other areas
Inter-Area-Router LSA	0x2004	Routes to routers in other areas
AS-External LSA	0x4005	Routes to networks external to the AS
Group-membership LSA	0x2006	Networks that contain multicast groups

continues

Table 11-9 *OSPFv3 LSA Types (Continued)*

LSA Name	LS Type	Description
NSSA Type 7 LSA	0x2007	Routers to networks external to the AS, injected to the NSSA
Link LSA	0x0008	Link-local addresses and list IPv6 prefixes associated with the link
Intra-Area-Prefix LSA	0x2009	IPv6 prefixes associated with a router, a stub network, or an associated transit network segment

IS-IS Summary

Know and understand the characteristics of IS-IS, as summarized in the following list:

- Link-state protocol.
- Uses OSI CLNP to communicate with routers.
- Classless protocol (supports VLSMs and CIDR).
- Default metric is set to 10 for all interfaces.
- Single metric: single link max = 63, path max = 1023
- Sends partial route updates only when changes occur.
- Authentication with clear-text passwords and MD5.
- Administrative distance is 115.
- Used in large networks. Sometimes attractive compared to OSPF and EIGRP.
- Described in ISO/IEC 10589; reprinted by the IETF as RFC 1142.
- Support for IPv6 in draft IETF RFC.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: A router needs to have all its interfaces in Area 0 to be considered an OSPF backbone router.
2. True or false: Both OSPF and IS-IS use a designated router in multiaccess networks.
3. Which multicast addresses do OSPFv2 routers use?
4. Which multicast addresses are used by OSPFv3 routers?
5. What are the Cisco administrative distances of OSPF and IS-IS?
6. True or false: By default, IS-IS assigns a cost metric of 10 to a T1 interface and also 10 to an Ethernet interface.
7. Which OSPFv2 router type generates the OSPF Type 3 LSA?
8. Which OSPFv2 router type generates the OSPF Type 2 LSA?
9. What is included in an OSPFv2 router LSA?
10. True or false: An IS-IS L2 router is analogous to an OSPF backbone router.
11. True or false: The router with the lowest priority is selected as the OSPF DR.
12. Match the routing protocol with the description:

    i. EIGRP

    ii. OSPFv2

    iii. RIPv2

    iv. IS-IS

    a. Distance-vector protocol used in the edge of the network

    b. IETF link-state protocol used in the network core

    c. Hybrid protocol used in the network core

    d. OSI link-state protocol
13. What router produces OSPF Type 2 LSAs?

14. True or false: IS-IS uses the IP layer to communicate between routers.
15. What is the default OSPF cost for a Fast Ethernet interface?
16. Which link-state protocols support VLSMs?
17. Which routing protocol do you use in the core of a large enterprise network that supports VLSMs for a network with a mix of Cisco and non-Cisco routers?
18. True or false: An IS-IS L1/L2 router is similar to an OSPF ABR.
19. You use _____ to connect a nondirectly connected OSPF area to the backbone.
20. What is the benefit of designing for stub areas?
21. What constraint does the OSPF network design have for traffic traveling between areas?
22. True or false: The OSPF and IS-IS default costs for Fast Ethernet interfaces are the same.
23. How is OSPFv3 identified as the upper-layer protocol in IPv6?
24. Which routing protocols are recommended for large enterprise networks?
    a. RIPv2
    b. OSPFv2
    c. EIGRP
    d. IS-IS
    e. A and B
    f. B and C
    g. B and D
    h. A, B, C, and D
25. What OSPFv3 has an LS type of 0x0008?
    a. Router LSA
    b. Inter-Area-Router LSA
    c. Link LSA
    d. Intra-Area-Prefix LSA

26. Which routing protocols support VLSMs?

- **a.** RIPv1
- **b.** OSPFv2
- **c.** EIGRP
- **d.** RIPv2
- **e.** B and C
- **f.** B, C, and D

27. Which routing protocols have fast convergence?

- **a.** RIPv1
- **b.** OSPFv2
- **c.** EIGRP
- **d.** RIPv2
- **e.** B and C
- **f.** B, C, and D

28. Which routing protocols have fast convergence?

- **a.** RIPng
- **b.** OSPFv3
- **c.** EIGRP for IPv6
- **d.** RIPv2
- **e.** B and C
- **f.** B, C, and D

29. A retail chain has about 800 stores that connect to the headquarters and a backup location. The company wants to limit the amount of routing traffic used on the WAN links. What routing protocol(s) is/are recommended?

- **a.** RIPv1
- **b.** RIPv2
- **c.** OSPFv2
- **d.** EIGRP
- **e.** IS-IS
- **f.** BGP
- **g.** B, C, and D
- **h.** C and D
- **i.** C, D, and E

30. Which of the following statements is correct?

    a. OSPFv3 provides changes to OSPFv2 for use in IPv4 networks.

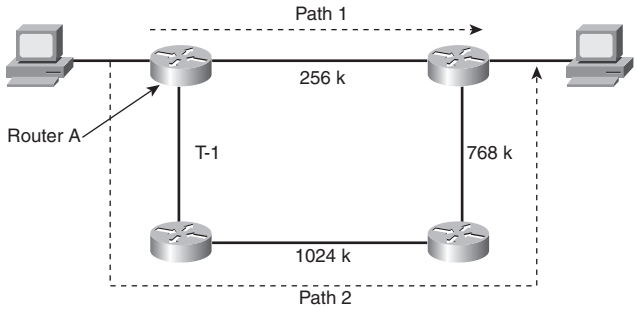
    b. OSPFv3 provides changes to OSPFv2 for use in IPv6 networks.

    c. OSPFv3 provides changes to OSPFv2 for use in IPv6 and IPv4 networks.

    d. OSPFng provides changes to OSPFv2 for use in IPv6 networks.

Use Figure 11-10 to answer the next two questions.

Figure 11-10 *Path Selection*



31. If IS-IS is enabled on all routers with the default metrics unchanged, what path is taken?

    a. Path 1

    b. Path 2

    c. Unequal load balance with Path 1 and Path 2

    d. Equal load balance with Path 1 and Path 2

32. If OSPF is enabled on all routers with the default metrics unchanged, what path is taken?

    a. Path 1

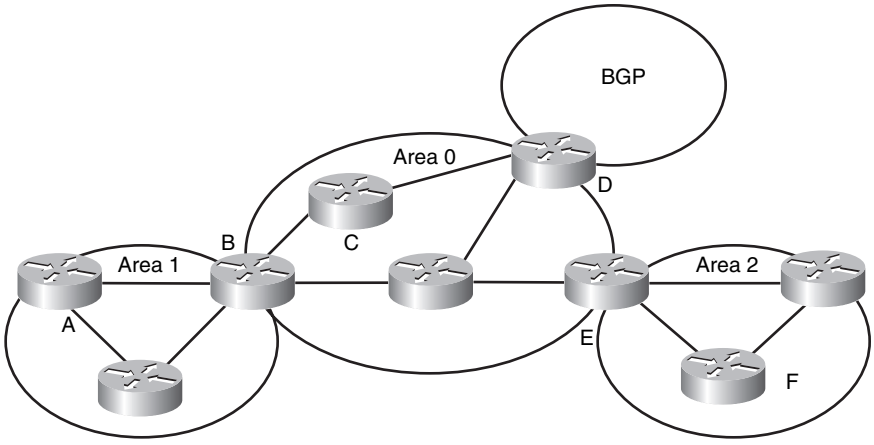
    b. Path 2

    c. Unequal load balance with Path 1 and Path 2

    d. Equal load balance with Path 1 and Path 2

Use Figure 11-11 to answer the following question.

Figure 11-11 *OSPF Router Types*



33. Identify the OSPF router types shown in Figure 11-11.

Router A = _____

Router B = _____

Router C = _____

Router D = _____

Router E = _____

Router F = _____

This chapter covers the following subjects:

- BGP
- Route Manipulation
- IP Multicast Review

CHAPTER 12

Border Gateway Protocol, Route Manipulation, and IP Multicast

This chapter covers the Border Gateway Protocol (BGP), which is used to exchange routes between autonomous systems. It is most frequently used between enterprises and service providers. The "Route Manipulation" section covers route summarization and redistribution of route information between routing protocols. The CCDA should know where redistribution occurs when required by the network design. This chapter also reviews policy-based routing (PBR) as a method to change the destination IP address based on policies. Finally, this chapter covers IP multicast protocols.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 12-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 12-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
BGP	1, 2, 7, 8
Route Manipulation	3, 4
IP Multicast Review	5, 6

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. What protocol do you use to exchange IP routes between autonomous systems?
   a. IGMP
   b. eBGP
   c. IGRP
   d. OSPF
2. What is the current version of BGP?
   a. BGP Version 2
   b. BGP Version 3
   c. BGP Version 4
   d. BGP Version 1
3. Where should routes be summarized?
   a. On the core routers
   b. On the distribution routers
   c. On the access routers
   d. None of the above
4. What is PBR?
   a. Public-Broadcast Routing
   b. Private-Based Routing
   c. Policy-Broadcast Routing
   d. Policy-Based Routing
5. What is IGMP?
   a. Interior Group Management Protocol
   b. Internet Group Management Protocol
   c. Interior Gateway Routing Protocol
   d. Interior Gateway Media Protocol
6. How many bits are mapped from the Layer 3 IPv4 multicast address to a Layer 2 MAC address?
   a. 16 bits
   b. 23 bits
   c. 24 bits
   d. 32 bits

7. What is the administrative distance of eBGP routes?

   a. 20

   b. 100

   c. 110

   d. 200

8. What is CIDR?

   a. Classful Intradomain Routing

   b. Classful Interior Domain Routing

   c. Classless Intradomain Routing

   d. Classless Interdomain Routing

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **7 or 8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

The "Foundation Topics" section includes discussions of BGP, PBR, route redistribution, and IP multicast protocols. The "BGP" section covers the characteristics and design of BGP. eBGP exchanges routes between autonomous systems. eBGP is commonly used between enterprises and their service providers.

The section "Route Manipulation" covers how you use PBR to change packets' destination addresses based on policies. This section also covers route summarization and redistribution of route information between routing protocols.

The section "IP Multicast Review" covers multicast protocols such as IGMP, Cisco Group Management Protocol (CGMP), and Protocol Independent Multicast (PIM).

BGP

This section covers BGP theory and design concepts. The current version of BGP, Version 4, is defined in RFC 1771 (March 1995). BGP is an interdomain routing protocol. What this means is that you use BGP to exchange routing information between autonomous systems. The primary function of BGP is to provide and exchange network-reachability information between domains or autonomous systems. BGP is a path vector protocol that is suited for setting routing policies between autonomous systems. In the enterprise campus architecture, BGP is used in the Internet connectivity module.

BGP is the de facto standard for routing between service providers on the Internet because of its rich features. You can also use it to exchange routes in large internal networks. The Internet Assigned Numbers Authority (IANA) reserved TCP Port 179 to identify the BGP protocol. BGPv4 was created to provide CIDR, a feature that was not present in the earlier versions of BGP. BGP is a path-vector routing protocol; it is neither a distance-vector nor link-state routing protocol.

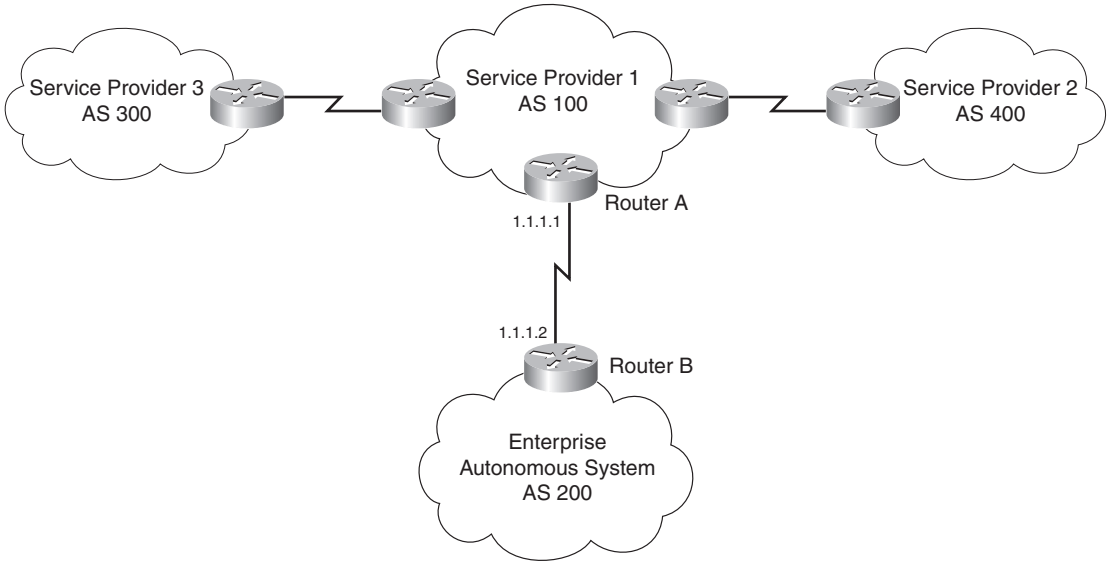
NOTE RFC 1519 describes CIDR, which provides the capability to forward packets based on IP prefixes only, with no concern for IP address class boundaries. CIDR was created as a means to constrain the growth of the routing tables in the Internet core through the summarization of IP addresses across network class boundaries. The early 1990s saw an increase in the growth of Internet routing tables and a reduction in Class B address space. CIDR provides a way for service providers to assign address blocks smaller than a Class B network but larger than a Class C network.

BGP Neighbors

BGP is usually configured between two directly connected routers that belong to different autonomous systems. Each autonomous system is under different technical administration. BGP is frequently used to connect the enterprise to service providers and to interconnect service providers, as shown in Figure 12-1. The routing protocol within the enterprise could be any interior gateway protocol (IGP). Common IGP choices include RIPv2, EIGRP, Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS). BGPv4 is the only deployed exterior gateway protocol (EGP). AS numbers are a managed resource allocated by the American Registry of Internet Numbers (ARIN). In IP, the AS numbers 64,512 through 65,535 are allocated to IANA and are designated for private use.

Before two BGP routers can exchange routing updates, they must become established neighbors. After BGP routers establish a TCP connection, exchange information, and accept the information, they become established neighbors and start exchanging routing updates. If the neighbors do not reach an established state, they do not exchange BGP updates. The information exchanged before the neighbors are established includes the BGP version number, AS number, BGP router ID, and BGP capabilities.

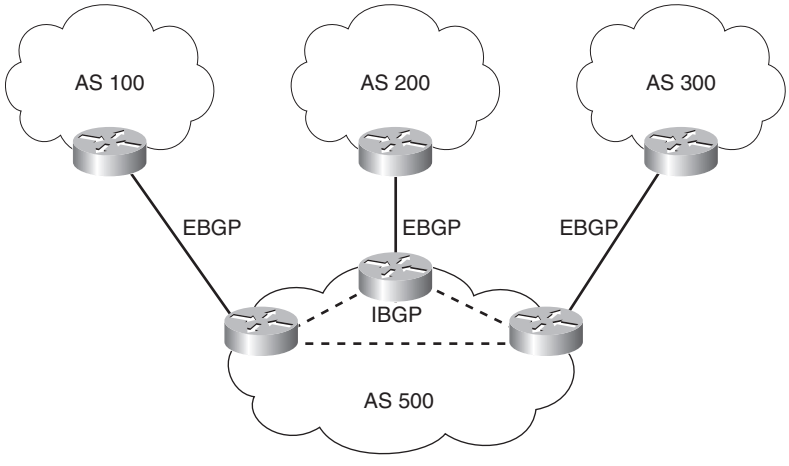
Figure 12-1 *BGP Neighbors*



eBGP

eBGP is the term used to describe BGP peering between neighbors in different autonomous systems. As required by RFC 1771, the eBGP peers share a common subnet. In Figure 12-2, all routers speak eBGP with routers in other autonomous systems. Within AS 500, the routers communicate using iBGP, which is covered next.

Figure 12-2 *eBGP Used Between Autonomous Systems*



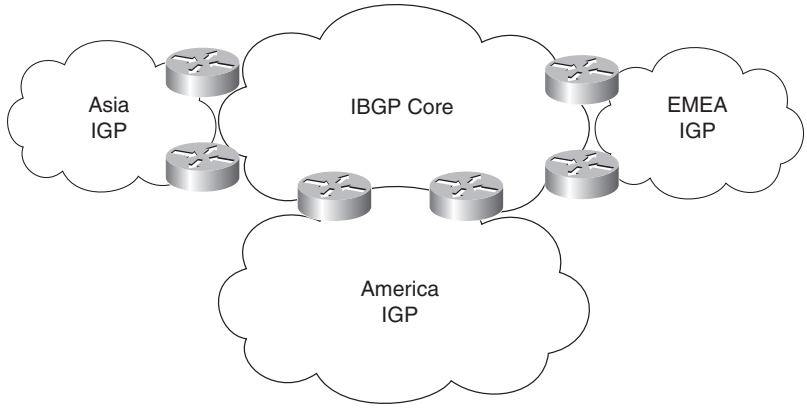
iBGP

iBGP is the term used to describe the peering between BGP neighbors in the same AS. iBGP is used primarily in transit autonomous systems. Transit autonomous systems forward traffic from one external AS to another external AS. If transit autonomous systems did not use iBGP, the eBGP-learned routes would have to be redistributed into an IGP and then redistributed into the BGP process in another eBGP router. Normally the number of eBGP routes is too large for an IGP to handle.

iBGP provides a better way to control the routes within the transit AS. With iBGP, the external route information (attributes) is forwarded. The various IGPs that might be used do not understand or forward BGP attributes, including AS paths, between eBGP routers.

Another use of iBGP is in large corporations where the IGP networks are in smaller independent routing domains along organizational or geographic boundaries. In Figure 12-3, a company has decided to use three independent IGPs: one for the Americas; another for Asia and Australia; and another for Europe, the Middle East, and Africa. Routes are redistributed into an iBGP core.

Figure 12-3 *iBGP in a Large Corporation*



Other Uses of iBGP

The CCDA should know at a high level these other uses for IBGP:

- **Applying policies in the internal AS with the help of BGP path attributes**—BGP path attributes are covered in a later section.
- **QoS Policy Propagation on BGP (QPPB)**—QPPB uses iBGP to spread common QoS parameters from one router to other routers in the network. It classifies packets using IP precedence bits based on BGP community lists, BGP AS paths, and access lists. After packets are classified, QoS features can enforce policies.
- **Multiprotocol BGP peering of Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPN)**—The multiprotocol version of BGP is used to carry MPLS VPN information between all PE routers within a VPN community.

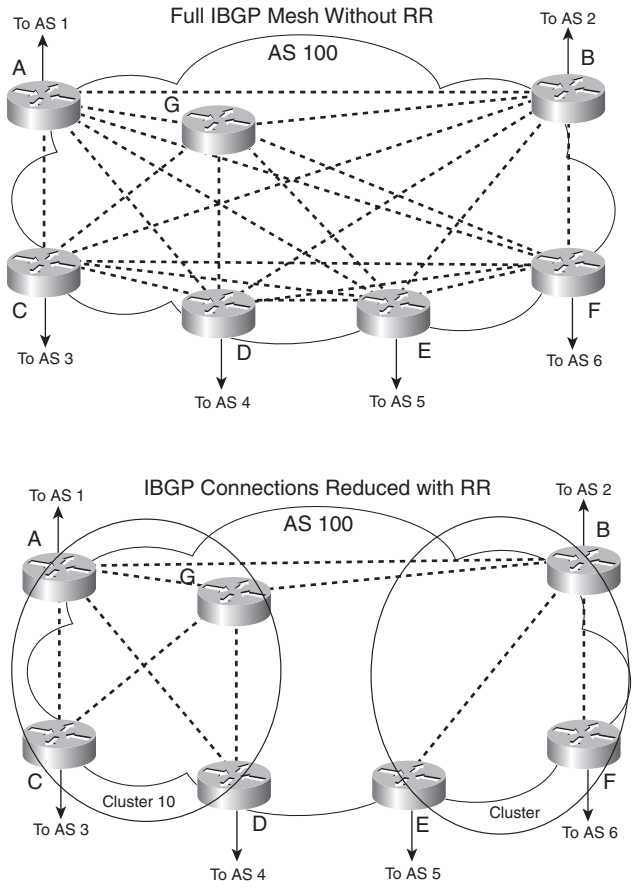
Route Reflectors

iBGP requires that all routers be configured to establish a logical connection with all other iBGP routers. The logical connection is a TCP link between all iBGP-speaking routers. The routers in each TCP link become BGP peers. In large networks, the number of iBGP-meshed peers can become very large. Network administrators can use route reflectors to reduce the number of required mesh links between iBGP peers. Some routers are selected to become the route reflectors to serve several other routers that act as route-reflector clients. Route reflectors allow a router to advertise or reflect routes to clients. The route reflector and its clients form a cluster. All client routers in the cluster peer with the route reflectors within the cluster. The route reflectors also peer with all other route reflectors in the internetwork. A cluster can have more than one route reflector.

In Figure 12-4, without route reflectors, all iBGP routers are configured in an iBGP mesh, as required by the protocol. When Routers A and G become route reflectors, they peer with Routers C and D; Router B becomes a route reflector for Routers E and F. Routers A, B, and G peer among each other.

NOTE The combination of the route reflector and its clients is called a cluster. In Figure 12-4, Routers A, G, C, and D form a cluster. Routers B, E, and F form another cluster.

Figure 12-4 *Route Reflectors*



Routers A and G are configured to peer with each other and with Routers B, C, and D. The configuration of Routers C and D is different from the rest; they are configured to peer with Routers A and G only. All route reflectors in the same cluster must have the same cluster ID number.

Router B is the route reflector for the second cluster. Router B peers with Routers A and G and with Routers E and F in its cluster. Routers E and F are route-reflector clients and peer only with

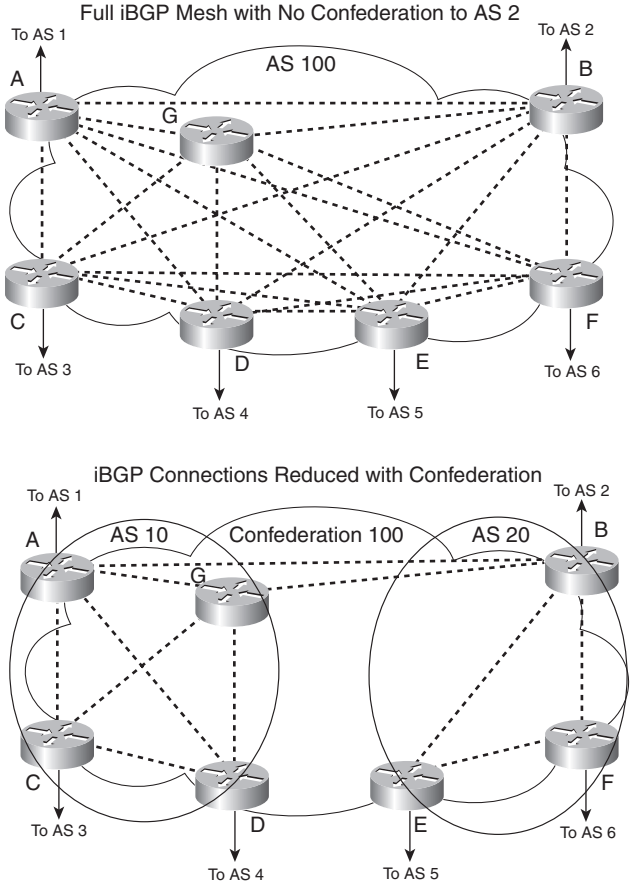
Router B. If Router B goes down, the cluster on the right goes down because no second route reflector is configured.

Confederations

Another method to reduce the iBGP mesh within an AS is BGP confederations. With confederations, the AS is divided into smaller, private autonomous systems, and the whole group is assigned a confederation ID. The private AS numbers or identifiers are not advertised to the Internet but are contained within the iBGP networks. The routers within each private AS are configured with the full iBGP mesh. Each private AS is configured with eBGP to communicate with other semiautonomous systems in the confederation. External autonomous systems see only the AS number of the confederation, and this number is configured with the BGP confederation identifier.

In Figure 12-5, a confederation divides the AS into two.

Figure 12-5 *BGP Confederations*



Routers A, B, and G are configured for eBGP between the private autonomous systems. You configure these routers with the **bgp confederation identifier** command. The confederation identifier number is the same for all routers in the network. You use the **bgp confederation peers** command to identify the AS number of other private autonomous systems in the confederation. Because Routers A and G are in AS 10, the peer confederation to Router B is AS 20. Router B is in AS 20, and its peer confederation to Routers A and G is AS 10. Routers C and D are part of AS 10 and peer with each other and with Routers A and G. Routers E and F are part of AS 20 and peer with each other and with Router B.

BGP Administrative Distance

The Cisco IOS Software assigns an administrative distance to eBGP and iBGP routes, as it does with other routing protocols. For the same prefix, the route with the lowest administrative distance is selected for inclusion in the IP forwarding table. Because iBGP-learned routes do not have metrics associated with the route as IGPs (OSPF and EIGRP) do, iBGP-learned routes are less trusted. For BGP, the administrative distances are

- **eBGP routes**—20
- **iBGP routes**—200

BGP Attributes, Weight, and the BGP Decision Process

BGP is a protocol that uses route attributes to select the best path to a destination. This subsection describes BGP attributes, the use of weight to influence path selection, and the BGP decision process.

BGP Path Attributes

BGP uses several attributes for the path-selection process. BGP uses path attributes to communicate routing policies. BGP path attributes include next hop, local preference, AS path, origin, multiexit discriminator (MED), atomic aggregate, and aggregator. Of these, the AS path is one of the most important attributes: It lists the number of AS paths to reach a destination network.

BGP attributes can be categorized as *well-known* or *optional*. Well-known attributes are recognized by all BGP implementations. Optional attributes do not have to be supported by the BGP process; they are used on a test or experimental basis.

Well-known attributes can be further subcategorized as *mandatory* or *discretionary*. Mandatory attributes are always included in BGP update messages. Discretionary attributes might or might not be included in the BGP update message.

Optional attributes can be further subcategorized as *transitive* or *nontransitive*. Routers must advertise the route with transitive attributes to its peers even if it does not support the attribute locally. If the path attribute is nontransitive, the router does not have to advertise the route to its peers.

The following subsections cover each attribute category.

Next-Hop Attribute

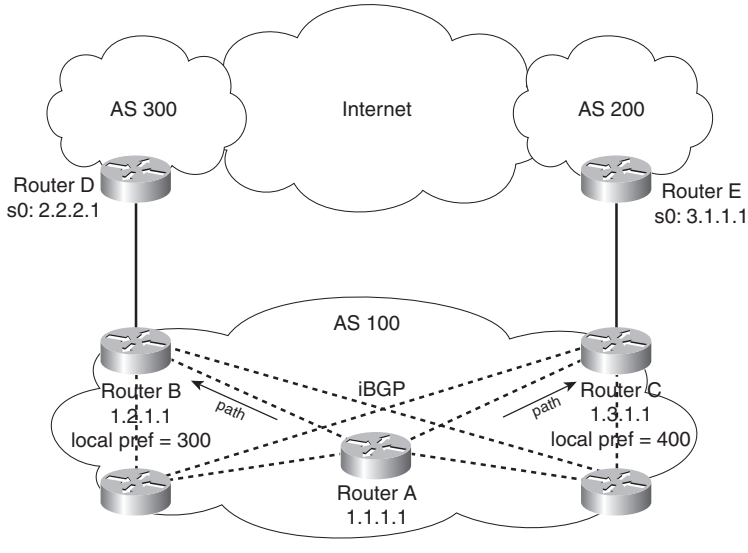
The next-hop attribute is the IP address of the next IP hop that will be used to reach the destination. The next-hop attribute is a well-known mandatory attribute. With eBGP, the eBGP peer sets the next hop when it announces the route. Multiaccess networks use the next-hop attribute where there is more than one BGP router.

Local Preference Attribute

The local preference attribute indicates which path to use to exit the AS. It is a well-known discretionary attribute used between iBGP peers and is not passed on to external BGP peers. In Cisco IOS Software, the default local preference is 100. The higher local preference is preferred.

The default local preference is configured on the BGP router with an external path; it then advertises its local preference to internal iBGP peers. Figure 12-6 shows an example of the local preference attribute where Routers B and C are configured with different local preference values. Router A and other iBGP routers then receive routes from both Router B and Router C. Router A prefers using Router C to route Internet packets because it has a higher local preference (400) than Router B (300). The arrows represent the paths taken to go out of the AS.

Figure 12-6 *BGP Local Preference*



Origin Attribute

Origin is a well-known mandatory attribute that defines the source of the path information. Do not confuse the origin with comparing whether the route is external (eBGP) or internal (iBGP). The origin attribute is received from the source BGP router. There are three types:

- **IGP**—Indicated by an i in the BGP table. Present when the route is learned by way of the **network** statement.
- **EGP**—Indicated by an e in the BGP table. Learned from EGP.
- **Incomplete**—Indicated by a ? in the BGP table. Learned from redistribution of the route.

In terms of choosing a route based on origin, BGP prefers routes that have been verified by an IGP over routes that have been learned from EGP peers, and BGP prefers routes learned from eBGP peers over incomplete paths.

AS Path Attribute

The AS path is a well-known mandatory attribute that contains a list of AS numbers in the path to the destination. Each AS prepends its own AS number to the AS path. The AS path describes all the autonomous systems a packet would have to travel to reach the destination IP network. It is used to ensure that the path is loop-free. When the AS path attribute is used to select a path, the route with the fewest AS hops is preferred. In the case of a tie, other attributes, such as MED, break the tie. Example 12-1 shows the AS path for network 200.50.32.0/19. To reach the destination, a packet must pass autonomous systems 3561, 7004, and 7418. The command **show ip bgp 200.50.32.0** displays the AS path information.

Example 12-1 *AS Path Attribute*

```
Router#show ip bgp 200.50.32.0
BGP routing table entry for 200.50.32.0/19, version 93313535
Paths: (1 available, best #1)
  Not advertised to any peer
  3561 7004 7418
    206.24.241.181 (metric 490201) from 165.117.1.219 (165.117.1.219)
      Origin IGP, metric 4294967294, localpref 100, valid, internal, best
      Community: 2548:182 2548:337 2548:666 3706:153
```

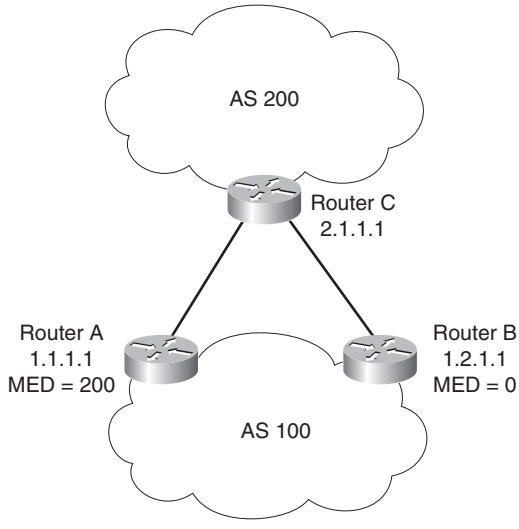
MED Attribute

The MED attribute, also known as a metric, tells external BGP peers the preferred path into the AS when multiple paths into the AS exist. In other words, MED influences which one of many paths a neighboring AS uses to reach destinations within the AS. It is an optional nontransitive attribute carried in eBGP updates. The MED attribute is not used with iBGP peers. The lowest

MED value is preferred, and the default value is 0. Paths received with no MED are assigned a MED of 0. The MED is carried into an AS but does not leave the AS.

Consider the diagram shown in Figure 12-7. With all attributes considered equal, consider that Router C selects Router A as its best path into AS 100 based on Router A's lower router ID (RID). If Router A is configured with a MED of 200, then that will make Router C select Router B as the best path to AS 100. No additional configuration is required on Router B, because the default MED is 0.

Figure 12-7 *MED Attribute*



Community Attribute

Although it is not an attribute used in the routing-decision process, the community attribute groups routes and applies policies or decisions (accept, prefer) to those routes. It is a group of destinations that share some common property. The community attribute is an optional transitive attribute of variable length.

Atomic Aggregate and Aggregator Attributes

The atomic aggregate attribute informs BGP peers that the local router used a less specific (aggregated) route to a destination without using a more specific route.

If a BGP router selects a less specific route when a more specific route is available, it must attach the atomic aggregate attribute when propagating the route. The atomic aggregate attribute lets the BGP peers know that the BGP router used an aggregated route. A more specific route must be in the advertising router's BGP table before it propagates an aggregate route.

When the atomic aggregate attribute is used, the BGP speaker has the option to send the aggregator attribute. The aggregator attribute includes the AS number and the IP address of the router that originated the aggregated route. In Cisco routers, the IP address used is the RID of the router that performs the route aggregation. Atomic aggregate is a well-known discretionary attribute, and aggregator is an optional transitive attribute.

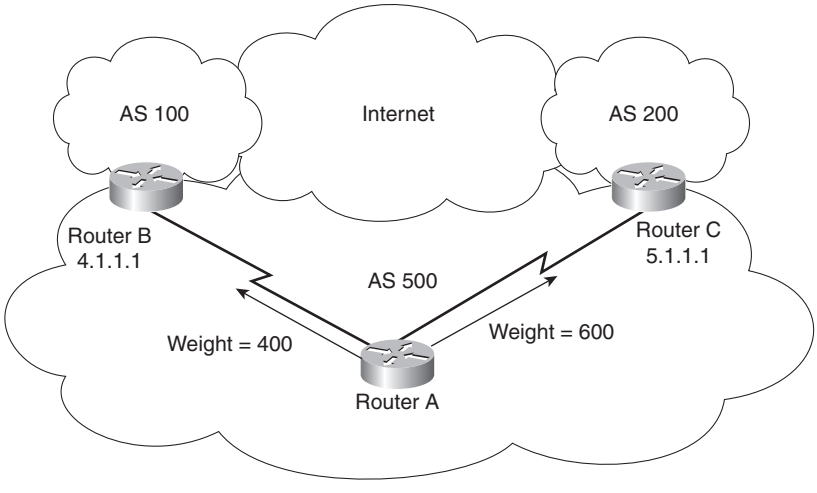
Weight

Weight is assigned locally on a router to specify a preferred path if multiple paths exist out of a router for a destination. Weights can be applied to individual routes or to all routes received from a peer. Weight is specific to Cisco routers and is not propagated to other routers. The weight value ranges from 0 to 65,535. Routes with a higher weight are preferred when multiple routes exist to a destination. Routes that are originated by the local router have a default weight of 32,768.

You can use weight instead of local preference to influence the selected path to external BGP peers. The difference is that weight is configured locally and is not exchanged in BGP updates. On the other hand, the local preference attribute is exchanged between iBGP peers and is configured at the gateway router.

When the same destinations are advertised from both Router B and Router C, as shown in Figure 12-8, Router A prefers the routes from Router C over Router B because the routes received from Router C have a larger weight (600) locally assigned.

Figure 12-8 *BGP Weight*



BGP Decision Process

By default, BGP selects only a single path to reach a specific destination (unless you specify maximum paths). The Cisco implementation of BGP uses a simple decision process. When the path is selected, BGP puts the selected path in its routing table and propagates the path to its neighbors.

To select the best path to a destination, Cisco routers running BGP use the following algorithm in the following order:

1. If the specified next hop is inaccessible, drop the path.
2. If the path is internal, synchronization is enabled, and the path is not in the IGP, drop the path.
3. Prefer the path with the largest weight. (This step is Cisco-specific, and weight is localized to the router.)
4. Prefer the path with the largest local preference. iBGP uses this path only to reach the preferred external BGP router.
5. Prefer the path that was locally originated via a **network** or **aggregate** BGP subcommand or through redistribution from an IGP. Local paths sourced by **network** or **redistribute** commands are preferred over local aggregates sourced by the **aggregate-address** command. (This step is Cisco-specific.)
6. If no route was originated, prefer the route that has the shortest AS path. (This step is Cisco-specific.)
7. If all paths have the same AS path length, prefer the path with the lowest origin type. Paths with an origin type of IGP (lower) are preferred over paths originated from an EGP such as BGP, and EGP origin is preferred over a route with an incomplete origin. (This step is Cisco-specific.)
8. If the origin codes are the same, prefer the path with the lowest MED attribute. An eBGP peer uses this attribute to select a best path to the AS. (This step is a tiebreaker, as described in the RFC that defines the BGP.)
9. If the paths have the same MED, prefer the external (eBGP) path over the internal (iBGP) path. (This step is Cisco-specific.)
10. If the paths are still the same, prefer the path through the closest IGP neighbor (best IGP metric). (This step is a tiebreaker, as described in the RFC that defines the BGP.)
11. Prefer the path with the BGP neighbor with the lowest router ID. (The RFC that defines the BGP describes the router ID.)

After BGP decides on a best path, it marks it with a > sign in the **show ip bgp** table and adds it to the IP routing table.

BGP Summary

The characteristics of BGP follow:

- BGP is an exterior gateway protocol (EGP) used in routing in the Internet. It is an interdomain routing protocol.
- BGP is a path vector routing protocol suited for strategic routing policies.
- It uses TCP port 179 to establish connections with neighbors.
- BGPv4 implements CIDR.
- eBGP is used for external neighbors. It is used between different autonomous systems.
- iBGP is used for internal neighbors. It is used within an AS.
- BGP uses several attributes in the routing-decision algorithm.
- It uses confederations and route reflectors to reduce BGP peering overhead.
- The MED (metric) attribute is used between autonomous systems to influence inbound traffic.
- Weight is used to influence the path of outbound traffic from a single router, configured locally.

Route Manipulation

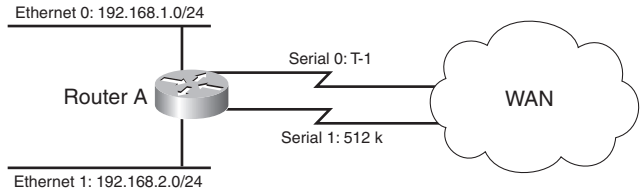
This section covers PBR, route summarization, and route redistribution. You can use PBR to modify the next hop of packets from what is selected by the routing protocol. PBR is useful when the traffic engineering of paths is required. Routes are summarized to reduce the size of routing tables and at network boundaries. Redistribution between routing protocols is required to inject route information from one routing protocol to another. The CCDA must understand the issues with the redistribution of routes.

PBR

You can use PBR to modify the next-hop address of packets or to mark packets to receive differential service. Routing is based on destination addresses; routers look at the routing table to determine the next-hop IP address based on a destination lookup. PBR is commonly used to modify the next-hop IP address based on the source address. You can also use PBR to mark the IP precedence bits in outbound IP packets so that you can apply quality-of-service (QoS) policies. In Figure 12-9, Router A exchanges routing updates with routers in the WAN. The routing protocol might select Serial 0 as the preferred path for all traffic because of the higher bandwidth. The company might have business-critical systems that use the T1 but does not want systems on

Ethernet 1 to affect WAN performance. You can configure PBR on Router A to force traffic from Ethernet 1 out on Serial 1.

Figure 12-9 *Policy-Based Routing*

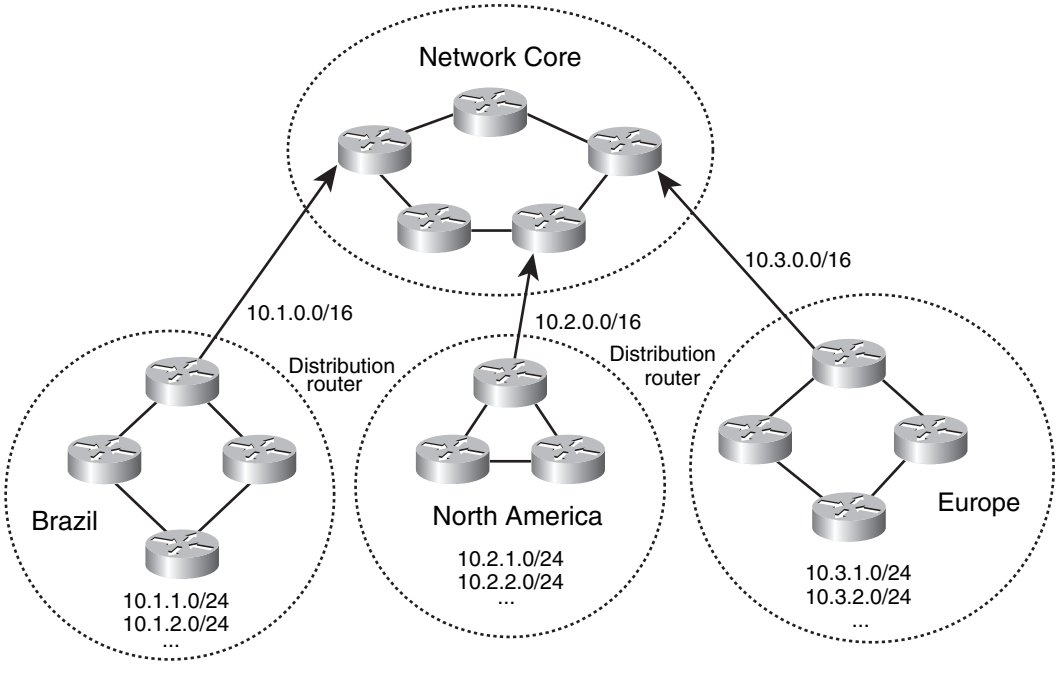


Route Summarization

Large networks can grow very quickly from 500 routes to 1000, to 2000, and so on. Network IP addresses should be allocated to allow for route summarization. Route summarization reduces the amount of route traffic on the network and unnecessary route computation. Route summarization also allows the network to scale as a company grows.

The recommended location for route summarization is to summarize at the distribution layer of the network topology. Figure 12-10 shows a hierarchical network. It has a network core, regional distribution routers, and access routes for sites.

Figure 12-10 *Route Summarization*



All routes in Brazil are summarized with a single 10.1.0.0/16 route. The North America and European routes are also summarized with 10.2.0.0/16 and 10.3.0.0/16, respectively. Routers in Europe only need to know the summarized route to get to Brazil and North America, and vice versa. Again, design best practices are to summarize at the distribution toward the core. The core only needs to know the summarized route of the regional areas.

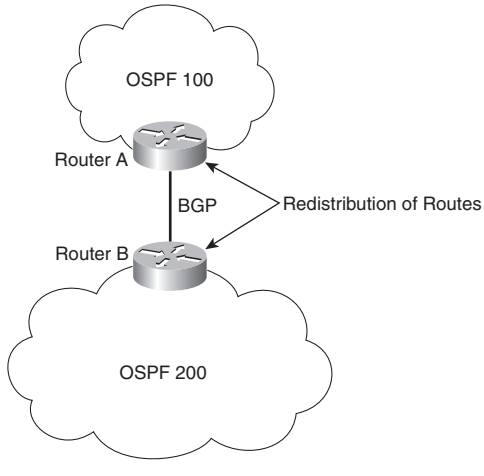
Route Redistribution

You configure the redistribution of routing protocols on routers that reside at the Service Provider Edge of the network. These routers exchange routes with other autonomous systems. Redistribution is also done on routers that run more than one routing protocol. Here are some reasons to do redistribution:

- Migration from an older routing protocol to a new routing protocol.
- Mixed-vendor environment in which Cisco routers might be using EIGRP and other vendor routers might be using OSPF.
- Different administrative domain between company departments using different routing protocols.
- Mergers and acquisitions in which the networks initially need to communicate. In this example two different EIGRP processes might exist.

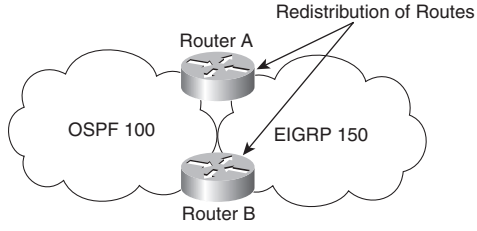
Figure 12-11 shows an example of the exchange of routes between two autonomous systems. Routes from AS 100 are redistributed into BGP on Router A. Routes from AS 200 are redistributed into BGP on Router B. Then, Routers A and B exchange BGP routes. Router A and Router B also implement filters to redistribute only the desired networks.

Figure 12-11 *Redistribution of BGP Routes*



A company might also acquire another company that might be running another routing protocol. Figure 12-12 shows a network that has both OSPF and EIGRP routing protocols. Routers A and B perform redistribution between OSPF and EIGRP. Both routers must filter routes from OSPF before redistributing them into EIGRP and filter routes from EIGRP before redistributing them into OSPF. This setup prevents route feedback.

Figure 12-12 *Redistribution Between IGPs*



Route feedback occurs when a routing protocol learns routes from another routing protocol and then announces the routes to the other routing protocol. In Figure 12-12, OSPF should not announce the routes it learned from EIGRP, and EIGRP should not announce the routes it learned from OSPF.

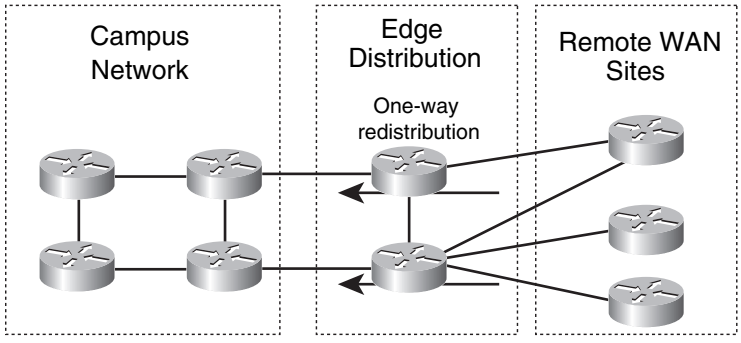
You can use access lists, distribution lists, and route maps when redistributing routes. You can use these methods to specify (select) routes for redistribution, to set metrics, or to set other policies for the routes. They are also used to control routes' redistribution direction. Redistribution can be accomplished by two methods:

- Two-way redistribution
- One-way redistribution

In two-way redistribution, routing information is exchanged between both routing protocols. No static routes are used in this exchange. Route filters are used to prevent routing loops. Routing loops can be caused by one route protocol redistributing routes that were learned from a second route protocol back to that second routing protocol.

One-way redistribution only allows redistribution from one routing protocol to another. Normally it is used in conjunction with a default or static route at the edge of a network. Figure 12-13 shows an example of one-way redistribution. The routing information from the WAN routes is redistributed into the campus. But campus routes are not redistributed out to the WAN. The WAN routers use a default gateway to get back to the campus.

Figure 12-13 *One-Way Route Redistribution*



Other locations for one-way redistribution are from building access networks, BGP routes or static routes into the IGP, and from VPN static routes into the IGP.

Default Metric

There is a default metric of 0 when redistributing routes into RIPv2, IS-IS, and EIGRP. You should configure the metric of the redistributed routes to a metric other than 0. You can configure the metric in the **redistribution** command or configure a default metric. You can also use the command in OSPF. IS-IS does not use the **default-metric** command. The **default-metric** command has the following syntax for EIGRP:

```
default-metric bandwidth delay reliability load mtu
```

OSPF Redistribution

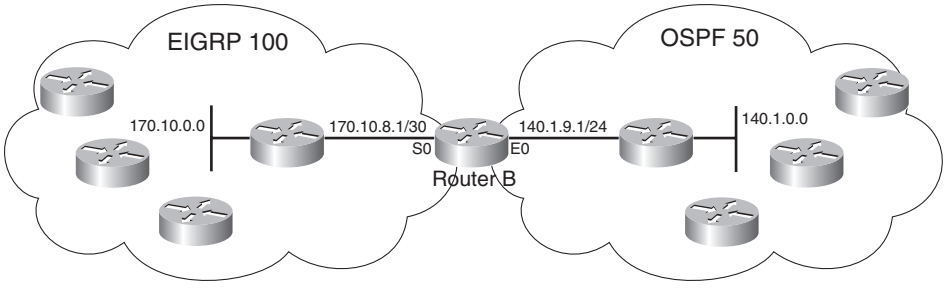
This subsection reviews a few things you need to remember when designing a network that will redistribute with OSPF.

When redistributing routes into OSPF, use the **subnets** keyword to permit subnetted routes to be received. If you do not use it, only the major network route is redistributed, without any subnetworks. In other words, OSPF performs automatic summarization to IP classful network values.

By default, redistributed routes are classified as external Type 2 (E2) in OSPF. You can use the **metric-type** keyword to change the external route to an external Type 1 (E1). The network design can take into account the after-redistribution cost (Type 2) or the after-redistribution cost plus the path's cost (Type 1).

In Figure 12-14, Router B is configured to perform mutual redistribution between EIGRP 100 and OSPF process ID 50. In this example, you can use route maps and access lists to prevent routing loops. The route maps permit or deny the networks that are listed in the access lists. The **subnets** keyword redistributes every subnet in EIGRP into OSPF. This book does not cover exact configurations.

Figure 12-14 *OSPF and EIGRP Redistribution*



IP Multicast Review

With multicast, packets are sent to a multicast group, which is identified with an IP multicast address. Multicast supports the transmission of IP packets from one source to multiple hosts. Packets with unicast addresses are sent to one device, and broadcast addresses are sent to all hosts; packets with multicast addresses are sent to a group of hosts.

Multicast Addresses

Multicast addressing uses Class D addresses from the IPv4 protocol. Class D addresses range from 224.0.0.0 to 239.255.255.255. IANA manages multicast addresses.

Routing protocols (RIPv2, EIGRP, and OSPF) use multicast addresses to speak to their neighbors. For example, OSPF routers use 224.0.0.6 to speak to the designated router (DR) in a multiaccess network. Class D multicast addresses range from 224.0.0.0 to 239.255.255.255. Multicast addresses in the range of 224.0.0.1 to 224.255.255.255 are reserved for special addresses or network protocol on a multiaccess link. RFC 2365 reserves multicast addresses in the range of 239.192.000.000 to 239.251.255.255 for organization-local scope. Similarly, 239.252.000.000 to 239.252.255.255, 239.254.000.000 to 239.254.255.255, and 239.255.000.000 to 239.255.255.255 are reserved for site-local scope.

Table 12-2 lists some well-known and multicast address blocks.

Table 12-2 *Multicast Addresses*

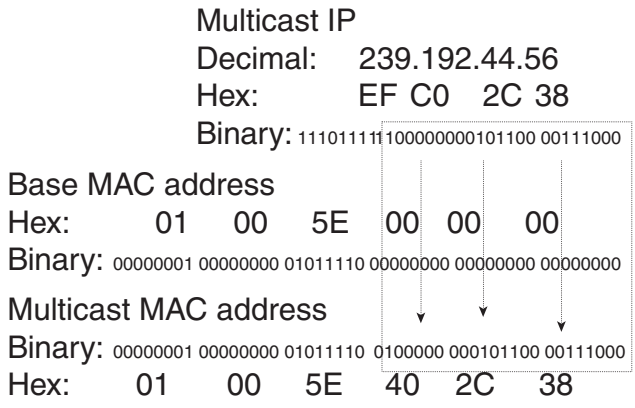
Multicast Address	Description
224.0.0.0/24	Local network control block
224.0.0.1	All hosts or all systems on this subnet
224.0.0.2	All multicast routers
224.0.0.4	Distance-Vector Multicast Routing Protocol (DVMRP) routers
224.0.0.5	All OSPF routers
224.0.0.6	All OSPF DR routers
224.0.0.9	RIPv2 routers
224.0.0.10	EIGRP routers
224.0.0.13	All PIM routers
224.0.1.0/24	Internetwork control block
224.0.1.39	Rendezvous point (RP) announce
224.0.1.40	RP discovery
224.0.2.0 to 224.0.255.0	Ad hoc block
239.000.000.000 to 239.255.255.255	Administratively scoped
239.192.000.000 to 239.251.255.255	Organization-local scope
239.252.000.000 to 239.254.255.255	Site-local scope

Layer 3 to Layer 2 Mapping

Multicast-aware Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) network interface cards use the reserved IEEE 802 address 0100.5e00.0000 for multicast addresses at the MAC layer. This includes Fast Ethernet and Gigabit Ethernet. Notice that for the address, the high-order byte 0x01 has the low-order bit set to 1. This bit is the Individual/Group (I/G) bit. It signifies whether the address is an individual address (0) or a group address (1). Hence, for multicast addresses, this bit is set to 1.

Ethernet interfaces map the lower 23 bits of the IP multicast address to the lower 23 bits of the MAC address 0100.5e00.0000. As an example, the IP multicast address 224.0.0.2 is mapped to the MAC layer as 0100.5e00.0002. Figure 12-15 shows another example looking at the bits of multicast IP 239.192.44.56. The IP address in hexadecimal is EF:C0:2C:38. The lower 23 bits get mapped into the lower 23 bits of the base multicast MAC to produce the multicast MAC address 01:00:5E:40:2C:38.

Figure 12-15 *Mapping of Multicast IP Addressing to MAC Addresses*



IGMP

IGMP is the protocol used in multicast implementations between the end hosts and the local router. RFC 2236 describes IGMP Version 2 (IGMPv2). RFC 3376 describes IGMP Version 3 (IGMPv3). RFC 1112 describes the first version of IGMP.

IP hosts use IGMP to report their multicast group memberships to routers. IGMP messages use IP protocol number 2. IGMP messages are limited to the local interface and are not routed.

IGMPv1

The first RFC describing IGMP (RFC 1112), written in 1989, describes the host extensions for IP multicasting. IGMPv1 provides simple message types for communication between hosts and routers. These messages are

- **Membership query**—Sent by the router to check whether a host wants to join a multicast group
- **Membership report**—Sent by the host to join a multicast group in the segment

The problem with IGMPv1 is the latency involved for a host to leave a group. With IGMPv1, the router sends membership queries periodically; a host must wait for the membership-query message to leave a group. The query interval is 60 seconds, and it takes three query intervals (3 minutes) for a host to leave the group.

IGMPv2

IGMPv2 improves over IGMPv1 by allowing faster termination or leaving of multicast groups.

IGMPv2 has three message types, plus one for backward compatibility:

- **Membership query**—Sent by the router to check whether a host wants to join a group.
- **Version 2 membership report**—A message sent to the group address with the multicast group members (IP addresses). It is sent to by hosts to join and remain in multicast groups on the segment.
- **Version 2 leave group**—Sent by the hosts to indicate that a host will leave a group; it is sent to destination 224.0.0.2. After the host sends the leave group message, the router responds with a group-specific query.
- **Version 1 membership report**—For backward compatibility with IGMPv1 hosts.

You enable IGMP on an interface when you configure a multicast routing protocol, such as PIM. You can configure the interface for IGMPv1, IGMPv2 or IGMPv3.

IGMPv3

IGMPv3 provides the extensions required to support source-specific multicast (SSM). It is designed to be backward-compatible with both prior versions of IGMP.

IGMPv3 has two message types, plus three for backward compatibility:

- **Membership query**—Sent by the router to check that a host wants to join a group.
- **Version 3 membership report**—A message sent to the group address with the multicast group members (IP addresses). It is sent by hosts to request and remain in multicast groups on the segment.
- **Version 2 membership report**—A message sent to the group address with the multicast group members (IP addresses). It is sent by hosts to request and remain in multicast groups on the segment. This message is used for backward compatibility with IGMPv2 hosts.
- **Version 2 leave group**—Sent by the hosts to indicate that a host will leave a group, to destination 224.0.0.2. The message is sent without having to wait for the IGMPv2 membership report message. This message is used for backward compatibility with IGMPv2 hosts.
- **Version 1 membership report**—This message is used for backward compatibility with IGMPv1 hosts.

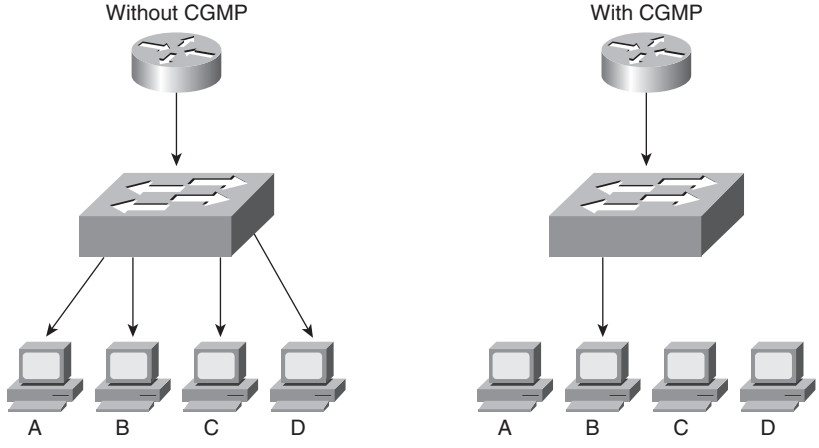
You enable IGMP on an interface when you enable a multicast routing protocol, such as PIM. You can configure the interface for IGMPv1, IGMPv2, or IGMPv3.

CGMP

CGMP is a Cisco-proprietary protocol implemented to control multicast traffic at Layer 2. Because a Layer 2 switch is unaware of Layer 3 IGMP messages, it cannot keep multicast packets from being sent to all ports.

As shown in Figure 12-16, with CGMP the LAN switch can speak with the IGMP router to find out the MAC addresses of the hosts that want to receive the multicast packets. With CGMP, switches distribute multicast sessions only to the switch ports that have group members.

Figure 12-16 *CGMP*



When a router receives an IGMP report, it processes the report and then sends a CGMP message to the switch. The switch can then forward the multicast messages to the port with the host receiving multicast traffic. CGMP fast-leave processing allows the switch to detect IGMP Version 2 leave messages sent by hosts on any of the switch ports. When a host sends the IGMPv2 leave message, the switch can then disable multicasting for the port.

IGMP Snooping

IGMP snooping is another way for switches to control multicast traffic at Layer 2. It listens to IGMP messages between the hosts and routers. If a host sends an IGMP query message to the router, the switch adds the host to the multicast group and permits that port to receive multicast traffic. The port is removed from multicast traffic if the host sends an IGMP leave message to the router. The disadvantage of IGMP snooping is that it has to process every IGMP control message, which can impact the CPU utilization of the switch.

Sparse Versus Dense Multicast Routing Protocols

IP multicast traffic for a particular (source, destination group) multicast pair is transmitted from the source to the receivers using a spanning tree from the source that connects all the hosts in the group. Each destination host registers itself as a member of interesting multicast groups through the use of IGMP. Routers keep track of these groups dynamically and build distribution trees that chart paths from each sender to all receivers. IP multicast routing protocols follow two approaches.

The first approach assumes that the multicast group members are densely distributed throughout the network (many of the subnets contain at least one group member) and that bandwidth is plentiful. The approach with dense multicast routing protocols is to flood the traffic throughout the network and then, at the request of receiving routers, stop the flow of traffic on branches of the network that have no members of the multicast group. Multicast routing protocols that follow this technique of flooding the network include DVMRP, Multicast Open Shortest Path First (MOSPF), and Protocol-Independent Multicast-Dense Mode (PIM-DM).

The second approach to multicast routing assumes that multicast group members are sparsely distributed throughout the network and that bandwidth is not necessarily widely available. Sparse mode does not imply that the group has few members, just that they are widely dispersed. The approach with sparse multicast routing protocols is to not send traffic until it is requested by the receiving routers or hosts. Multicast routing protocols of this type are Core-Based Trees (CBT) and Protocol-Independent Multicast-Sparse Mode (PIM-SM). CBT is not widely deployed and is not discussed in this book.

Multicast Source and Shared Trees

Multicast distribution trees control the path that multicast packets take to the destination hosts. The two types of distribution trees are source and shared. With *source* trees, the tree roots from the source of the multicast group and then expands throughout the network in spanning-tree fashion to the destination hosts. Source trees are also called shortest-path trees (SPT) because they create paths without having to go through a rendezvous point (RP). The drawback is that all routers through the path must use memory resources to maintain a list of all multicast groups. PIM-DM uses a source-based tree.

Shared trees create the distribution tree's root somewhere between the network's source and receivers. The root is called the RP. The tree is created from the RP in spanning-tree fashion with no loops. The advantage of shared trees is that they reduce the memory requirements of routers in the multicast network. The drawback is that initially the multicast packets might not take the best paths to the receivers because they need to pass through the RP. After the data stream begins to flow from sender to RP to receiver, the routers in the path optimize the path automatically to remove any unnecessary hops. The RP function consumes significant memory on the assigned router. PIM-SM uses an RP.

PIM

PIM comes in two flavors: *sparse mode* (PIM-SM) and *dense mode* (PIM-DM). The first uses shared trees and RPs to reach widely dispersed group members with reasonable protocol bandwidth efficiency. The second uses source trees and reverse path forwarding (RPF) to reach relatively close group members with reasonable processor and memory efficiency in the network devices of the distribution trees.

With RPF, received multicast packets are forwarded out all other interfaces, allowing the data stream to reach all segments. If no hosts are members of a multicast group on any of the router's attached or downstream subnets, the router sends a prune message up the distribution tree (the reverse path) to tell the upstream router not to send packets for the multicast group. So, the analogy for PIM-DM is the push method for sending junk mail, and the intermediate router must tell upstream devices to stop sending it.

PIM-SM

PIM-SM is defined in RFC 2362 (experimental). PIM-SM assumes that no hosts want to receive multicast traffic unless specifically requested. In PIM-SM, a router is selected as the RP. The RP gathers the information from senders and makes the information available to receivers. Routers with receivers have to register with the RP. The end-host systems request multicast group membership using IGMP with their local routers. The routers serving the end systems then register as traffic receivers with the RPs for the specified group in the multicast network.

Joining PIM-SM

With PIM-SM, DRs on end segments receive IGMP query messages from hosts wanting to join a multicast group. The router checks whether it is already receiving the group for another interface. If it is receiving the group, the router adds the new interface to the table and sends membership reports periodically on the new interface.

If the multicast group is not in the multicast table, the router adds the interface to the multicast table and sends a join message to the RP with multicast address 224.0.0.13 (all PIM routers) requesting the multicast group.

Pruning PIM-SM

When a PIM-SM does not have any more multicast receiving hosts or receiving routers out any of its interfaces, it sends a prune message to the RP. The prune message includes the group to be pruned or removed.

PIM DR

A designated router is selected in multiaccess segments running PIM. The PIM DR is responsible for sending join, prune, and register messages to the RP. The PIM router with the highest IP address is selected as the DR.

Auto-RP

Another way to configure the RP for the network is to have the RP announce its services to the PIM network. This process is called auto-RP. Candidate RPs send their announcements to RP mapping agents with multicast address 224.0.1.39 (**cisco-rp-announce**). RP mapping agents are also configured. In smaller networks, the RP can be the mapping agent. Configured RP mapping agents listen to the announcements. The RP mapping agent then selects the RP for a group based on the highest IP address of all the candidate RPs. The RP mapping agents then send RP-discovery messages to the rest of the PIM-SM routers in the internetwork with the selected RP-to-group mappings.

PIMv2 Bootstrap Router

Instead of using auto-RP, you can configure a PIMv2 bootstrap router (BSR) to automatically select an RP for the network. The RFC for PIM Version 2, RFC 2362, describes BSR. With BSR, you configure BSR candidates (C-BSR) with priorities from 0 to 255 and a BSR address. C-BSRs exchange bootstrap messages. Bootstrap messages are sent to multicast IP 224.0.0.13 (all PIM routers). If a C-BSR receives a bootstrap message, it compares it with its own. The largest priority C-BSR is selected as the BSR.

After the BSR is selected for the network, it collects a list of candidate RPs. The BSR selects RP-to-group mappings, which is called the RP set, and distributes the selected RPs using bootstrap messages sent to 224.0.0.13 (all PIM routers).

DVMRP

RFC 1075 describes DVMRP. It is the primary multicast routing protocol used in the multicast backbone (MBONE). The MBONE is used in the research community.

DVMRP operates in dense mode using RPF by having routers send a copy of a multicast packet out all paths. Routers that receive the multicast packets then send prune messages back to their upstream neighbor router to stop a data stream if no downstream receivers of the multicast group exist (either receiving routers or hosts on connected segments). DVMRP implements its own unicast routing protocol, similar to RIP, based on hop counts. DVMRP has a 32 hop-count limit. DVMRP does not scale suboptimally. Cisco's support of DVMRP is partial; DVMRP networks are usually implemented on UNIX machines running the **mrouted** process. A DVMRP tunnel is typically used to connect to the MBONE DVMRP network.

IPv6 Multicast Addresses

IPv6 retains the use and function of multicast addresses as a major address class. IPv6 prefix FF00::/8 is allocated for all IPv6 multicast addresses. IPv6 multicast addresses are described in RFC 2373. EIGRP for IPv6, OSPFv3, and RIPng routing protocols use multicast addresses to communicate between router neighbors.

The format of the IPv6 multicast address is described in Chapter 8, "Internet Protocol Version 6." The common multicast addresses are repeated in Table 12-3.

Table 12-3 *Well-Known Multicast Addresses*

Multicast Address	Multicast Group
FF01::1	All nodes (node-local)
FF02::1	All nodes (link-local)
FF01::2	All routers (node-local)
FF02::2	All routers (link-local)
FF02::5	OSPFv3 routers
FF02::6	OSPFv3 designated routers
FF02::9	Routing Information Protocol (RIPng)
FF02::A	EIGRP routers
FF02::B	Mobile agents
FF02::C	DHCP servers/relay agents
FF02::D	All PIM routers

References and Recommended Readings

Border Gateway Protocol. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm.

Chandra, R., P. Traina, and T. Li. RFC 1997, *BGP Communities Attribute*. Available from http://www.ietf.org/rfc.

Deering, S. RFC 1112, *Host Extensions for IP Multicasting*. Available from http://www.ietf.org/rfc.

Doyle, J. and J. Carroll. *Routing TCP/IP,* Volume I, Second Edition. Indianapolis: Cisco Press, 2005.

Doyle, J. and J. Carroll. *Routing TCP/IP,* Volume II. Indianapolis: Cisco Press, 2001.

Estrin, D., D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei. RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification* (experimental). Available from http://www.ietf.org/rfc.

Fenner, W. RFC 2236, *Internet Group Management Protocol, Version 2*. Available from http://www.ietf.org/rfc.

Fuller, V., T. Li, J. Yu, and K. Varadhan. RFC 1519, *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy.* Available from http://www.ietf.org/rfc.

Halabi, S. *Internet Routing Architectures*. Indianapolis: Cisco Press, 2000.

"Internet Protocol (IP) Multicast Technology Overview" (white paper). Available from http://www.cisco.com/en/US/products/ps5763/products_white_paper0900aecd804d5fe6.shtml.

Meyer, D. RFC 2365, *Administratively Scoped IP Multicast*. Available from http://www.ietf.org/rfc.

Rekhter, Y. and T. Li. RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*. Available from http://www.ietf.org/rfc.

Waitzman, D., C. Partride, and S. Deering. RFC 1075, *Distance Vector Multicast Routing Protocol*. Available from http://www.ietf.org/rfc.

Williamson, B. *Developing IP Multicast Networks*. Indianapolis: Cisco Press, 1999.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

This chapter covered the following topics that you need to master for the CCDA exam:

- **BGP**—The characteristics and design of BGP.
- **Route manipulation**—How you use PBR to change the destination address of packets based on policies. This material also covers route summarization and the redistribution of routes between routing protocols.
- **IP multicast protocols**—Multicast protocols such as IGMP, CGMP, and PIM.

The material summarized next can help you review some of these topical areas.

BGP Summary

The characteristics of BGP follow:

- BGP is an exterior gateway protocol (EGP) used in routing in the Internet. It is an interdomain routing protocol.
- BGP is a path vector routing protocol suited for strategic routing policies.
- BGP uses TCP Port 179 to establish connections with neighbors.
- BGPv4 implements CIDR.
- eBGP is for external neighbors. It's used between separate autonomous systems.
- iBGP is for internal neighbors. It's used within an AS.
- BGP uses several attributes in the routing-decision algorithm.
- BGP uses confederations and route reflectors to reduce BGP peering overhead.
- The MED (metric) attribute is used between autonomous systems to influence inbound traffic.
- Weight is used to influence the path of outbound traffic from a single router, configured locally.

Route Redistribution

Route redistribution can occur

- In mixed vendor environments, where Cisco routers might be using EIGRP and other vendor routers using OSPF.
- In migrations from older routing protocol.
- In different administrative domains.
- From static routes and BGP routes into IGP.
- From VPN static routes into IGP.
- Between campus core and WAN routers.
- From selected building access protocols.

IP Multicast

Table 12-4 summarizes IP multicast protocols.

Table 12-4 *IP Multicast Protocols*

Multicast Protocol	Description
IGMP	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to routers.
CGMP	Cisco Group Management Protocol. Used to control multicast traffic at Layer 2.
IGMP snooping	Another method used to control multicast traffic at Layer 2.
PIM	Protocol Independent Multicast. IP multicast routing protocol.
DVMRP	Distance-Vector Multicast Routing Protocol. Primary multicast routing protocol used in the MBONE.

Table 12-5 summarizes IP multicast addresses.

Table 12-5 *IP Multicast Addresses*

Multicast Address	Description
224.0.0.0/24	Local network control block
224.0.0.1	All hosts or all systems on this subnet
224.0.0.2	All routers on this subnet
224.0.0.4	DVMRP routers

Table 12-5 *IP Multicast Addresses (Continued)*

Multicast Address	Description
224.0.0.5	All OSPF routers
224.0.0.6	All OSPF DR routers
224.0.0.9	RIPv2 routers
224.0.0.10	EIGRP routers
224.0.0.13	All PIM routers
224.0.1.0/24	Internetwork control block
224.0.1.39	RP announce
224.0.1.40	RP discovery
224.0.2.0 to 224.0.255.0	Ad hoc block
239.000.000.000 to 239.255.255.255	Administratively scoped
239.192.000.000 to 239.251.255.255	Organization-local scope
239.252.000.000 to 239.254.255.255	Site-local scope

Table 12-6 shows IPv6 multicast addresses.

Table 12-6 *IPv6 Multicast Addresses*

Multicast Address	Multicast Group
FF01::1	All nodes (node-local)
FF02::1	All nodes (link-local)
FF01::2	All routers (node-local)
FF02::2	All routers (link-local)
FF02::5	OSPFv3 routers
FF02::6	OSPFv3 designated routers
FF02::9	Routing Information Protocol (RIPng)
FF02::A	EIGRP routers
FF02::B	Mobile agents
FF02::C	DHCP servers/relay agents
FF02::D	All PIM routers

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: You use iBGP to exchange routes between different autonomous systems.
2. True or false: BGP Version 4 includes support for CIDR.
3. True or false: eBGP and iBGP redistribute automatically on a router if the BGP peers are configured with the same AS number.
4. Use _____ to modify the next hop of packets based on source IP address.
5. eBGP routes have an administrative distance of ____ , and iBGP routes have an administrative distance of ____.
6. True or false: IGMP snooping and CGMP are methods to reduce the multicast traffic at Layer 2.
7. True or false: PIM has a 32 hop-count limit.
8. True or false: PIM-SM routers use the multicast 224.0.0.13 address to request a multicast group to the RP.
9. True or false: AS path is the only attribute BGP uses to determine the best path to the destination.
10. List three IP routing protocols that use multicast addresses to communicate with their neighbors.
11. What IPv6 multicast address does EIGRP use for IPv6?
12. Match the IP multicast address with its description:

    i. 224.0.0.1

    ii. 224.0.0.2

    iii. 224.0.0.5

    iv. 224.0.0.10

    a. All OSPF routers

    b. All routers

    c. EIGRP routers

    d. All hosts

13. Match the BGP attribute with its description:

    i. Local preference

    ii. MED

    iii. AS path

    iv. Next hop

    a. IP address

    b. Indicates the path used to exit the AS

    c. Tells external BGP peers the preferred path into the AS

    d. List of AS numbers

14. Which Cisco feature can you use instead of local preference to influence the selected path to external BGP routers?

15. What is the purpose of route reflectors?

16. When BGP confederations are used, which number do external peers see?

17. With _____ all routers peer with each other within the private AS, and with _____ client routers peer only with the reflector.

18. Which of the following shows the correct order that BGP uses to select a best path?

    a. Origin, lowest IP, AS path, weight, local preference, MED

    b. Weight, local preference, AS path, origin, MED, lowest IP

    c. Lowest IP, AS path, origin, weight, MED, local preference

    d. Weight, origin, local preference, AS path, MED, lowest IP

19. What feature did BGPv4 implement to provide forwarding of packets based on IP prefixes?

20. What route should be used to summarize the following networks?

    10.150.80.0/23, 10.150.82.0/24, 10.150.83.0/24, 10.150.84.0/22

    a. 10.150.80.0/23, 10.150.82.0/23, and 10.150.84.0/22

    b. 10.150.80.0/22 and 10.150.84/22

    c. 10.150.80.0/21

    d. 10.150.80.0/20

21. Match the IPv6 multicast address with its description:

i. FF02::1

ii. FF02::2

iii. FF02::5

iv. FF02::9

v. FF02::A

a. OSPFv3 routers

b. RIPng routers

c. All routers

d. EIGRP routers

e. All nodes

22. Route summarization and redistribution occur in which layer of the hierarchical model?

a. Building access

b. Distribution

c. Core

d. Server access

23. Which of the following best describes route summarization?

a. Grouping contiguous addresses to advertise a large Class A network

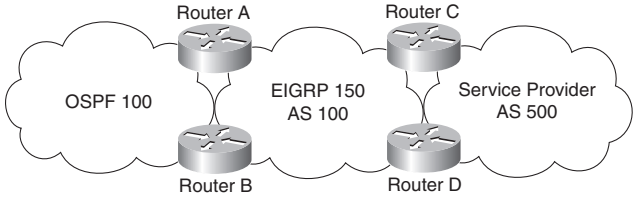
b. Grouping noncontiguous addresses to advertise a larger network

c. Grouping contiguous addresses to advertise a larger network

d. Grouping Internet addresses

Refer to Figure 12-17 to answer the following questions.

Figure 12-17 *Network Scenario*



24. Where should you configure BGP?

    a. Routers A and B

    b. Routers C and D

    c. Answers A and B

    d. Routers A and C

25. On which router should you configure redistribution for OSPF and EIGRP?

    a. Router A only

    b. Router B only

    c. Routers A and B

    d. Redistribution occurs automatically.

26. To announce the networks from AS 100 to AS 500, which routing protocols should you redistribute into BGP?

    a. OSPF only

    b. EIGRP only

    c. OSPF and EIGRP

    d. iBGP

27. Where should you use filters?

    a. Routers A and B

    b. Routers C and D

    c. Routers A and C

    d. Answers A and B

This part covers the following CCDA exam topics (to view the CCDA exam overview, visit http://www.cisco.com/web/learning/le3/current_exams/640-863.html):

- Describe Network Management Protocols and Features
- Describe the Security Lifecycle
- Identify Cisco Technologies to Mitigate Security Vulnerabilities
- Select Appropriate Cisco Security Solutions and Deployment Placement
- Describe Traditional Voice Architectures and Features
- Describe Cisco IP Telephony
- Identify the Design Considerations for Voice Services

Part IV: Security, Convergence, and Network Management

This chapter covers the following subjects:

- Network Security Overview
- Security Threats
- Security Risks
- Security Policy and Process
- Trust and Identity Management
- Secure Connectivity
- Threat Defense

CHAPTER 13

Security Management

This chapter discusses network security in terms of security management and policy. You will be tested on security threats, risks, policy compliance, and securing network connectivity. You must understand how network security management and policy provide a framework for secure networks. This chapter also covers trust and identity management and threat defense.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 13-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 13-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Network Security Overview	1
Security Threats	2, 3
Security Risks	4, 5
Security Policy and Process	6, 7
Trust and Identity Management	8
Secure Connectivity	9
Threat Defense	10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. Which of the following security legislations applies protection to electronic private health information?
   a. SOX
   b. GLBA
   c. HIPAA
   d. EU Data Protection Directive
2. What classification of security threat gathers information about the target host?
   a. Gaining Unauthorized Access
   b. Reconnaissance
   c. Denial of Service
   d. None of the above
3. What type of security threat works to overwhelm network resources such as memory, CPU, and bandwidth?
   a. Denial of Service
   b. Reconnaissance
   c. Gaining Unauthorized Access
   d. NMAP scans
4. What is used to control the rate of bandwidth of incoming traffic?
   a. Unicast RPF
   b. DHCP snooping
   c. Access control lists
   d. Rate limiting
5. What is it called when attackers change sensitive data without proper authorization?
   a. VLAN filtering
   b. ACLs
   c. Integrity violations
   d. Loss of availability

6. What security document focuses on the processes and procedures for managing network events in addition to emergency-type scenarios?
   a. Acceptable-use policy
   b. Incident-handling policy
   c. Network access control policy
   d. Security management policy
7. Which of the following should be included in a security policy? (Choose all that apply.)
   a. Identification of assets
   b. Definition of roles and responsibilities
   c. Description of permitted behaviors
   d. All of the above
8. Authentication of the identity is based on what attributes? (Select all that apply.)
   a. Something the subject knows
   b. Something the subject has
   c. Something the subject is
   d. None of the above
9. What uses two different keys for encryption and relies on Public Key Infrastructure (PKI)?
   a. Asymmetric cryptography
   b. HMAC
   c. IKE
   d. Shared keys
10. Which of the following describe the main areas of focus for the Threat Defense component of Cisco's Self-Defending Network? (Select all that apply.)
   a. Adding full security services for network endpoints
   b. Enhancing the security of the existing network
   c. Enabling integrated security in routers, switches, and appliances
   d. Analyzing the need for transmission integrity

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers security management topics that you need to master for the CCDA exam. It begins by explaining the reasons for network security and some ways to prevent attacks. Next, the chapter describes the types of attacks that can compromise network security and classifications of threats. It goes on to cover the risks inherent in network security, along with a series of risk examples. This chapter provides a framework for network security built around a company's security policy.

In addition, this chapter explores how to control and permit network access at any point within the network. Finally, it looks at enabling security in network equipment and traffic isolation techniques.

Network Security Overview

For many years, networks were designed to be fairly open in nature and did not require much security. The greatest area of concern was physical access. Over time, networks grew in size, and complexity increased the need for network security. For today's businesses, security is now a mandatory part of designing IT systems, because the risks are too high if critical data is lost or tampered with. Security teams within organizations must now provide adequate levels of protection for the business to conduct its operations.

Network security is used to defend against network attacks and prevent unauthorized access from intruders. In addition, network security protects data from manipulation and theft. Businesses today also need to comply with company policy and security legislation that is in place to help protect data and keep it private.

Network security needs to be transparent to the end users and should also be designed to prevent attacks by

- Blocking external attackers from accessing the network
- Permitting access to only authorized users
- Preventing attacks from sourcing internally
- Supporting different levels of user access
- Safeguarding data from tampering or misuse

Security Legislation

A number of legislative bodies along with the public have insisted that security controls be in place to protect private information and make certain that it is handled properly. These legislative bodies influence network security by imposing mandates with which organizations are required to comply. These requirements may include protecting customer information with regards to privacy and, in some cases, requiring encryption of the data in question.

The U.S. has a growing body of security legislation that you need to be aware of:

- **U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley or SOX)**—Focuses on the accuracy and controls imposed on a company's financial records.
- **Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)**—Provides protection against the sale of bank and account information that is regularly bought and sold by financial institutions. GLBA also guards against the practice of obtaining private information through false pretenses.
- **U.S. Health Insurance Portability and Accountability Act (HIPAA)**—Applies to the protection of private health information that is used electronically. The purpose is to enable better access to health information, reduce fraud, and lower the cost of health care in the U.S.
- **EU Data Protection Directive 95/46/EC**—Calls for the protection of people's privacy with respect to the processing of personal data.

Security Threats

It is important to be aware of the different types of attacks that can impact system security. Security threats can be classified into three broad categories:

- **Reconnaissance**—The goal of reconnaissance is to gather as much information as possible about the target host and/or network. Generally this type of information-gathering is done before an attack is carried out.
- **Gaining unauthorized access**—This is the act of attacking or exploiting the target system or host. Operating systems, services, and physical access to the target host have known system vulnerabilities that the attacker can take advantage of and use to increase his or her privileges. Social engineering is another technique for obtaining confidential information from employees by manipulation. As a result of the attacker exploiting the host, confidential information can be read, changed, or deleted from the system.
- **Denial of service (DoS)**—DoS attacks aim to overwhelm resources such as memory, CPU, and bandwidth, thus impacting the target system and denying legitimate users access. Distributed DoS attacks involve multiple sources working together to deliver the attack.

Reconnaissance and Port Scanning

Reconnaissance network tools are used to gather information from the hosts attached to the network. They have many capabilities, including identifying the active hosts and what services the hosts are running. In addition, these tools can find trust relationships, determine OS platforms, and identify user and file permissions.

Some of the techniques that these scanning tools use are TCP connects, TCP SYNs, ACK sweeps, ICMP sweeps, SYN sweeps, and null scans. Here are some of the popular port-scanning tools and their uses:

- **NMAP** (Network Mapper) is designed to scan large networks or even a single host. It is an open-source utility used for network exploration and/or security audits.
- **Superscan** provides high-speed scanning, host detection, Windows host enumeration, and banner grabbing. Superscan is made for Windows clients.
- **NetStumbler** identifies wireless networks using 802.11a/b/g WLAN standards with or without SSID being broadcast. It runs on Windows platforms, including Windows Mobile.
- **Kismet** is an 802.11 wireless sniffer and IDS application that can collect traffic from 802.11a/b/g networks. It collects packets and detects wireless networks—even some that are hidden.

Vulnerability Scanners

Vulnerability scanners determine what potential exposures are present in the network. Passive scanning tools are used to analyze the traffic flowing on the network. Active testing injects sample traffic onto the network. General vulnerability information is published at the following links:

- **CERT CC**—http://www.cert.org
- **MITRE**—http://www.cve.mitre.org
- **Microsoft**—http://www.microsoft.com/technet/security/bulletin/summary.mspx
- **Cisco Security Notices**—http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Here are some tools used for vulnerability scanning:

- **Nessus** is designed to automate the testing and discovery of known vulnerabilities. Nessus is an open-source tool that requires Linux/UNIX or Windows to run.
- **SAINT** (Security Administrator's Integrated Network Tool) is a vulnerability assessment application that runs on UNIX hosts.

- **MBSA** (Microsoft Baseline Security Analyzer) is used to scan systems and identify if patches are missing for Windows products such as operating systems, IIS, SQL, Exchange Server, Internet Explorer, Media Player, and Microsoft Office applications. MBSA also alerts you if it finds any known security vulnerabilities such as weak or missing passwords and other common security issues.

Unauthorized Access

Another threat that you need to be concerned with is attackers gaining access. Hackers use several techniques to gain system access. One approach is when unauthorized people use usernames and passwords to escalate the account's privilege levels. Furthermore, some system user accounts have default administrative username and password pairings that are common knowledge, which makes them very insecure. Trust relationships between systems and applications are another way unauthorized access takes place.

Unauthorized access is also obtained through the use of social engineering—the practice of acquiring confidential information by manipulating legitimate users. Actually, most confidential information such as badges, usernames, and passwords can be uncovered just by walking around an organization. The psychology method is another way of getting confidential information. For example, someone pretending to be from the IT department calls a user and asks for her account information to maintain or correct an account discrepancy.

In addition to these approaches, hackers can obtain account information by using password-cracking utilities or by capturing network traffic.

Security Risks

To protect network resources, processes, and procedures; technology needs to address security risks. Important network characteristics that can be at risk from security threats include data confidentiality, data integrity, and system availability:

- System availability should ensure uninterrupted access to critical network and computing resources to prevent business disruption and loss of productivity.
- Data integrity should ensure that only authorized users can change critical information and guarantee the authenticity of data.
- Data confidentiality should ensure that only legitimate users can view sensitive information to prevent theft, legal liabilities, and damage to the organization.

In addition, the use of redundant hardware and encryption can significantly reduce the risks associated with system availability, data integrity, and data confidentiality.

Targets

Given the wide range of potential threats, just about everything in the network has become vulnerable and is a potential target. Ordinary hosts top the list as the favorite target, especially for worms and viruses. After a host has been compromised, it is frequently used to start new attacks with other nearby systems.

Other high-value targets include devices that support the network. Here is a list of some devices, servers, and security devices that stand out as potential targets:

- **Infrastructure devices**—Routers, switches
- **Security devices**—Firewalls, IDS/IPS
- **Network services**—DHCP and DNS servers
- **Endpoints**—Management stations and IP phones
- **Infrastructure**—Network throughput and capacity

Loss of Availability

Denial-of-service (DoS) attacks try to block or deny access to impact the availability of network services. These types of attacks can interrupt business transactions, cause considerable loss, or damage the company's reputation. DoS attacks are fairly straightforward to carry out, even by an unskilled attacker. Distributed DoS (DDoS) attacks are initiated by multiple source locations within the network to increase the attack's size and impact.

DDoS attacks occur when the attacker takes advantage of vulnerabilities in the network and/or host. Here are some common failure points:

- A network, host, or application fails to process large amounts of data sent to it, which crashes or breaks communication ability.
- A host or application is unable to handle an unexpected condition, such as improperly formatted data and memory or resource depletion.

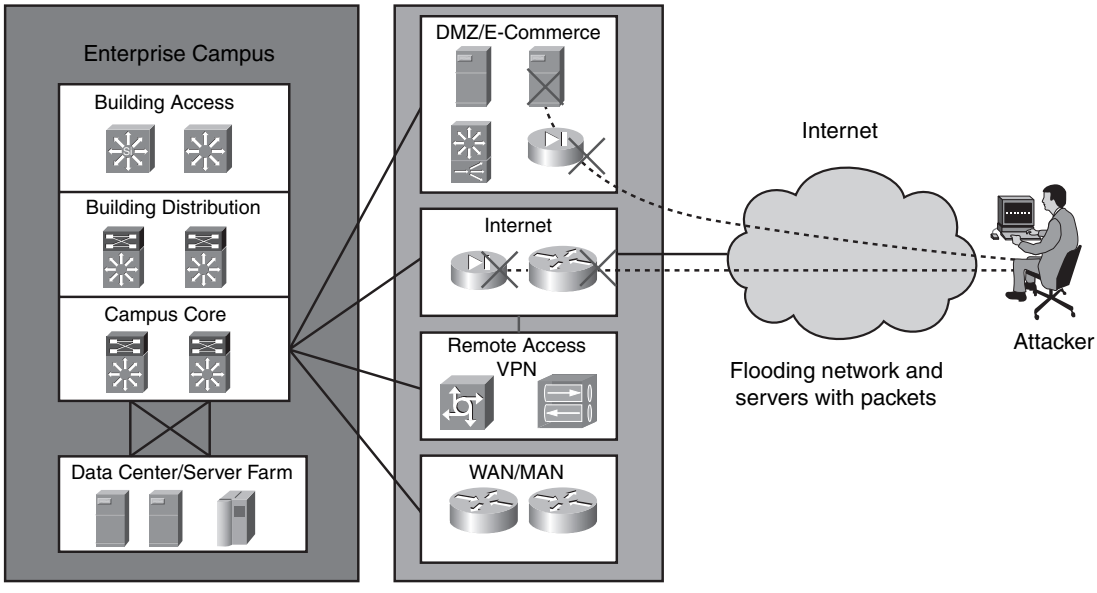
Nearly all DoS attacks are carried out with spoofing and flooding methods. Here are some ways to combat DoS attacks:

- **DHCP snooping** verifies DHCP transactions and prevents rogue DHCP servers from interfering with production traffic.
- **Dynamic ARP inspection** intercepts ARP packets and verifies that they have valid IP-to-MAC bindings.

- **Unicast RPF** prevents unknown source addresses from using the network as a transport mechanism to carry out attacks.
- **Access control lists (ACLs)** control what traffic is allowed on the network.
- **Rate limiting** controls the rate of bandwidth that incoming traffic is using, such as ARPs and DHCP requests.

Figure 13-1 shows a DoS threat on availability. The attacker is performing a DoS attack on the network and servers using a flood of packets. Keep in mind that this is an external attack; however, an internal attack is also certainly possible.

Figure 13-1 *DoS Threat*



Integrity Violations and Confidentiality Breaches

When attackers change sensitive data without the proper authorization, this is called an integrity violation. For example, an attacker might access financial data and delete critical information. The effect of this change may not be felt for some time or until a significant loss has occurred. Integrity attacks like this are considered by many companies to be one of the most serious threats to their business. Furthermore, identifying these attacks can be very difficult, and the effects can be devastating.

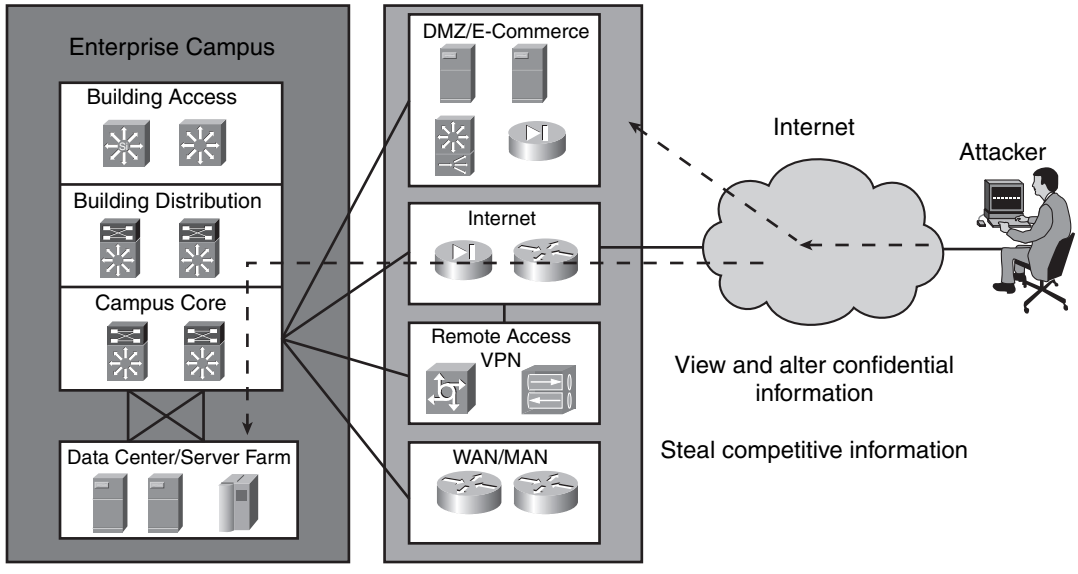
Confidentiality breaches occur when the attacker attempts to read sensitive information. It is difficult to detect these types of attacks, and the loss of data can happen without the owner's knowledge.

It is important to use restrictive access controls to prevent integrity violations and confidentiality attacks. Here are some ways to enforce access control in order to reduce risks:

- Restrict access by separating networks (VLANs) and using packet-filtering firewalls.
- Restrict access with OS-based controls in both Windows and UNIX.
- Limit user access by using user profiles for different departmental roles.
- Use encryption techniques to secure data or digitally sign data.

Figure 13-2 shows an attacker viewing, altering, and stealing competitive information. Pay particular attention to the obstacles the attacker must go through to get to the data.

Figure 13-2 *Confidentiality and Integrity Threats*



Security Policy and Process

To provide the proper levels of security and increase network availability, a security policy is a crucial element in providing secure network services. In addition, it is important to understand that network security is built around a security policy that is part of a system life cycle.

In terms of network security in the system life cycle, business needs are a key area to consider. Business needs define what the business wants to do with the network.

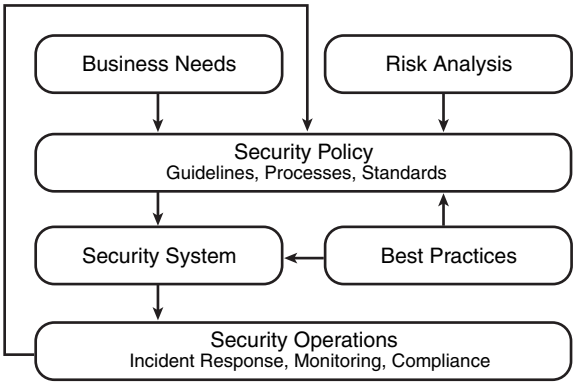
Risk assessment is another part of the system life cycle. It explains the risks and their costs. Business needs and risk assessment feed information into the security policy.

The security policy describes the organization's processes, procedures, guidelines, and standards. Furthermore, industry and security best practices are leveraged to provide well-known processes and procedures.

Finally, an organization's security operations team needs to have processes and procedures defined. This information helps explain what needs to happen for incident response, security monitoring, system maintenance, and managing compliance.

Figure 13-3 shows the flow of the network security life cycle.

Figure 13-3 *Network Security: System Life Cycle*



Security Policy Defined

RFC 2196 says, "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." When developing security policies for an organization, RFC 2196 can serve as a guide for developing security processes and procedures. This RFC lists issues and factors that an organization must consider when setting its policies. Organizations need to make many decisions and come to agreement when creating their security policy.

Basic Approach of a Security Policy

To help create a security policy, here is a generally accepted approach from RFC 2196:

Step 1 Identify what you are trying to protect.

Step 2 Determine what you are trying to protect it from.

Step 3 Determine how likely the threats are.

Step 4 Implement measures that protect your assets in a cost-effective manner.

Step 5 Review the process continuously, and make improvements each time a weakness is found.

Purpose of Security Policies

One of the main purposes of a security policy is to describe the roles and requirements for securing technology and information assets. The policy defines the ways in which these requirements will be met.

There are two main reasons for having a security policy:

- It provides the framework for the security implementation:
  - Identifies assets and how to use them
  - Defines and communicates roles and responsibilities
  - Describes tools and procedures
  - Clarifies incident handling of security events
- It creates a security baseline of the current security posture:
  - Describes permitted and nonpermitted behaviors
  - Defines consequences of asset misuse
  - Provides cost and risk analysis

Here are some questions you may need to ask when developing a security policy:

- What data and assets will be included in the policy?
- What network communication is permitted between hosts?
- How will policies be implemented?
- What happens if the policies are violated?
- How will the latest attacks impact your network and security systems?

Security Policy Components

A security policy is divided into smaller parts that help describe the overall risk management policy, identification of assets, and where security should be applied. Other components of the security policy explain how responsibilities related to risk management are handled throughout the enterprise.

Further documents concentrate on specific areas of risk management:

- **Acceptable-use policy** is a general end-user document that is written in simple language. This document defines the roles and responsibilities within risk management and should have clear explanations to avoid confusion.
- **Network access control policy** defines general access-control principles used and how data is classified, such as confidential, top-secret, or internal.
- **Security management policy** explains how to manage the security infrastructure.
- **Incident-handling policy** defines the processes and procedures for managing incidents and even emergency-type scenarios.

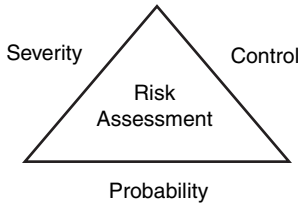
Several other documents supplement these; they vary depending on the organization. The security policy requires the acceptance and support of all employees to make it successful. All the key stakeholders, including members of senior management, should have input into the development of the security policy. In addition, they should continue to participate in the updates to the security policy.

Risk Assessment

Within network security, proper risk management is a technique used to lower risks to within acceptable levels. A well-thought-out plan for network security design implements the components included in the security policy. The security policies that an organization employs use risk assessments and cost-benefit analysis to reduce security risks.

Figure 13-4 shows the three major components of risk assessment. Control refers to how you use the security policy to minimize potential risks. Severity describes the level of the risk to the organization, and probability is the likeliness that an attack against the assets will occur.

Figure 13-4 *Risk Assessment Components*



Risk assessments should explain the following:

- What assets to secure
- The monetary value of the assets
- The actual loss that would result from an attack

- The severity and the probability that an attack against the assets will occur
- How to use security policy to control or minimize the risks

Security costs can be justified by describing the loss of productivity during security incidents.

Generally, network systems are built with just enough security to reduce potential losses to a reasonable level. However, some organizations have higher security requirements, such as complying with SOX or HIPAA regulations, so they need to employ stronger security mechanisms.

A risk index is used to consider the risks of potential threats. The risk index is based on risk assessment components (factors):

- Severity of loss if the asset is compromised
- Probability of the risk actually occurring
- Ability to control and manage the risk

One approach to determining a risk index is to give each risk factor a value from 1 (lowest) to 3 (highest). For example, a high-severity risk would have a substantial impact on the user base and/or the entire organization. Medium-severity risks would have an effect on a single department or site. Low-severity risks would have limited impact and would be relatively straightforward to mitigate.

The risk index is calculated by multiplying the severity and probability factors and then dividing that by the control factor:

risk index = (severity factor * probability factor) / control factor

Table 13-2 shows a sample risk index calculation for a typical large corporation facing a couple of typical risks. If the risk index number calculated is high, there is more risk and thus more impact to the organization. The lower the index number calculated means that there is less risk and less impact to the organization.

Table 13-2 *Risk Index Calculation*

Risk	Severity (S) Range 1 to 3	Probability (P) Range 1 to 3	Control Range 1 to 3	Risk Index (S * P)/ C Range .3 to 9
DoS attack lasting for 1.5 hours on the e-mail server	2	2	1	4
Breach of confidential customer lists	3	1	2	1.5

Continuous Security

As requirements change and new technology is developed, the network security policy should be updated to reflect the changes. Four steps are used to facilitate continuing efforts in maintaining security policies:

Step 1 **Secure**—Identification, authentication, ACLs, stateful packet inspection (SPI), encryption, and VPNs

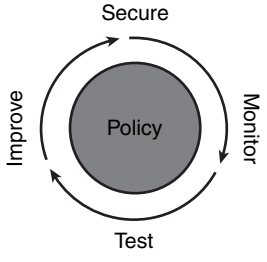
Step 2 **Monitor**—Intrusion and content-based detection and response

Step 3 **Test**—Assessments, vulnerability scanning, and security auditing

Step 4 **Improve**—Security data analysis, reporting, and intelligent network security

Figure 13-5 shows the four-step process that updates and continues the development of security policies.

Figure 13-5 *Continuous Security*



Integrating Security Mechanisms into Network Design

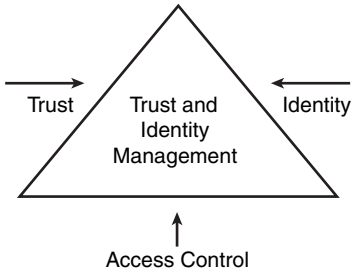
Today's network designs demonstrate an increased use of security mechanisms and have become more tightly integrated with network design. Many security services such as IDS/IPS, firewalls, and IPsec VPN concentrators now reside within the internal network infrastructure. It is recommended that you incorporate network security during the network design planning process. This requires close coordination between the various engineering and operation teams.

Trust and Identity Management

Trust and Identity Management is part of the Cisco Self-Defending Network, which is crucial for the development of a secure network system. It defines who and what can access the network, as well as when, where, and how that access can occur. Access to the business applications and network equipment is based on the user level rights granted to users. Trust and Identity Management also attempts to isolate and keep infected machines off the network by enforcing

access control. The three main components of Trust and Identity Management are trust, identity, and access control, as shown in Figure 13-6. The following sections cover these components in detail.

Figure 13-6 *Trust and Identity Management*



Trust

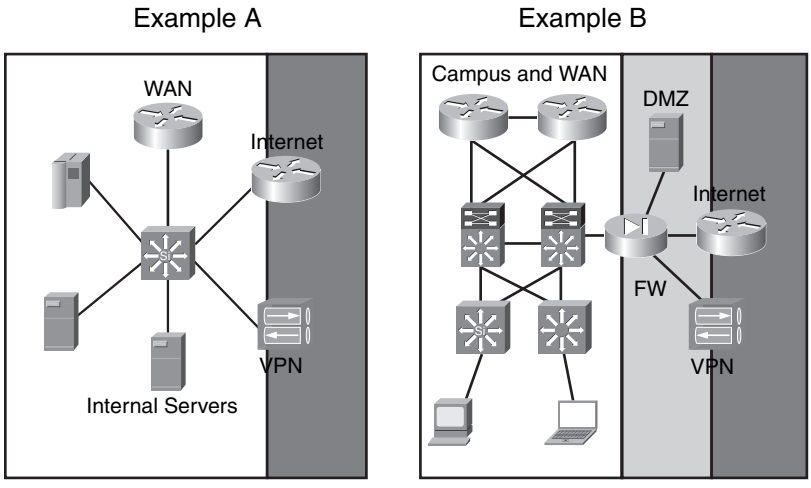
Trust is the relationship between two or more network entities that are permitted to communicate. Security policy decisions are largely based on this premise of trust. If you are trusted, you are allowed to communicate as needed. However, at times security controls need to apply restraint to trust relationships by limiting access to the designated privilege level. Trust relationships can be explicit or implied by the organization. Some trust relationships can be inherited or passed down from one system to another. However, keep in mind that these trust relationships can also be abused.

Domains of Trust

Domains of Trust are a way to group network systems that share a common policy or function. Network segments have different trust levels, depending on the resources they are securing. When applying security controls within network segments, it is important to consider the trust relationships between the segments. Keep in mind that customers, partners, and employees each have their unique sets of requirements from a security perspective that can be managed independently with Domains of Trust classifications. When Domains of Trust are managed in this way, consistent security controls within each segment can be applied.

Figure 13-7 shows two examples of Trust Domains with varying levels of trust segmented. The lighter shading indicates internal higher security and more secure networks and the darker areas represent less secure areas and lower security.

Figure 13-7 *Domains of Trust*



Trust levels such as the internal network can be very open and flexible, whereas the outside needs to be considered unsafe and thus needs strong security to protect the resources. Table 13-3 shows different levels of trust, going from low to high.

Table 13-3 *Domains of Trust: Risks from Low to High*

Domain	Level	Safeguards Required
Production to lab	Low risk	ACLs and network monitoring
Headquarters to branch (IPsec VPN)	Medium risk	Authentication, confidentiality, integrity concerns, ACLs, route filtering
Inside (private) to outside (public)	High risk	Stateful packet inspection, intrusion protection (IPS), security monitoring

Identity

Identity is the "who" of a trust relationship. This can be users, devices, organizations, or all of these. Network entities are validated by credentials. Authentication of the identity is based on the following attributes:

- **Something the subject knows**—Knowledge of a secret, password, PIN, or private key
- **Something the subject has**—Possession of an item such as a token card, smartcard, or hardware key
- **Something the subject is**—Human characteristics such as a fingerprint, retina scan, or voice recognition

Generally, identity credentials are checked by requiring passwords, tokens, or certificates.

Passwords

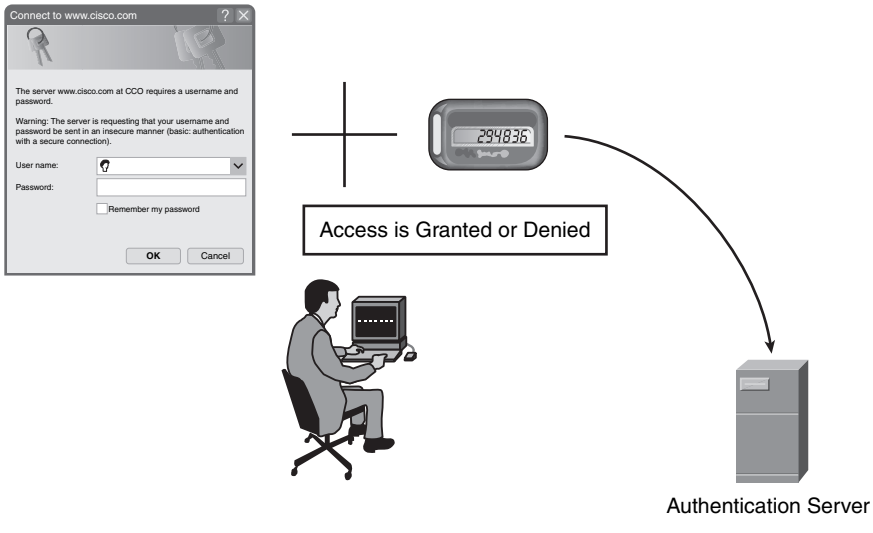
Passwords are used to give users access and allow them to access network resources. Passwords are an example of the authentication attribute called "something you know." Typically, users do not want to use strong passwords; they want to do what is easiest for them. This presents a problem with security and requires you to enforce a password policy. Passwords should not be common dictionary words and should be time-limited. Passwords should never be shared or posted on a computer monitor.

Tokens

Tokens represent a way to increase security by requiring "two-factor authentication." This type of authentication is based on "something you know" and "something you have." For example, one factor may be a six-digit PIN, and another would be the seven-digit code on the physical token. The code on the tokens changes frequently and is not useful without the PIN. The code plus the PIN is transmitted to the authentication server for authorization. Then the server permits or denies access based on the user's predetermined access level.

Figure 13-8 shows two-factor authentication using a username and password along with a token access code.

Figure 13-8 *Using Tokens*



Certificates

Certificates are used to digitally prove your identity or right to access information or services. Certificates, also known as digital certificates, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A digital certificate is signed and issued by a certification authority (CA) with the CA's private key. A digital certificate contains the following:

- Owner's public key
- Owner's name
- Expiration date of the public key
- Name of the certificate authority
- Serial number
- Digital signature of the CA

Certificates can be read or written by an application conforming to the X.509 CCITT international standard.

Access Control

Access control is a security mechanism for controlling admission to networks and resources. These controls enforce the security policy and employ rules about which resources can be accessed. Access control ensures the confidentiality and integrity of the network resources.

The core of network access control consists of the following:

- **Authentication** establishes the user's identity and access to the network resources.
- **Authorization** describes what can be done and what can be accessed.
- **Accounting** provides an audit trail of activities by logging the actions of the user.

Authentication, authorization, and accounting are the network security services supported by AAA that help manage the network access control on your network equipment.

Secure Connectivity

Secure connectivity is a component of the Cisco Self-Defending Network. This component aims to protect the integrity and privacy of organizations' sensitive information. With increased security risks on the rise, it is critical that security be implemented within today's network environments. Internal network segments have traditionally been considered trusted. However, internal threats are now more than ten times more expensive and destructive than external threats. Data that flows

across the network needs to be secured so that its privacy and integrity are preserved. These are important concepts to keep in mind when making business decisions about securing connectivity.

The Cisco Secure Connectivity System provides secure transport for data and applications using encryption and authentication techniques. Many security technologies exist for securing data, voice, and video traffic using wired or wireless networks.

Security technologies include

- IP Security (IPsec)
- Secure Shell (SSH)
- Secure Socket Layer (SSL)
- Multiprotocol Label Switching (MPLS) VPNs
- MPLS VPNs with IPsec

Encryption Fundamentals

Cryptography uses encryption to keep data private, thus protecting its confidentiality. The encapsulated data is encrypted with a secret key that secures the data for transport. When the data reaches the other side of the connection, another secret key is used to decrypt the data and reveal the message transmitted. The encryption and decryption can be used only by authorized users. Most encryption algorithms require the user to have knowledge of the secret keys. IPsec is an example of a security protocol framework that uses encryption algorithms to hide the IP packet payload during transmission.

Encryption Keys

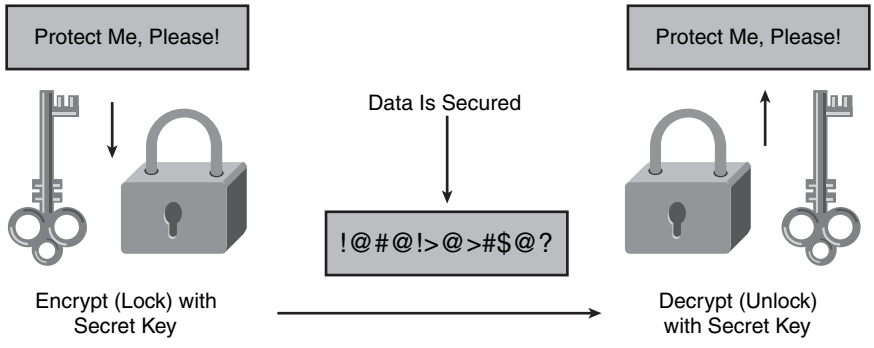
An encryption session between two endpoints needs a key to encrypt the traffic and a key to decrypt the traffic at the remote endpoint. There are two ways to send a key to the remote endpoint—shared secrets and Public-Key Infrastructure (PKI):

- Shared secrets
  - Both sides can use the same key or use a transform to create the decryption key.
  - The key is placed on the remote endpoint out of band.
  - This is a simple mechanism, but it has security issues because the key does not change frequently enough.

- PKI
  - It relies on asymmetric cryptography, which uses two different keys for encryption.
  - Public keys are used to encrypt and private keys to decrypt.
  - PKI is used by many e-commerce sites on the Internet.

Figure 13-9 shows what occurs during the encryption process using secret keys.

Figure 13-9 *Encryption Keys*



VPN Protocols

The two most common VPN protocols are IPsec and SSL:

- IPsec
  - Uses AH and ESP to secure data
  - Uses Internet Key Exchange (IKE) for dynamic key exchange
  - Endpoints need IPsec software
- SSL
  - Uses TCP port 443 (HTTPS)
  - Provides encrypted VPN connectivity using a web browser
  - All major browsers support SSL VPN

IPsec comes in two forms—IP encapsulating security payload (ESP) and IP authentication header (AH)—which use protocol numbers 50 and 51, respectively. ESP is defined in RFC 2406, and AH is defined in RFC 2402. ESP provides confidentiality, data origin authentication, integrity, and anti-replay service. AH allows for connectionless integrity, origin authentication, and anti-replay

protection. These protocols can be used together or independently. Most IPsec clients or routers use IKE to exchange keys and ESP to encrypt the traffic.

SSL VPNs have become increasingly popular because of their clientless nature. A major advantage of SSL VPNs is that you do not need client software—only a web browser that can be accessed wherever an Internet connection exists.

Transmission Confidentiality

To ensure that data is kept private over insecure networks such as the Internet, transmission confidentiality is used. Because the Internet is a public network, ordinary access control mechanisms are unavailable. Therefore, you need to encrypt the data before transporting over any untrusted network such as the Internet.

To provide transmission confidentiality, IPsec VPNs that support encryption can create a secure tunnel between the source and destination. As packets leave one site, they are encrypted; when they reach the remote site, they are decrypted. Eavesdropping in the Internet can occur, but with IPsec encrypted packets, it is much more difficult.

IPsec VPNs commonly use well-known algorithms to perform the confidentiality treatment for packets. The well-known cryptographic algorithms include Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and Rivest Cipher 4 (RC4). These algorithms are thoroughly tested and checked and are considered trusted. However, keep in mind that cryptography can pose some performance problems, depending on the network's state. That is why it is important to carefully analyze the network before deploying VPNs with IPsec.

Data Integrity

Cryptographic protocols protect data from tampering by employing secure fingerprints and digital signatures that can detect changes in data integrity.

Secure fingerprints function by appending a checksum to data that is generated and verified with the secret key. The secret key is known only to those who are authorized. An example of secure fingerprints is Hash-based Message Authentication Code (HMAC), which maintains packet integrity and the authenticity of the data protected.

Digital signatures use a related cryptography method that digitally signs the packet data. A signer creates the signature using a key that is unique and known only to the original signer. Recipients of the message can check the signature by using the signature verification key. The cryptography inherent in digital signatures guarantees accuracy and authenticity because the originator signed it. Financial businesses rely on digital signatures to electronically sign documents and also to prove that the transactions did in fact occur.

Here are some data integrity guidelines to keep in mind:

- Analyze the need for transmission integrity.
- Factor in performance, but use the strongest cryptography.
- Always use well-known cryptographic algorithms.

Threat Defense

As part of the Cisco Self-Defending Network, Threat Defense enhances the security in the network infrastructure by adding increased levels of security protection on network devices, appliances, and endpoints. Both internal and external threats have become much more destructive than in the past. DoS attacks, man-in-the-middle attacks, and Trojan horses have the potential to severely impact business operations. The Cisco Threat Defense system provides a strong defense against these internal and external threats.

Threat Defense has three main areas of focus:

- **Enhancing the security of the existing network**—Preventing loss of downtime, revenue, and reputation
- **Adding full security services for network endpoints**—Securing servers and desktops with Cisco Security Agent
- **Enabling integrated security in routers, switches, and appliances**—Security techniques enabled throughout the network, not just in point products or locations

Physical Security

During your security implementations, it is essential to incorporate physical security to increase the strength of the overall security design. Physical security helps protect and restrict access to network resources and physical network equipment. Sound security policies must defend against potential attacks that can cause loss of uptime or reputation, or even revenue impacts.

Here are some considerations for potential physical threats:

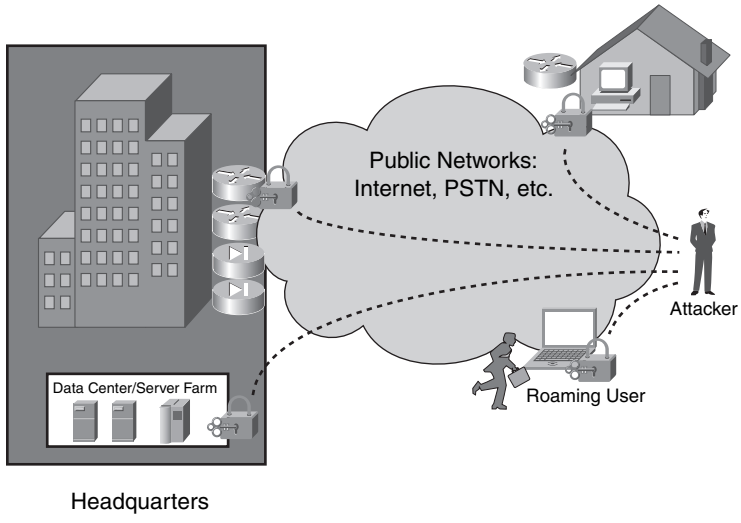
- Vulnerabilities inherent in systems when attackers access the hardware directly through console access or untrusted software.
- Access to the network, allowing attackers to capture, alter, or remove data flowing in the network.
- Attackers may use their own hardware, such as a laptop or router, to inject malicious traffic onto the network.

Here are some physical security guidelines to keep in mind when designing physical security architectures:

- Use physical access controls such as locks or alarms.
- Evaluate potential security breaches.
- Assess the impact of stolen network resources and equipment.
- Use controls such as cryptography to secure traffic flowing on networks outside your control.

Figure 13-10 shows some physical security threat locations that an attacker could potentially exploit.

Figure 13-10 *Physical Security Threats*



Infrastructure Protection

The infrastructure needs to be protected using security features and services to meet the growing needs of business without disruption. Infrastructure protection is the process of taking steps to reduce the risks and threats to the network infrastructure and to maintain the integrity and high availability of network resources.

By using best practices and a security policy, you can secure and harden the infrastructure equipment to prevent potential attacks. To combat network threats, Cisco has enhanced Cisco IOS with security features to support the secure infrastructure and increase the network's availability.

Here are some solutions for equipment that has built-in integrated security features:

- **Adaptive Security Appliance (ASA)** integrates essential security technologies in one platform (firewall, IPS, IPsec VPN, and SSL VPN).
- **Routers** consolidates IOS firewall, IPS, IPsec VPN, DMVPN, and SSL VPN into the routing platforms to secure the router if attacked.
- **Catalyst switches** combines firewall, IPS, SSL VPN, IPsec VPN, DoS mitigation, and virtual services to build into security zones.

Here are some recommended best practices for infrastructure protection:

- Access network equipment remotely with SSH instead of Telnet.
- Use AAA for access control management.
- Enable SYSLOG collection; review the logs for further analysis.
- Use SNMPv3 for its security and privacy features.
- Disable unused network services such as tcp-small-servers and udp-small-servers.
- Use FTP or SFTP instead of TFTP to manage images.
- Use access classes to restrict access to management and the CLI.
- Enable routing protocol authentication when available (EIGRP, OSPF, IS-IS, BGP, HSRP, VTP).
- Use one-step lockdown in Security Device Manager (SDM) before connecting the router to the Internet.

References and Recommended Readings

IANA protocol numbers, http://www.iana.org/assignments/protocol-numbers

"Managing Risk and Compliance with Cisco Self-Defending Network—U.S.," http://www.cisco.com/en/US/netsol/ns625/networking_solutions_white_paper0900aecd80351e82.shtml

"Managing Security Best Practices with Cisco Self-Defending Network," http://www.cisco.com/en/US/netsol/ns625/networking_solutions_white_paper0900aecd803b5fc9.shtml

Module 6, "Evaluating Security Solutions," Designing for Cisco Internetwork Solution Course (DESGN) v2.0

RFC 2402, *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt

RFC 2406, *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics covered in this chapter:

- **U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley or SOX)** focuses on the accuracy and the controls imposed on a company's financial records.
- **Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)** provides protection against the sale of bank and account information that is regularly bought and sold by financial institutions.
- **U.S. Health Insurance Portability and Accountability Act (HIPAA)** applies to the protection of private health information that is used electronically.
- **EU Data Protection Directive 95/46/EC** calls for the protection of people's privacy with respect to the processing of personal data.
- **Reconnaissance** gathers as much information as possible about the target host and/or network.
- **Gaining unauthorized access** is the act of attacking or exploiting the target host system.
- **Denial of service (DoS)** attacks try to overwhelm resources such as memory, CPU, and bandwidth, thus impacting the attacked system and denying legitimate users access.
- **NMAP** (Network Mapper) scans large networks or one host. It is an open-source utility used for network exploration and/or security audits.
- **Superscan** (made for Windows) provides high-speed scanning, host detection, and Windows host enumeration and banner grabbing.
- **DHCP snooping** verifies DHCP transactions and prevents rogue DHCP servers from interfering with production traffic.
- **Dynamic ARP inspection** intercepts ARP packets and verifies that the packets have valid IP-to-MAC bindings.

- **Unicast RPF** prevents unknown source addresses from using the network as a transport mechanism to carry out attacks.
- **Access control lists (ACLs)** control what traffic is allowed on the network.
- **Rate limiting** controls the rate of bandwidth that incoming traffic is using, such as ARPs and DHCP requests.
- **NetStumbler** identifies wireless networks using 802.11a/b/g WLAN standards.
- **Kismet** is an 802.11 wireless sniffer and IDS that can collect traffic from 802.11a/b/g networks.
- **Acceptable-use policy** is a document that defines the roles and responsibilities within risk management and should have clear explanations to avoid confusion.
- **Network access control policy** is a document that defines general access control principles used and how data is classified, such as confidential, top-secret, or internal.
- **Security management policy** explains how to manage the security infrastructure.
- **Incident-handling policy** defines the processes and procedures for managing incidents and even emergency-type scenarios.
- **Secure**—Identification, authentication, ACLs, stateful packet inspection (SPI), encryption, and VPNs.
- **Monitor**—Intrusion and content-based detection and response.
- **Test**—Assessments, vulnerability scanning, and security auditing.
- **Improve**—Security data analysis, reporting, and intelligent network security.
- **Authentication** establishes the user's identity and access to the network resources.
- **Authorization** describes what can be done and what can be accessed.
- **Accounting** provides an audit trail of activities by logging the actions of the user.
- **Adaptive Security Appliance (ASA)** integrates essential security technologies in one platform (firewall, IPS, IPsec VPN, and SSL VPN).
- **Routers** consolidates IOS firewall, IPS, IPsec VPN, DMVPN, and SSL VPN into the routing platforms to secure the router if it is attacked.
- **Catalyst switches** combines firewall, IPS, SSL VPN, IPsec VPN, DoS mitigation, and virtual services to build into security zones.

Table 13-4 shows a sample risk index calculation for a typical large corporation facing a couple of typical risks. If the risk index number calculated is high, you have more risk and thus more impact to the organization. The lower the index number calculated means that there is less risk and less impact to the organization.

Table 13-4 *Risk Index Calculation*

Risk	Severity (S) Range1 to 3	Probability (P) Range1 to 3	Control Range1 to 3	Risk Index (S * P)/ C Range .3 to 9
DoS attack lasting for 1.5 hours on the e-mail server	2	2	1	4
Breach of confidential customer lists	3	1	2	1.5

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What technique can be used to protect private information that is transported over the Internet between the headquarters and branch office? (Select the best answer.)
   a. Authentication
   b. Log all data
   c. Encryption
   d. Accounting
2. What would be recommended to protect database servers attached to a switch with a T1 to the Internet? (Select all that apply.)
   a. Firewall
   b. Server Load Balancing (SLB)
   c. Implement host-based security
   d. SPAN
3. What network security issue does 3DES encryption aim to solve?
   a. Data integrity
   b. User authentication
   c. Data authentication
   d. Data confidentiality
4. Users are reporting a DoS attack in the DMZ. All the servers have been patched, and all unnecessary services have been turned off. What else can you do to alleviate some of the attack's effects? (Select all that apply.)
   a. Rate-limit traffic on the firewall's ingress
   b. Use ACLs to let only allowed traffic into the network
   c. Block all TCP traffic from unknown sources
   d. DHCP Snooping for the DMZ segment

5. You are a network engineer for ABC Corp. You need to bring your coworkers up to date on network security threats. What would you discuss with them? (Select all that apply.)
   a. Reconnaissance and gaining unauthorized access
   b. DHCP snooping
   c. Rate limits
   d. DoS
6. True or false: IPsec can ensure data integrity and confidentiality across the Internet.
7. What focuses on the accuracy and controls imposed on a company's financial records?
   a. HIPAA
   b. GLBA
   c. SOX
   d. EU Data Protection Directive
8. What are components of managing the security infrastructure? (Select all that apply.)
   a. Security management policy
   b. Incident-handling policy
   c. Network access control policy
   d. None of the above
9. Which security legislative body calls for the protection of people's privacy?
   a. HIPAA
   b. GLBA
   c. EU Data Protection Directive
   d. SOX
10. True or false: HIPAA protects companies' financial records.
11. True or false: Distributed DoS attacks are when multiple sources work together to deliver an attack.
12. True or false: Social engineering involves manipulating users into giving out confidential information.
13. How can attackers obtain sensitive account information? (Select all that apply.)
   a. Password-cracking utilities
   b. Capturing network traffic
   c. Social engineering
   d. All of the above

14. What best describes how to protect data's integrity?
    a. System availability
    b. Data confidentiality
    c. Ensuring that only legitimate users can view sensitive data
    d. Allowing only authorized users to modify data
15. List some targets that are used for attacks.
16. What provides an audit trail of network activities?
    a. Authentication
    b. Accounting
    c. Authorization
    d. SSHv1
17. What authenticates valid DHCP servers to prevent them from interfering with production?
18. True or False: Unicast RPF is used to prevent unknown source addresses from using the network to route traffic.
19. What can control the rate of traffic that is allowed into the network?
20. What contains the organization's procedures, guidelines, and standards?
21. How can you enforce access control? (Select all that apply.)
    a. Restrict access using VLANs
    b. Restrict access using OS-based controls
    c. Use encryption techniques
    d. All of the above
22. What is a general user document that is written in simple language to describe the roles and responsibilities within risk management?
23. True or false: The network access control policy defines the general access control principles used and how data is classified, such as confidential, top-secret, or internal.
24. What are the four steps used to facilitate continuing efforts in maintaining security policies?
    a. Secure, monitor, maintain, close out
    b. Monitor, test, evaluate, purchase
    c. Improve, test, purchase, evaluate
    d. Secure, monitor, test, improve

25. True or false: As part of the Cisco Self-Defending Network, Trust and Identity Management defines who and what can access the network, as well as when, where, and how that occurs.

26. True or false: A common two-factor authentication technique involves the use of a six-digit PIN from a token in addition to a user password.

27. Match the encryption keys and VPN protocols with their definitions:

    i. IPsec

    ii. SSL

    iii. Shared secret

    iv. PKI

    a. Both sides use the same key

    b. Uses AH and ESP

    c. Web browser TCP port 443

    d. Asymmetric cryptography

This chapter covers the following subjects:

- Cisco Self-Defending Network
- Trust and Identity Technologies
- Detecting and Mitigating Threats
- Security Management Applications
- Integrating Security into Network Devices
- Securing the Enterprise

CHAPTER 14

Security Technologies and Design

This chapter covers the Cisco Self-Defending Network (SDN) architecture, security technologies, and design options for securing the enterprise. The CCDA candidate can expect many questions related to integrating security technologies and mitigating security exposures. This chapter also focuses on how to integrate security into existing network devices and security platforms throughout your network. Furthermore, the CCDA must understand the different types of security features available and where to deploy them.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 14-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 14-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Cisco Self-Defending Network	1, 2
Trust and Identity Technologies	3, 4
Detecting and Mitigating Threats	5, 6
Security Management Applications	7
Integrating Security into Network Devices	8
Securing the Enterprise	9, 10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. The Cisco Self-Defending Network consists of which of the following components? (Select all that apply.)
   a. Trust and identity management
   b. Secure connectivity
   c. Threat defense
   d. Self healing
2. What network security platform combines a high-performance firewall with an IPS, antivirus, IPsec, and an SSL VPN in a single unified architecture?
   a. Integrated services routers
   b. Cisco Catalyst switches
   c. Adaptive security appliances
   d. NAC
3. Which media-level access control standard developed by IEEE permits and denies access to the network and applies traffic policy based on identity?
   a. AES
   b. 802.1X
   c. NAC
   d. FWSM
4. What mechanism protects networks from threats by enforcing security compliance on all devices attempting to access the network?
   a. NAC
   b. CSA MC
   c. ASDM
   d. SDM

5. Which of the following can be used to perform firewall filtering with the use of ACLs? (Select the best answer.)
   a. ASA
   b. PIX
   c. FWSM
   d. All of the above
6. What Cisco software is loaded on hosts and referred to as HIPS?
   a. Cisco Security Agent
   b. NetFlow
   c. CS-MARS
   d. FWSM
7. Which security management solution integrates the configuration management of firewalls, VPNs, routers, switch modules, and IPS devices?
   a. CSM
   b. SDM
   c. ASDM
   d. ACS
8. When integrating security into the network, which of the following can be used? (Select all that apply.)
   a. PIX
   b. ASA
   c. Cisco IOS IPS
   d. RME
9. Which of the following is used to detect and mitigate threats?
   a. 802.1X
   b. NetFlow
   c. NAC
   d. SSH

10. What Cisco Security Management platform is used to control the TACACS and RADIUS protocols?

    a. SSH
    b. NIPS
    c. ACS
    d. HIPS

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers security topics that you need to master for the CCDA exam. It begins with a discussion of the Cisco Self-Defending Network and covers the strategy for identifying and responding to security threats. The next section, "Trust and Identity Technologies," discusses the technologies and services used on network security devices such as routers and firewalls. The section, "Detecting and Mitigating Threats," covers the technologies supporting threat defense, such as network- and host-based intrusion prevention systems, ASAs, and Cisco MARS.

The "Security Management Applications" section describes the Cisco Security Management framework of products designed to support the Cisco Self-Defending Network devices. Next, the "Integrating Security into Network Devices" section covers the security features integrated into Cisco network devices, such as routers, firewalls, IPS, endpoint security, and Catalyst Service modules. Finally, the "Securing the Enterprise" section reviews the locations to deploy security devices and solutions in the enterprise campus, data center, and WAN edge.

Cisco Self-Defending Network

The Self-Defending Network is Cisco's strategy for securing an organization's business by identifying, preventing, and adapting to security threats. This level of protection allows organizations to make better use of their network resources, thus improving business processes and increasing revenue.

Operational management and policy control serves as a component of the Self-Defending Network to establish security policies that in turn enforce security access levels. In addition, this serves as the basis for the secure transport of data communications throughout the network.

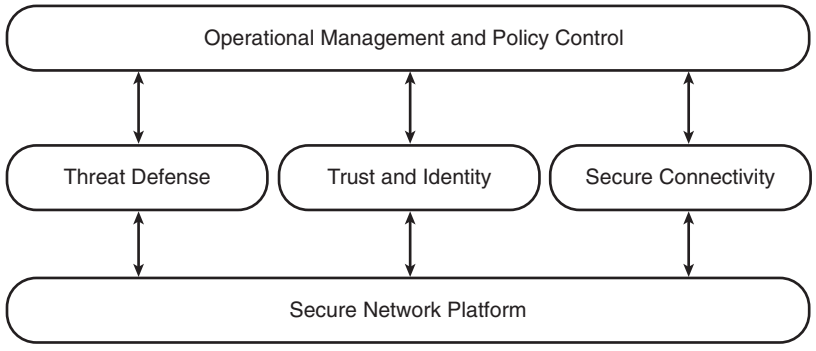
Security must be fully integrated into all components of the network using advanced technologies and services to protect assets, respond to threats, and ensure confidentiality. The Cisco Self-Defending Network has defined three critical components:

- **Trust and identity management**—Securing critical assets
- **Threat defense**—Responding to the effects of security outbreaks
- **Secure connectivity**—Ensuring privacy and confidentiality of data communications

The underlying foundation of the Cisco Self-Defending Network is the secure network. The Cisco SDN provides transport for all the far-reaching security features and services. These feature and service elements are controlled by the operational management, and the policy control is governed by the organization.

Figure 14-1 shows the Cisco Self-Defending Network framework and how the three critical components tie to management, policy, and the secure network foundation.

Figure 14-1 *Cisco Self-Defending Network*



Network Security Platforms

Network security starts with having a secure underlying network. The underlying network provides an ideal place to implement core and advanced security solutions. The center of these secure network solutions includes the Adaptive Security Appliances (ASA), Integrated Services Routers (ISR), and Cisco Catalyst switches that have integrated security embedded in them. These are highly intelligent network security devices with many built-in security features that provide a framework for incorporating security throughout the network. Here is a description of some important security device platforms:

- **Adaptive Security Appliance (ASA)** is a high-performance firewall appliance with intrusion prevention system (IPS), antivirus, IPsec, and SSL VPN technologies integrated into a single unified architecture. ASA also has embedded Network Admission Control (NAC) capabilities.
- **Integrated Services Router (ISR)** combines IOS firewall, VPN, and IPS services across the router portfolio, which enables new security features on existing routers. ISR routers also have NAC enabled.
- **Cisco Catalyst switches** include denial of service (DoS) and man-in-the-middle attack mitigations, integrate the use of service modules for high protection, and provide for secure connectivity.

Self-Defending Network Phases

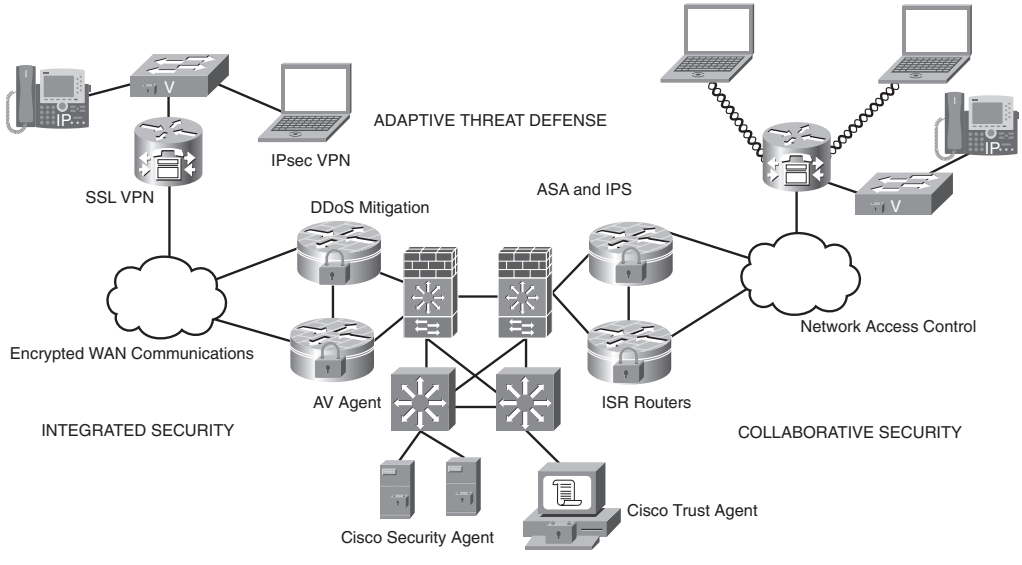
The Self-Defending Network has three network phases that function together to provide a strong, secure network from the network layer up to the application layer. Here is some more information about each of the network phases:

- **Integrated security**—Security throughout the existing infrastructure in which each network device acts as a point of defense. Hardware devices include routers, switches, wireless, and security appliances supporting firewalling, SSL VPN, IPsec VPN, and encrypted WAN communications.
- **Collaborative security**—Security components that work together with an organization's security policies. Network Admission Control is an example of a control that allows access to endpoints only after they have passed authentication based on security policies.
- **Adaptive threat defense**—Tools used to defend against security threats and varying network conditions. Application awareness defends against Internet-based attacks, and behavioral recognition defends against viruses, spyware, and DoS attacks. Network control provides monitoring functions and manages the security infrastructure, enabling tools for audits and analysis.

Additionally, other security services are contained in this framework, such as Cisco Security Agent, Cisco Trust Agent, NAC, and intrusion prevention. These Self-Defending Network products can be deployed independently or merged to allow for a more complete security solution.

Figure 14-2 illustrates the three Cisco Self-Defending Network phases and where various security technologies, mechanisms, and applications reside.

Figure 14-2 *Self-Defending Network Phases*



Trust and Identity Technologies

Trust and identity technologies are security controls that enable network traffic security. The following are examples of technologies used to support trust and identity management:

- **Access control lists**—ACLs are used on routers, switches, and firewalls to control access. For example, ACLs are commonly used to restrict traffic on the ingress or egress of an interface by a wide variety of methods, such as using IP addresses and TCP or UDP ports.
- **Firewall**—A security device designed to permit or deny network traffic based on source address, destination address, protocol, and port. The firewall enforces security by using the access and authorization policy to determine what is trusted and untrusted. The firewall also performs stateful packet inspection (SPI), which keeps track of the state of each TCP/UDP connection. SPI permits ingress traffic if the traffic originated from a higher security interface, such as the inside.
- **Network Admission Control (NAC)**—Protects the network from security threats by enforcing security compliance on all devices attempting to access the network.
- **802.1X**—An IEEE media-level access control standard that permits and denies admission to the network and applies traffic policy based on identity.
- **Cisco Identity-Based Network Services (IBNS)**—Based on several Cisco solutions integrated to enable authentication, access control, and user policies to secure network infrastructure and resources.

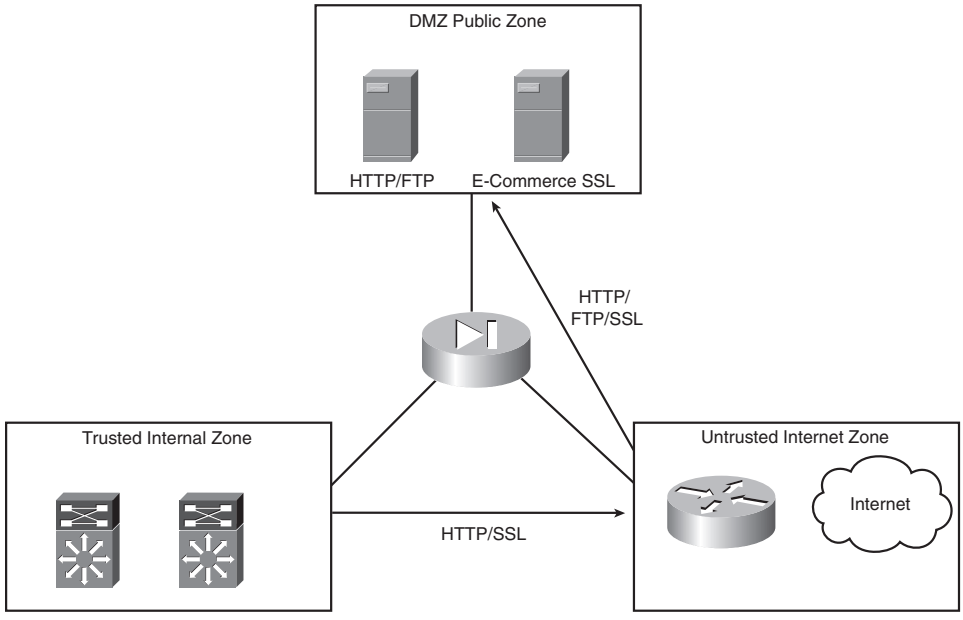
The following sections cover some of these trust and identity technologies in more detail.

Firewall ACLs

Firewalls are used to control access to and from the Internet and to provide interaction with customers, suppliers, and employees. But because the Internet is insecure, firewalls need to use ACLs to permit and deny traffic flowing through it. Firewalls use security zones to define trust levels that are associated with the firewall's interfaces. For example, the trusted zone is associated with an interface connected to the internal network, and the untrusted zone is associated with an interface connected to outside of the firewall. Common security zones include the inside, outside, and DMZ, but others can be created as needed.

Figure 14-3 shows a PIX firewall with three zones and the permitted policy and flow of the traffic.

Figure 14-3 *Firewall ACLs and Zones*



The policy for the firewall shown in Figure 14-3 includes the following:

- Allow HTTP and HTTPS to the Internet
- Allow HTTPS and FTP to the public web and FTP server
- Allow HTTPS to the public e-commerce server

NAC Framework and Appliance

Cisco NAC Framework and Cisco NAC Appliance are two ways to deploy NAC and meet the organization's technology and operational needs. The NAC Framework is an integrated solution led by Cisco that incorporates the network infrastructure and third-party software to impose security policy on the attached endpoints. The NAC Appliance is a self-contained product that integrates with the infrastructure to provide user authentication and enforce security policy for devices seeking entry into the network. NAC Appliances can also repair vulnerabilities before allowing access to the network infrastructure.

NAC can restrict access to noncompliant devices but permits access to trusted wired or wireless endpoints such as desktops, laptops, PDAs, and servers.

Both of these deployment options use the common NAC infrastructure and have considerations for timeframes and customer requirements.

Cisco Identity-Based Network Services

The Cisco Identity-Based Network Services solution is a way to authenticate host access based on policy for admission to the network. IBNS supports identity authentication, dynamic provisioning of VLANs on a per-user basis, guest VLANs, and 802.1X with port security.

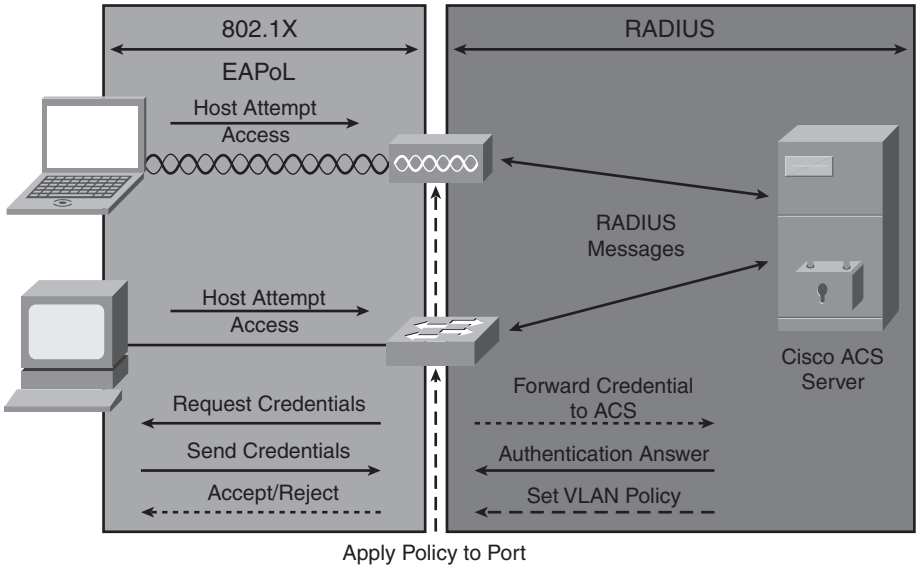
The 802.1X protocol is a standards-based protocol for authenticating network clients by permitting or denying access to the network. The 802.1X protocol operates between the end-user client seeking access and an Ethernet switch or wireless access point providing the connection to the network. In 802.1X terminology, clients are called supplicants, and switches and APs are called authenticators. A back-end RADIUS server such as a Cisco Access Control Server (ACS) provides the user account database used to apply authentication and authorization.

With an IBNS solution, the host uses 802.1X and Extensible Authentication Protocol over LANs (EAPoL) to send the credentials and initiate a session to the network. After the host and switch establish LAN connectivity, username and password credentials are requested. The client host then sends the credentials to the switch, which forwards them to the RADIUS ACS.

The RADIUS ACS performs a lookup on the username and password to determine the credentials' validity. If the username and password are correct, an accept message is sent to the switch or AP to allow access to the client host. If the username and password are incorrect, the server sends a message to the switch or AP to block the host port.

Figure 14-4 illustrates the communication flow of two hosts using 802.1X and EAPoL with the switch, AP, and back-end RADIUS server.

Figure 14-4 *802.1X and EAPoL*



Identity and Access Control Deployments

Validating user authentication should be implemented as close to the source as possible, with an emphasis on strong authentication for access from untrusted networks. Access rules should enforce policy deployed throughout the network with the following guidelines:

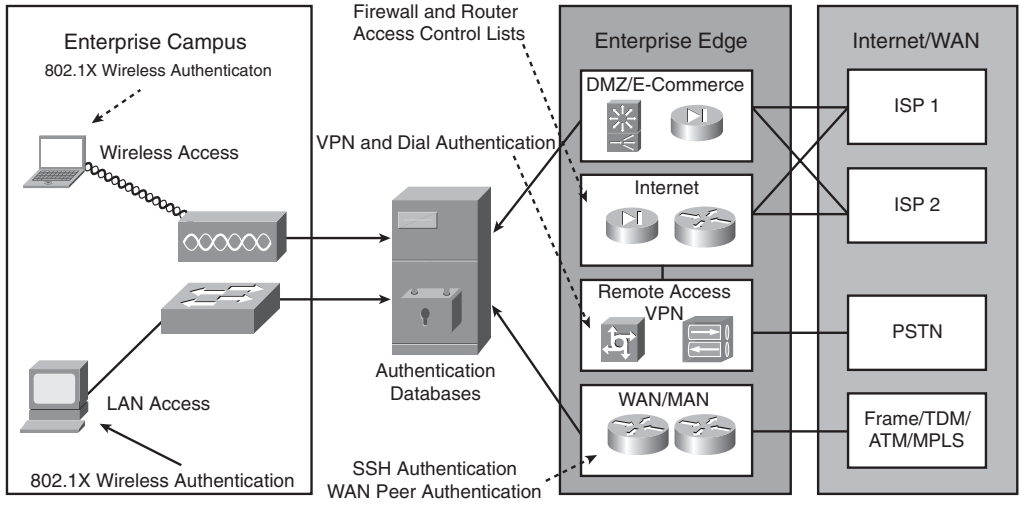
- Source-specific rules with *any* type destinations should be applied as close to the source as possible.
- Destination-specific rules with *any* type sources should be applied as close to the destination as possible.
- Mixed rules integrating both source and destination should be used as close to the source as possible.

An integral part of identity and access control deployments is to allow only the necessary access. Highly distributed rules allow for greater granularity and scalability but unfortunately increase the management complexity. On the other hand, centralized rule deployment eases management but lacks flexibility and scalability.

Practicing "defense in depth" by using security mechanisms that back each other up is an important concept to understand. For example, the perimeter Internet routers should employ ACLs to filter packets in addition to the firewall inspecting packets at a deeper level.

Figure 14-5 shows the importance of the authentication databases and how many network components in the Enterprise rely on them for authentication services.

Figure 14-5 *Identity and Access Control*



Detecting and Mitigating Threats

The use of threat detection and mitigation techniques enables early detection of and notifications about unwanted malicious traffic. The goals are to detect, notify, and help stop unforeseen and unauthorized traffic. These techniques help increase the network's availability, particularly against unidentified and unexpected attacks. Threat detection and mitigation solutions include the following:

- **Endpoint protection**—Viruses and worms can create havoc by propagating infections from host to host throughout the network. To combat these infestations, endpoint protection such as Cisco's Security Agent is used. It limits the scope of virus outbreaks and is adaptable to new and emerging threats. In addition, antivirus services can aid hosts with detection and removing infections based on known virus pattern markings.

- **Application security and anti-*X* Defense**—Several new application-layer network products have been released that help address new classes of threats, such as spam, phishing, spyware, packet abuse, and unauthorized point-to-point file sharing. Anti-X defense provides comprehensive antivirus, anti-spyware, file-blocking, anti-spam, URL blocking, and content filtering services. These products supplement traditional firewalls and network-based intrusion detection system (NIDS) solutions with more granular traffic inspection services, thereby quarantining traffic so that it does not propagate throughout the network.

- **Infection containment**—Cisco's ASA, PIX, Firewall Services Module (FWSM), and IOS firewalls protect the network by creating security zones that partition the network into separate segments. The firewall services provide perimeter network security but do not eliminate the need for continuous network monitoring. As part of the Cisco SDN architecture, NAC is also used in the perimeter to perform policy-based admission control, thus reducing potential threats.

- **Inline IPS and anomaly detection**—Cisco has innovated in the area of network intrusion detection systems by being the first to incorporate NIDS into the IOS on routing and switching platforms. In addition, IPS solutions have inline filtering features that can remove unwanted traffic with programmable features that classify traffic patterns. The 4200 IPS sensor appliances, IDSM-2, and the IOS IPS can identify, analyze, and stop unwanted traffic from flowing on the network. Another set of tools used to prevent DDoS attacks and ensure business continuity are the Cisco Traffic Anomaly Detector XT and Guard XT, along with the Cisco Traffic Anomaly Detector Services and Cisco Guard Services module.

Threat Detection and Mitigation Technologies

- Here are some examples of Cisco's Threat Detection and Mitigation technologies:
  - PIX—Firewall appliances
  - FWSM—Catalyst 6500 Firewall Services Module
  - ASA—Adaptive Security Appliance (Robust firewall and/or network-based intrusion prevention system [NIPS])

  - IOS firewall—Cisco IOS Software feature set
  - IPS sensor appliance—NIPS
  - IPS—Intrusion prevention system (IOS feature)
  - CSA—Cisco Security Agent (host-based intrusion prevention system [HIPS])
- Network monitoring:
  - NetFlow—Stats on packets flowing through router (IOS feature)
  - Syslog—Logging data (IOS feature)
  - SNMP—Simple Network Management Protocol (IOS feature)
  - MARS—Monitoring, Analysis, and Response System
  - Cisco Traffic Anomaly Detector Module—Detects high-speed denial-of-service attacks

Threat Detection and Mitigation Solutions

Threat detection and mitigation solutions are deployed throughout the network and can serve as an effective layered defense for secure network communications. For example, let's say your network is being attacked from the Internet, such as a worm or virus outbreak. The Internet WAN routers are your first line of protection and can be used to spot increasing network load or suspicious NetFlow data. After some information has been collected, specific granular ACLs can be used to further identify the attack.

The network IPS provides deep packet inspection to determine the additional details about the attack's signature. HIPS can be deployed using hardware appliances or IOS feature integration; both include signature-based attack detection mechanisms. HIPS also allows for host policy enforcement and verification.

Firewalls can perform stateful packet inspections and block unwanted network traffic locally in the event of an attack. However, it is preferable to engage the ISP and have them block the attack from even entering your network.

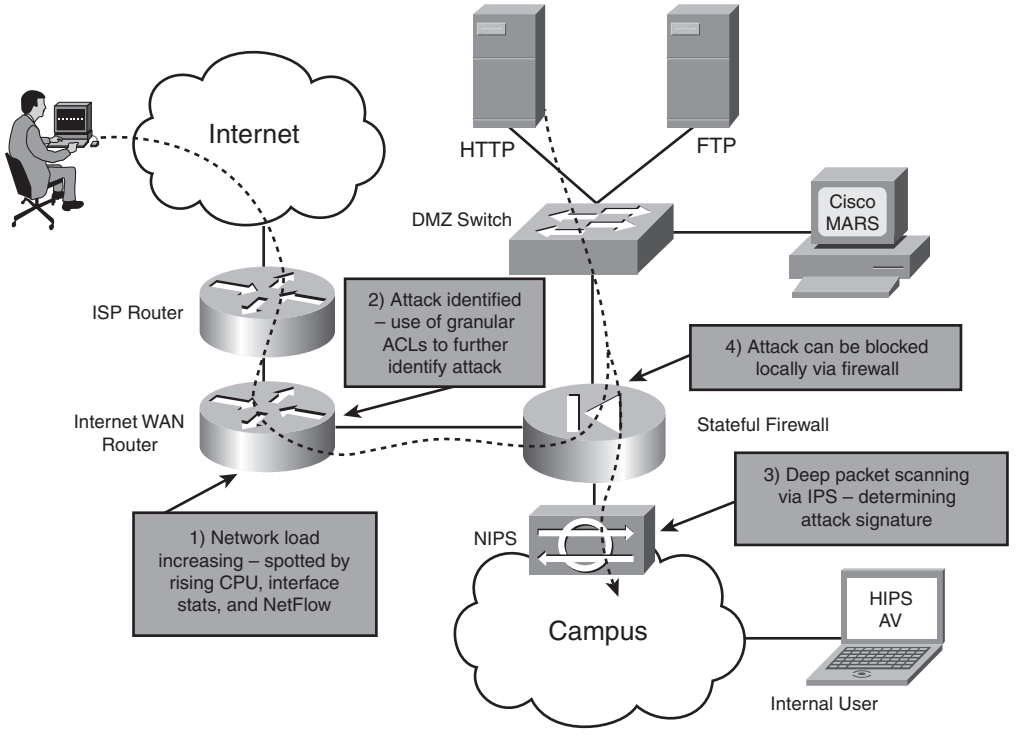
To successfully detect threats and mitigate them, it is important to understand where to look for potential threats. The following are good sources of information for detecting and mitigating threats:

- NetFlow
- Syslog
- RMON events

- SNMP thresholds and traps
- CPU and interface statistics
- Cisco Security MARS reporting

Figure 14-6 depicts an attacker sourcing from the Internet and targeting the internal network and how the threat can be detected and mitigated.

Figure 14-6 *Threat Detection and Mitigation*



Security Management Applications

Security management applications consolidate network management and monitoring, which allows more secure control of the network. Security management provides several functions:

- Central repository for collecting network information for further analysis of security-related events. In addition, many applications have reporting capabilities to help network managers' present technical information to upper management. Some examples include Authentication, Authorization, and Accounting (AAA) with TACACS and RADIUS servers, Syslog servers, and intrusion detection systems, which enable deep inspection of complex security events.

- Allows for easier deployment of security policies into the security devices via graphical user interface tools. These tools help you maintain the consistency of the security policies across a broad spectrum of network device types.
- Role-based access control for all accounts to separate administrative tasks and user functions.

Security implementations need to be planned properly using the security policies governed by the organization to make good use of the security applications. From time to time, audits are necessary, which requires updates to the security policy and related security management applications. A major risk to security implementations is policy error. Management needs to be cognizant of the security policy and know how to manage incidents properly.

Security Platform Solutions

Cisco has a variety of security management products and technologies that allow scalable administration and enforcement of security policy for the Cisco Self-Defending Network platform. These solutions reduce the operational management and automate many of the common tasks, including configuration, analysis, incident response, and reporting. Some of the security management platforms consist of the following:

- **Cisco Security Manager (CSM)** is an integrated solution for configuration management of firewall, VPN, router, switch module, and IPS devices. CSM has capabilities for security policies to be deployed by device, by group, or globally for all devices.
- **Cisco Secure Access Control Server (ACS)** provides centralized control for administrative access to Cisco devices and security applications. ACS provides for both TACACS and RADIUS security services and supports routers, switches, firewalls, VPN concentrators, content switches, wireless, and VoIP solutions.
- **Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)** is an appliance-based solution for network security administrators to monitor, identify, isolate, and respond to security threats. MARS understands the network topology and device configurations from routers, switches, firewalls, and IPS devices. MARS also can model packet flows on the network.
- **Management Center for CSA (CSA MC)** is an SSL web-based tool for managing Cisco Security Agent configurations. CSAs can be grouped to deploy security policies to multiple agents.
- **Cisco Router and Security Device Manager (SDM)** is a web-based tool for routers and supports a wide range of IOS software. SDM improves productivity, simplifies router deployments, and can help troubleshoot network issues. SDM is free software for Cisco router models ranging from the Cisco 830 series to the Cisco 7301.

- **Cisco Adaptive Security Device Manager (ASDM)** is a web-based tool for managing Cisco ASA 5500 series appliances, PIX 500 series appliances (version 7.0 and higher), and Cisco Catalyst 6500 Firewall Services Modules (FWSM version 3.1 and higher). ASDM comes with wizards to automate many common tasks and comprehensive monitoring services.
- **Cisco Intrusion Prevention System Device Manager (IDM)** is a web-based application that configures and manages IPS sensors. IDM runs a web server and is accessible via SSL supporting IPS v5.0 sensors.

Integrating Security into Network Devices

It is crucial to integrate security into all network devices throughout your network. Common device types include

- IOS routers and switches
- PIX firewalls
- Adaptive Security Appliances (ASA)
- VPN concentrators
- Intrusion Prevention Systems (NIPS/HIPS)
- Catalyst 6500 service modules
- Endpoint security

The following sections discuss device security integration in more detail.

IOS Security

Cisco has developed many security features that are integrated into the IOS base software or security-specific feature sets. Here are some of the major areas of security focus that have been included with IOS releases:

- **Cisco IOS Firewall** feature set provides stateful firewall functionality for perimeter routers running IOS. IOS Firewall allows businesses to protect networks from network and application layer attacks, improve uptime, and offer policy enforcement for internal and external connections.
- **Cisco IOS IPS** offers inline deep-packet inspection to successfully diminish a wide range of network attacks. IOS IPS can identify, classify, and block malicious traffic in real time. IOS IPS operates by loading attack signatures on the router and then matching the attacks based on signatures.

- **Cisco IOS IPsec** encrypts data at the IP packet level using a set of standards-based protocols. IPsec provides data authentication, anti-replay, and data confidentially, and is the preferred method of securing VPNs.
- **Cisco IOS Trust and Identity** is a set of services that includes the following:
  - AAA—Framework and mechanisms for controlling device access
  - Secure Shell (SSH)—Used for encrypted router access
  - Secure Socket Layer (SSL)—Secure web application access
  - 802.1X—Standards-based access control protocol to permit or deny network access
  - PKI—Strong authentication for e-commerce applications

ISR Security Hardware Options

The Cisco Integrated Services Routers have additional hardware options that enhance the routers' security capabilities. Here are some of the available hardware options:

- **Built-in VPN Acceleration** is hardware-based encryption that offloads VPN processing from the router's internal CPU to improve VPN throughput.
- **High-Performance AIM** is a VPN encryption advanced integration module used to terminate large numbers of VPN tunnels such as with DMVPN. The module supports 3DES and AES, which increases the router encryption and compression performance.
- **IDS Network Module (NM-CIDS)** provides technologies to prevent a large range of security threats. IDS network modules also include correlation and validation tools to decrease the number of false positives.
- **Secure Voice** is digital signal processor (DSP) slots on the ISR for use with packet voice/fax DSP modules (PVDM). These offer capabilities such as conferencing and transcoding. In addition, Secure Real-time Transport Protocol (SRTP) protects the entire voice payload by encryption, except for the header, which remains in clear text to support QoS.
- **Network Analysis Module** allows capturing of traffic flows from hosts and the decoding of packets for detailed network analysis. It also collects NetFlow data to increase the visibility into application flows.
- **Content Engine Module** is an Integrated Content module for 2800/3800 series routers that supports 40-GB and 80-GB internal hard disks for application and content networking.

NOTE For a quick reference and complete list of ISR modules, go to http://www.cisco.com/warp/public/765/tools/quickreference/isr.pdf.

Cisco Security Appliances

Cisco Security Appliances provide robust security services and protection, including IPsec VPNs and stateful packet filtering. The following is an overview of Cisco Security Appliances:

- **Adaptive Security Appliance (ASA)**—The ASA is a high-performance multifunction security appliance that offers a comprehensive set of services for securing network environments. The services are customized through product editions tailored for firewall, IPS, anti-*X*, and VPN. The ASA is a critical component of the Cisco Self-Defending Network that provides proactive threat mitigation, controls application data flows, and delivers flexible VPN and IPS services. In addition, the ASA is very cost-effective and easy to manage, and offers advanced integration modules that enhance the processing capabilities.

- **PIX Security Appliance**—The Cisco PIX series of appliances provides robust firewall services for users and application policy enforcement, attack protection, and security VPN connectivity services. The PIX appliances are easy to deploy and are very cost-effective for most network environments. The appliances range from the desktop PIX 501 (SOHO) up to the modular PIX 535, offering Gigabit network interfaces and failover capabilities.

- **VPN concentrators**—The Cisco VPN 3000 concentrators provide businesses with IPsec and SSL VPN connectivity. VPN concentrators are flexible and offer many deployment scenarios. However, they are commonly used to terminate VPN sessions for remote-access connections. VPN concentrators can also be used to terminate site-to-site tunnels with other VPN concentrators, routers, or even PIX firewalls. The centralized architecture and web-based management ease the administrative burden and consolidate the VPN connectivity for the enterprise. Many organizations are now starting to look at the Cisco ASAs instead of the VPN concentrators due to the increased security options in addition to VPN functionality.

Intrusion Prevention

The Cisco IPS solution integrates passive intrusion detection, inline prevention services, and new technologies to increase accuracy and keep legitimate traffic from being affected. The Cisco IPS 4200 series sensors offer significant protection by detecting and stopping threats from attacking your network. With Cisco IPS, version 5.1 supports inline (IPS) or passive (IDS) capabilities. The IPS appliances support multivector threat identification through detailed inspection of data flows in Layers 2 through 7. Multivector identification secures the network from policy violations, vulnerability exploits, and abnormal reconnaissance activities. The following IPS sensors support bandwidth requirements from 65 Mbps to 1 Gbps:

- **IPS 4215** reviews traffic and provides protection up to 65 Mbps.

- **IPS 4240** reviews traffic and provides protection up to 240 Mbps with support for multiple 10/100/1000 interfaces. IPS 4240-DC supports DC power and is Network Equipment Building Standards (NEBS)-compliant.

- **IPS 4255** delivers 500 Mbps of performance and can be used to protect partially utilized Gigabit connected subnets.
- **IPS 4260** delivers 1 Gbps of performance and can be used on Gigabit subnets with copper or fiber network connections, providing additional flexibility.

Catalyst 6500 Services Modules

The Catalyst 6500 switching platform supports additional security services and functionality through the use of services modules. Several modules enable firewall, IDS, SSL, and network analysis services, in addition to IPsec VPN connectivity and anomaly traffic support.

Catalyst 6500 service modules include the following:

- **Firewall Services Module (FWSM)** is a high-speed firewall module for use in the Cisco Catalyst 6500 and Cisco 7600 series routing platforms. Up to four FWSMs can be installed in a single chassis, providing 5 Gbps of throughput performance per module. For service provider environments, the FWSM supports advanced features such as multiple security contexts for both routed and bridged firewall modes.
- **Intrusion Detection Service Module 2 (IDSM2)** is an IDS module that supports both inline (IPS) and passive (IDS) operation. IDSM2 provides up to 500 Mbps of packet inspection capabilities to efficiently protect your infrastructure.
- **SSL Service Module** is an integrated services module for terminating SSL sessions on Cisco Catalyst 6500 series switch or Cisco 7600 series routing platforms. By offloading the SSL terminations with the SSL module, the web server farms can support more connections, increasing operational efficiency. Up to four SSL modules can be used in a single chassis.
- **IPsec VPN SPA** enables scalable VPN services using the Cisco Catalyst 6500 series switches and Cisco 7600 series routing platforms. The module does not have any interfaces, but instead uses the other module interfaces available on the chassis.
- **Network Analysis Module** provides packet-capture capabilities and visibility into all the layers of the data flows. You can analyze application traffic between hosts and networks. The NAMs support RMON2 and mini-RMON features to provide port-level Layer 2 traffic statistics.
- **Traffic Anomaly Detector Module** uses behavioral analysis and attack recognition technology to identify attack patterns. It monitors traffic destined for application servers and builds detailed profiles based on the normal operating conditions. If the module detects any abnormal behavior in the per-flow data conversations, it considers this behavior a potential attack and responds based on the configured preference. You can have the module send an operator an alert or launch the Cisco Anomaly Guard Module to begin mitigation services.

- **Anomaly Guard Module** provides the attack response by blocking malicious traffic at Gbps line rates. With multiple layers of defense, it can divert only traffic destined for targeted devices without affecting legitimate traffic.

Endpoint Security

The Cisco Security Agent (CSA) software protects server and desktop endpoints from the latest threats caused by malicious network attacks. CSA can identify and prevent network attacks that are considered unknown or "Day Zero"-type threats. CSAs are packed with many features, including firewall capabilities, intrusion prevention, malicious mobile code protection, operating-system integrity assurance, and audit log consolidation. All these features can be configured and managed through the use of the Management Center for Cisco Security Agents. CSAs can be used with Cisco MARS by sending important endpoints to MARS, thereby improving MARS threat identification and security investigations throughout the network.

The Management Center for Cisco Security Agents provides centralized web-based management for all CSAs deployed in your network. The MC for CSAs comes with more than 20 preconfigured policies that can be used to deploy thousands of agents quickly across the enterprise network. You can create software distribution packages, create or modify security policies, monitor security alerts, and generate reports. It also has features for running the agents in "IDS mode," in which suspicious activity is only alerted to the MC console, not blocked.

Securing the Enterprise

The Cisco Self-Defending Network provides the most comprehensive security systems for securing the enterprise network from the threats of today and tomorrow.

Each location in the enterprise network has unique security requirements because concerns are different and vary by location. However, in most cases customizing network security solutions by functional area offers the best protection for the enterprise network.

The next sections examine some ways to use Cisco security systems in the campus, data center, and enterprise edge.

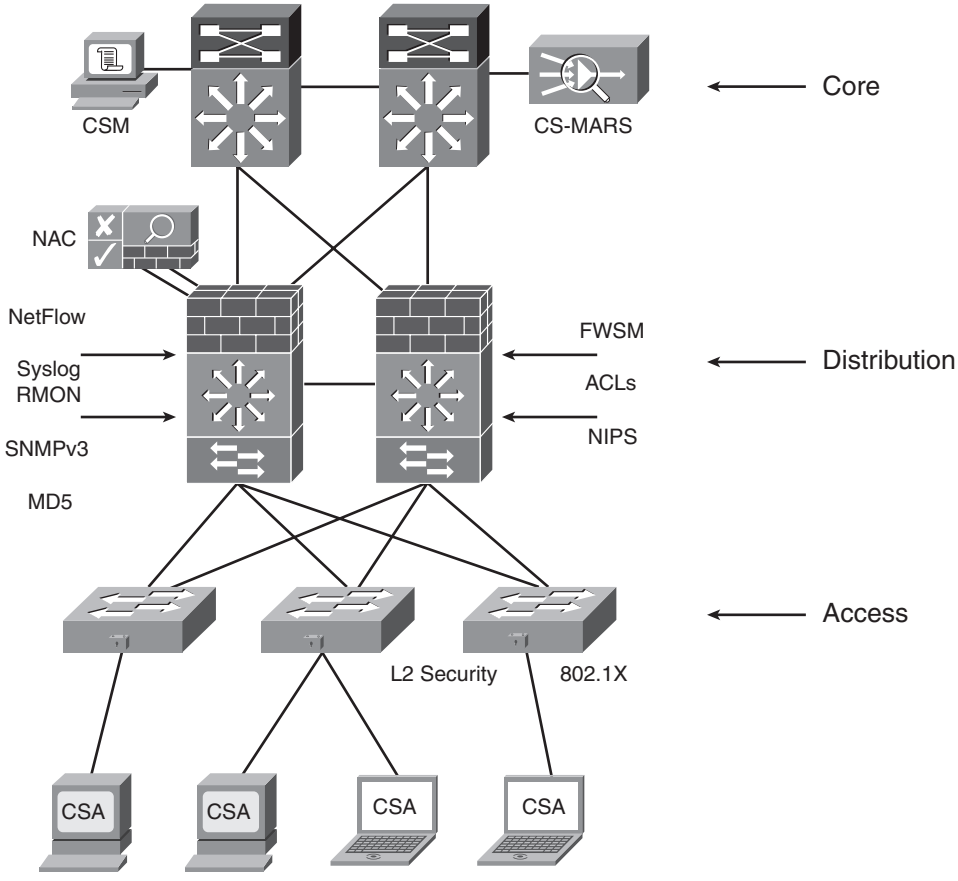
Implementing Security in the Campus

Security for the campus begins with remembering that you need to implement security throughout your network. Several technologies, protocols, solutions, and devices work together to provide the secure campus. Network security should be implemented in the core, distribution, and access layers and can be grouped into four broad categories:

- **Identity and access control**—802.1X, NAC, ACLs, and firewalls
- **Threat detection and mitigation**—NetFlow, Syslog, SNMP, RMON, CS-MARS, NIPS, and HIPS
- **Infrastructure protection**—AAA, TACACS, RADIUS, SSH, SNMP v3, IGP/EGP MD5, and Layer 2 security features
- **Security management**—CSM, CS-MARS, ACS

Figure 14-7 illustrates the use of Enterprise Campus Security and shows where security technologies, protocols, and mechanisms can be deployed in the enterprise campus.

Figure 14-7 *Enterprise Campus Security*



Implementing Security in the Data Center

The Enterprise Data Center hosts critical servers and applications for the main campus and the branch offices. Many of the servers require high availability due to the importance of the information and the high volume of users they serve. Several of the servers may contain sensitive information that is crucial to the business and therefore cannot become compromised. Thus, it needs to be highly secured. Network performance is another area that is critically important, which can limit the choice of protection mechanisms and technologies. Here are some of the risks inherent with Enterprise Data Centers:

- Compromised applications and unauthorized access to critical information
- Exploiting different servers in the business by launching an attack from the compromised servers

To provide adequate security protection, organizations can implement the following:

- **Identity and access control**—802.1X, NAC, ACLs, and firewalls (FWSM/PIX)
- **Threat detection and mitigation**—NetFlow, Syslog, SNMP, RMON, NAM modules, IDS modules, CS-MARS NIPS, and HIPS
- **Infrastructure protection**—AAA, TACACS, RADIUS, SSH, SNMP v3, IGP/EGP MD5, and Layer 2 security features
- **Security management**—CSM, CS-MARS, IDM, and ACS

Figure 14-8 illustrates the use of Enterprise Data Center security and shows where security technologies, protocols, and mechanisms can be deployed in the Enterprise Data Center.

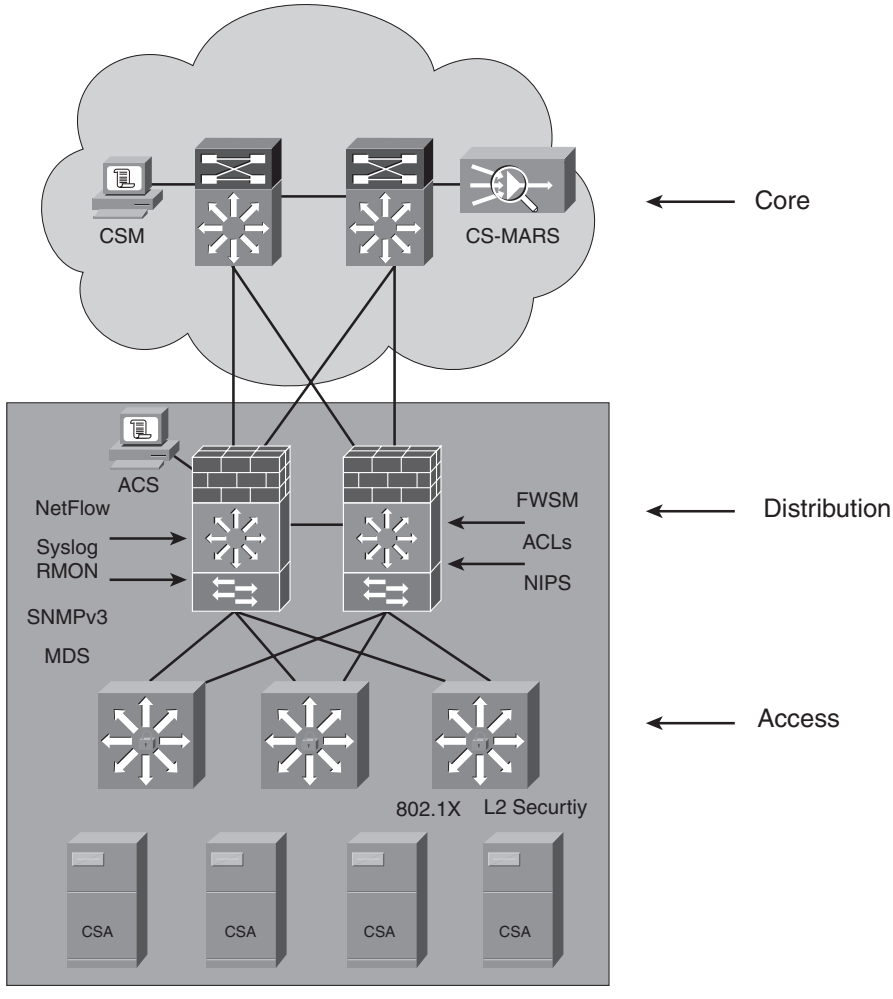
Implementing Security in the Enterprise Edge and WAN

The Enterprise Edge and WAN provide connectivity to other parts of your network over both private and public networks. It is important to consider the available security options when transferring data between locations and over WAN and Internet transports.

Here are some potential risk areas to keep in mind when moving data between locations:

- Attackers obtain access to the network and compromise the confidentiality and integrity of sensitive information with eavesdropping or data manipulation.
- Misconfiguration of the WAN network could cause inappropriate WAN configuration and unwanted connectivity.

Figure 14-8 *Enterprise Data Center Security*

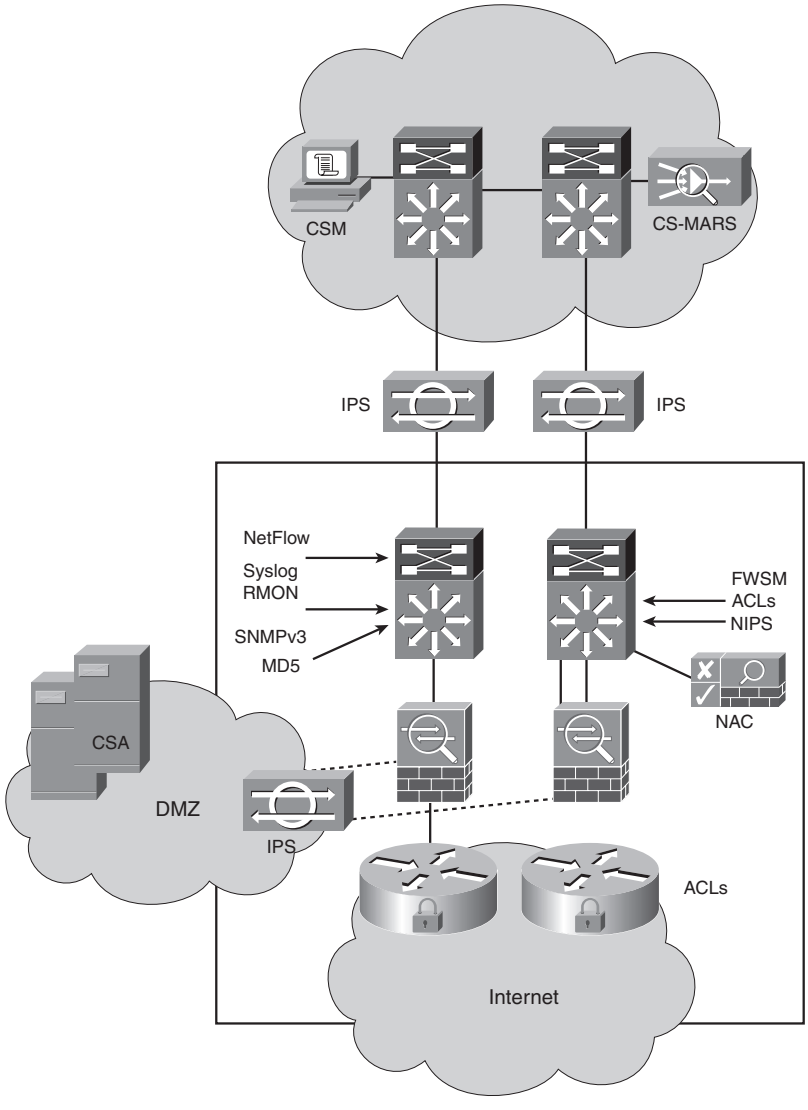


To provide adequate security protection between locations, organizations can implement the following:

- **Identity and access control**—Firewalls, IPsec, SSL VPN, ACLs, and Unicast RPF
- **Threat detection and mitigation**—NetFlow, Syslog, SNMP, RMON, NAM modules, IDS modules, CS-MARS NIPS, and HIPS
- **Infrastructure protection**—AAA, TACACS, RADIUS, SSH, SNMP v3, IGP/EGP MD5, RFC 2827 ingress filtering, and Layer 2 security features
- **Security management**—CSM, CS-MARS, IDM, and ACS

Figure 14-9 illustrates the use of Enterprise Edge and WAN Security, and where security technologies, protocols, and mechanisms can be deployed in the Enterprise Edge and WAN.

Figure 14-9 *Enterprise Edge and WAN Security*



References and Recommended Readings

"The Cisco ASA 5500 as a Superior Firewall Solution," http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd8058ec85.shtml

Cisco ISR series at-a-glance, http://www.cisco.com/warp/public/765/tools/quickreference/isr.pdf

"Core Elements of the Cisco Self Defending Network Strategy," http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd80247914.shtml

"Deploying Firewalls Throughout Your Organization," http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd8057f042.shtml

Module 6 (Evaluating Security Solutions for the Network)—Designing for Cisco Internetwork Solution Course (DESGN) 2.0

"Protecting Against Threats Using the Self-Defending Network," http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/netbr0900aecd803e3629.html

RFC 2827, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, http://www.faqs.org/rfcs/rfc2827.html

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics covered in this chapter:

- Critical components of the Self-Defending Network:
  - Trust and identity management—Securing critical assets
  - Threat defense—Responding to the effects of security outbreaks
  - Secure connectivity—Ensuring privacy and confidentiality of data communications
- Cisco Self-Defending Network phases:
  - **Integrated security**—Security throughout the existing infrastructure in which each network device acts as a point of defense
  - **Collaborative security**—Security components that work with an organization's security policies
  - **Adaptive threat defense**—Tools used to defend against security threats and varying network conditions
- Trust and identify technologies:
  - **Access control lists**—ACLs are used on routers, switches, and firewalls to control access
  - **Firewall**—A security device designed to permit or deny network traffic based on source address, destination address, protocol, and port
  - **Network Admission Control (NAC)**—Protects the network from threats by enforcing security compliance on all devices attempting to access the network
  - **802.1X**—An IEEE media-level access control standard that permits and denies access to the network and applies traffic policy based on identity
  - **Cisco Identity-Based Network Services (IBNS)**—Based on several integrated Cisco solutions to enable authentication, access control, and user policies to secure network infrastructure and resources

- Threat detection and mitigation technologies:
  - PIX—Firewall appliances
  - FWSM—Catalyst 6500 Firewall Services Module
  - ASA—Adaptive Security Appliance (Robust firewall and/or network-based intrusion prevention system [NIPS])
  - IOS firewall—Cisco IOS Software feature set
  - IPS sensor appliance (NIPS)
  - IPS—Intrusion prevention system (IOS feature)
  - CSA—Cisco Security Agent (HIPS)
  - NetFlow—Stats on packets flowing through router (IOS feature)
  - Syslog—Logging data (IOS feature)
  - SNMP—Simple Network Management Protocol (IOS feature)
  - MARS—Monitoring, Analysis, and Response System
  - Cisco Traffic Anomaly Detector Module detects high-speed denial-of-service attacks
- Security management solutions:
  - **Cisco Security Manager (CSM)** is an integrated solution for configuration management of firewall, VPN, router, switch module, and IPS devices.
  - **Cisco Secure Access Control Server (ACS)** provides centralized control for administrative access to Cisco devices and security applications.
  - **Cisco Security Monitoring, Analysis, and Response System (MARS)** is an appliance-based solution for network security administrators to monitor, identify, isolate, and respond to security threats.
  - **Management Center for CSA (CSA MC)** is an SSL web-based tool for managing Cisco Security Agent configurations.
  - **Cisco Router and Security Device Manager (SDM)** is a web-based tool for routers and supports a wide range of IOS software.
  - **Cisco Adaptive Security Device Manager (ASDM)** is a web-based tool for managing Cisco ASA 5500 series appliances, PIX 500 series appliances (version 7.0 or higher), and Cisco Catalyst 6500 Firewall Services Modules (FWSM version 3.1 or higher).
  - **Cisco Intrusion Prevention System Device Manager (IDM)** is a web-based application that configures and manages IPS sensors.

- Integrating security:
  - Cisco IOS Firewall
  - Cisco IOS IPS
  - Cisco IOS IPsec
  - Cisco IOS trust and identity
  - Cisco IOS Routers and Switches
  - Adaptive Security Appliance (ASA)
  - PIX security appliance
  - VPN concentrator
  - IPS modules
  - Catalyst 6500 series service modules
  - Endpoint Security
- Securing the enterprise:
  - Identity and access control—802.1X, NAC, ACLs, and firewalls
  - Threat detection and mitigation—NetFlow, Syslog, SNMP, RMON, CS-MARS, NIPS, and HIPS
  - Infrastructure protection—AAA, TACACS, RADIUS, SSH, SNMP v3, IGP/EGP MD5, and Layer 2 security features
  - Security management—CSM, CS-MARS, and ACS

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What security device combines IOS Firewall with VPN and IPS services?
   a. ASA
   b. ISR
   c. Cisco Catalyst switches
   d. IPS
2. What is a standards-based protocol for authenticating network clients?
   a. NAC
   b. PoE
   c. 802.1X
   d. CSM
3. Cisco _____ Framework is an integrated solution led by Cisco that incorporates the network infrastructure and third-party software to impose security policy attached endpoints.
   a. ASA
   b. CSM
   c. ISR
   d. NAC
4. What is an appliance-based solution for network security administrators to monitor, identity, isolate, and respond to security threats? (Select the best answer.)
   a. CS-MARS
   b. CSA MC
   c. ASDM
   d. IDM

5. Cisco IOS Trust and Identity has a set of services that include which of the following? (Select all that apply.)
   a. 802.1X
   b. SSL
   c. AAA
   d. ASDM
6. True or false: SSH provides unencrypted router access.
7. Cisco IOS _____ offers data encryption at the IP packet level using a set of standards-based protocols.
   a. IPS
   b. IPsec
   c. L2TP
   d. L2F
8. True or false: PKI provides strong authentication for e-commerce applications.
9. What provides hardware VPN encryption for terminating a large number of VPN tunnels for ISRs?
   a. FWSM
   b. IDS Network Module
   c. Network Analysis Module
   d. High-Performance AIM
10. True or false: Integrated Content Module for 2800/3800 series routers captures traffic flows from hosts and allows detailed network analysis.
11. True or false: Cisco VPN 3000 concentrators provide robust firewall servers for users and application policy enforcement, attack protection, and security VPN connectivity services.
12. Which of the following services modules do Cisco Catalyst 6500 switches support? (Select all that apply.)
    a. FWSM
    b. IDSM2
    c. VPN3000
    d. ASA

13. What provides attack responses by blocking malicious traffic with Gbps line rates?
    a. Network Analysis Module
    b. Anomaly Guard Module
    c. Content Switch Module
    d. Traffic Anomaly Detector Module
14. Which of the following are identity and access control protocols and mechanisms? (Select all that apply.)
    a. 802.1X
    b. ACLs
    c. NAC
    d. NetFlow
15. True or false: The Cisco Security Agent protects server and desktop endpoints from the latest threats caused by malicious network attacks.
16. What SSL web-based tool is used to manage Cisco Security Agent configurations?
    a. CSM
    b. IDM
    c. ASDM
    d. CSA MC
17. True or false: IDM is a web-based application that configures and manages IPS sensors.
18. True or false: NetFlow is used for threat detection and mitigation.
19. Which of the following is not one of the phases of the Cisco Self-Defending Network?
    a. Integrated Security
    b. Collaborative Security
    c. Network Admission Control
    d. Adaptive Threat Defense
20. True or false: Cisco ASAs, PIX security appliances, FWSM, and IOS firewall are part of Infection Containment.
21. What IOS feature offers inline deep-packet inspection to successfully diminish a wide range of network attacks?
    a. IOS SSH
    b. IOS SSL VPN
    c. IOS IPsec
    d. IOS IPS

22. The 4200 _____ sensor appliances can identify, analyze, and block unwanted traffic from flowing on the network.

23. What provides centralized control for administrative access to Cisco devices and security applications?

    a. CSM

    b. ACS

    c. CS-MARS

    d. CSA MC

24. True or false: ASDM provides management of Cisco ASAs, PIX, and FWSMs.

25. True or false: IPS 4255 delivers 10000 Mbps of performance and can be used to protect partially utilized Gigabit connected subnets.

26. True or false: FWSM is a high-speed firewall module for use in the Cisco Catalyst 6500 and 7600 series routers.

27. Match each protocol, mechanism, or feature with its security grouping:

    i. CSM

    ii. IGP/EGP MD5

    iii. NetFlow

    iv. NAC

    a. Identity and access control

    b. Threat detection and mitigation

    c. Infrastructure protection

    d. Security management

This chapter covers the following subjects:

- Traditional Voice Architectures
- Integrated Multiservice Networks
- IPT Design

CHAPTER 15

Traditional Voice Architectures and IP Telephony Design

The designs of enterprise voice networks are migrating from the traditional use of Private Branch Exchange (PBX) switches to the use of IP telephony architectures such as Cisco Unified CallManager. Enterprise networks now have to be designed with IP telephony in mind. This chapter reviews Public Switched Telephone Network (PSTN) and PBX voice networks, integrated IP telephony, and quality of service (QoS) for IP telephony (IPT) networks.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 15-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 15-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Traditional Voice Architectures	5, 9
Integrated Multiservice Networks	1, 2, 3, 4, 6, 7
IPT Design	8, 10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. Which International Telecommunication Union (ITU) standard provides a framework for multimedia protocols for the transport of voice, video, and data over packet-switched networks?
   a. Session Initiation Protocol (SIP)
   b. Voice over IP (VoIP)
   c. H.323
   d. Weighted Fair Queuing (WFQ)
2. What is the default coder-decoder (codec) used with VoIP dial peers?
   a. G.711
   b. G.723
   c. G.728
   d. G.729
3. Real-time Transport Protocol (RTP) operates at what layer of the OSI model?
   a. Application
   b. Session
   c. Transport
   d. Network
4. Which H.323 protocol is responsible for call setup and signaling?
   a. H.245
   b. G.711
   c. H.225
   d. RTCP
5. What unit measures the number of voice calls in one hour?
   a. Kbps
   b. Erlang
   c. DS0
   d. FXS
6. Which feature does not transmit packets when there is silence?
   a. Ear and mouth (E&M)
   b. Voice Activity Detection (VAD)
   c. Dial peers
   d. Digital Silence Suppressor (DSS)

7. What does Compressed Real-time Transport Protocol (CRTP) compress?
   a. RTP headers
   b. RTP, TCP, and IP headers
   c. RTP, User Datagram Protocol (UDP), and IP headers
   d. Real-time Transport Control Protocol (RTCP) headers
8. Which QoS mechanism is recommended for VoIP networks?
   a. Custom queuing
   b. Low-latency queuing (LLQ)
   c. Priority queuing
   d. Switched-based queuing
9. Where is the local loop located?
   a. Between phones and the central office (CO) switch
   b. Between two PBXs
   c. Between the loopback interfaces of two VoIP routers
   d. Between two PSTN switches
10. What is jitter?
   a. The echo caused by mismatched impedance
   b. The loss of packets in the network
   c. The variable delay of received packets
   d. The fixed delay of received packets

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

This chapter covers traditional voice architectures, integrated voice design, and QoS in voice networks. The section "Traditional Voice Architectures" covers the architecture of time-division multiplexing (TDM) voice networks. It also discusses PSTN technologies and limitations.

The section "Integrated Multiservice Networks" covers IP telephony design for Cisco Unified Communications. The "IPT Design" section covers QoS mechanisms used in IPT networks and provides IPT design recommendations.

Traditional Voice Architectures

This section reviews technologies and concepts to help you understand traditional voice networks.

The PSTN is the global public voice network that provides voice services. The PSTN is a variety of networks and services that are in place worldwide; it provides a circuit-switched service using Signaling System 7 (SS7) for out-of-band call provisioning through the network. Central office (CO) switches exchange SS7 messages to place and route voice calls throughout the network. The PSTN uses Time-Division Multiplexing (TDM) facilities for calls within the network. From the CO to the customer premises, the call can be analog, ISDN, or TDM digital. Each call consumes 64 Kbps of bandwidth, called digital service zero (DS0).

PBX and PSTN Switches

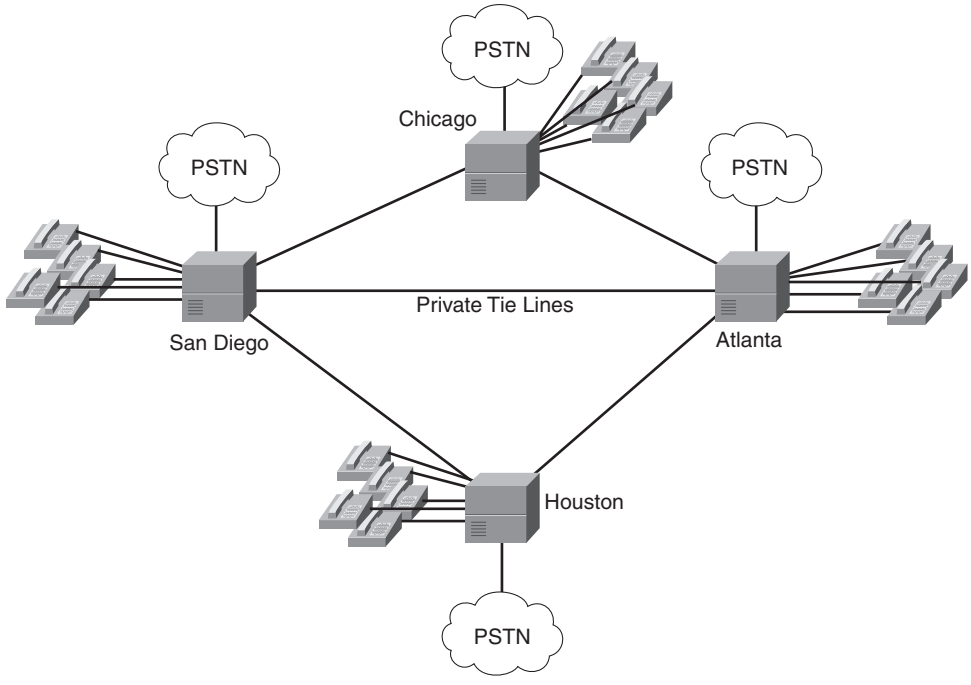
Traditional switches and PBXs route voice using TDM technology and use 64-kbps circuits. The CCDA must understand some of the differences between these devices. The PBX, as its name states, is used in a private network and uses proprietary protocols. The PBX is located in the enterprise's data center. Each PBX may scale up to 1000 phones. Companies deploy PBX networks to obtain enterprise features and to prevent PSTN long-distance charges.

PBXs are customer-owned voice switches. Enterprise companies install and configure their own PBXs to provide telephony service, four-digit dialing, remote-office extensions, voice mail, and private-line routing within other features. Organizations can reduce toll charges by using private tie-lines between their switches. Calls that are placed between offices through the private voice network are called on-net. If a user needs to place a call outside the private network, the call is routed to the local PSTN. If the call is forwarded to the PSTN, it is called off-net.

Figure 15-1 shows a PBX network for an enterprise. Callers use the PBX network when they place calls from San Diego to Chicago, Atlanta, or Houston. The enterprise reduces toll charges by using its private voice network. A separate private network is in place for data traffic. If a user places a

call from San Diego to Los Angeles, it is routed to the PSTN from the San Diego PBX. Then, toll charges are incurred for the call.

Figure 15-1 *PBX Network*



Another issue in the design is the limitation on the number of calls per private line. If the private lines are T1s, they are each limited to carrying 24 concurrent calls at a time. This is because each call takes 64 kbps of bandwidth with the g.711 codec, and 24 calls times 64 kbps/call equals 1.536 Mbps, the bandwidth of a T1.

PSTN switches are not private. They scale up to 100,000 phones and use open standards because they have to communicate with other switches, PBXs, fax machines, and home telephones. PSTN switches normally are located at the CO of the local or interexchange carrier.

Local Loop and Trunks

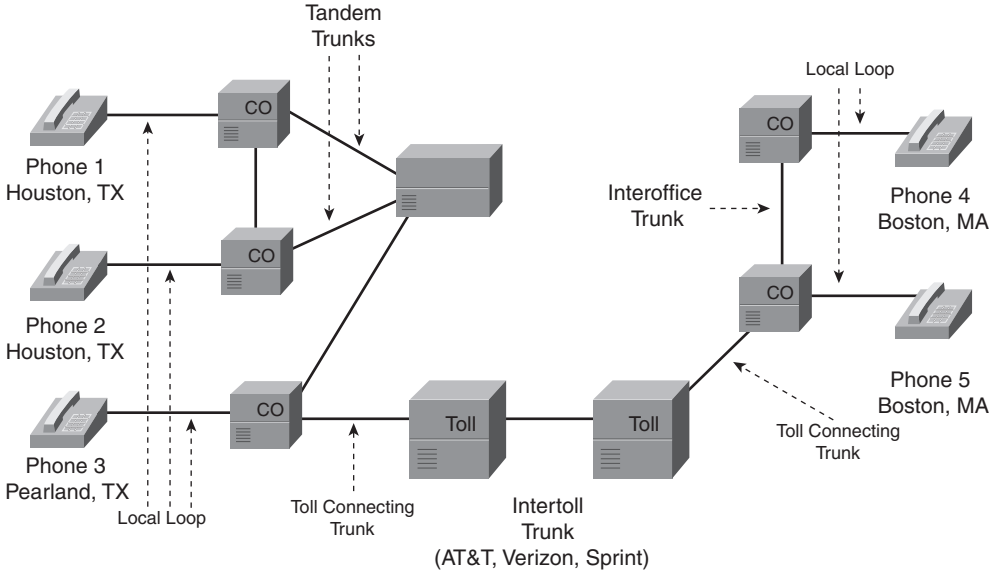
Depending on the dialed digits, a call routes through the local loop, one or more trunks, and the destination local loop to reach the destination phone. The local loop is the pair of wires that runs from the CO to the home or business office.

Trunks connect two switches. The type of trunk depends on the function of the switches the trunk is connecting. The term *tie-line* is frequently used instead of *trunk* to describe a dedicated line connecting two telephone switches within a single organization. The following is a list of trunk types:

- **Interoffice trunk** connects two CO switches. Also called a PSTN switch trunk.
- **Tandem trunk** connects central offices within a geographic area.
- **Toll-connecting trunk** connects the CO to the long-distance office.
- **Intertoll trunk** connects two long-distance offices.
- **Tie trunk** connects two PBXs. Also called a private trunk.
- **PBX-to-CO trunk or CO-to-PBX business line** connects the CO switch to the enterprise PBX.

Figure 15-2 shows an example of the PSTN. All phones connect to their local CO via the local loop. Calls between Phones 1 and 2 and between Phones 4 and 5 go through interoffice trunks. Calls between Phones 2 and 3 go through tandem trunks within a region. When you place calls between Texas and Massachusetts, they are forwarded to the long-distance toll provider via a toll-connecting trunk and are routed through intertoll trunks.

Figure 15-2 *Local Loops and Trunks*



Ports

You can use several ports to connect to voice end stations (phones) and private voice switches:

- **Foreign Exchange Station (FXS)** connects to an end device such as an analog phone or fax machine. It provides line power, dial tone, and ring voltage.
- **Foreign Exchange Office (FXO)** connects to the PSTN. It is an RJ-11 connector that allows an analog connection to be directed to the PSTN's central office or to a station interface on a PBX. The FXO sits on the switch end of the connection. It plugs directly into the line side of the switch, so the switch thinks the FXO interface is a telephone.
- **Ear and Mouth (E&M)** connects private switches. It is an analog trunk used to connect to a voice switch; it supports tie-line facilities or signaling between phone switches. E&M can be connected with two-wire and four-wire. E&M is also called Earth and Magnet.
- **Channelized T1 (or E1)** is commonly used as a digital trunk line to connect to a phone switch where each DS0 supports an active phone call connection. Provides 24 (for T1) or 32 (for E1) channels or DS0 for voice calls. The total bandwidth for a T1 is 1.536 Mbps, and the total bandwidth for an E1 is 2.048 Mbps.
- **ISDN Primary Rate Interface (PRI)** is a digital trunk link used to connect to a phone switch. A separate channel is used for common channel-signaling messages. T1 PRIs provide 23 channels for voice, and E1 PRIs provide 30 channels for voice.

Major Analog and Digital Signaling Types

Signaling is needed to provide the state of telephones, digit dialing, and other information. For a call to be placed, managed, and closed, all of the following signaling categories have to occur:

- **Supervisory** provides call control and phone state (on-hook and off-hook).
- **Addressing** provides dialed digits.
- **Informational** provides information such as dial and busy tones and progress indicators.

These different signaling categories are provided by analog and digital signaling types.

The signaling type depends on the type of connection. The major areas are

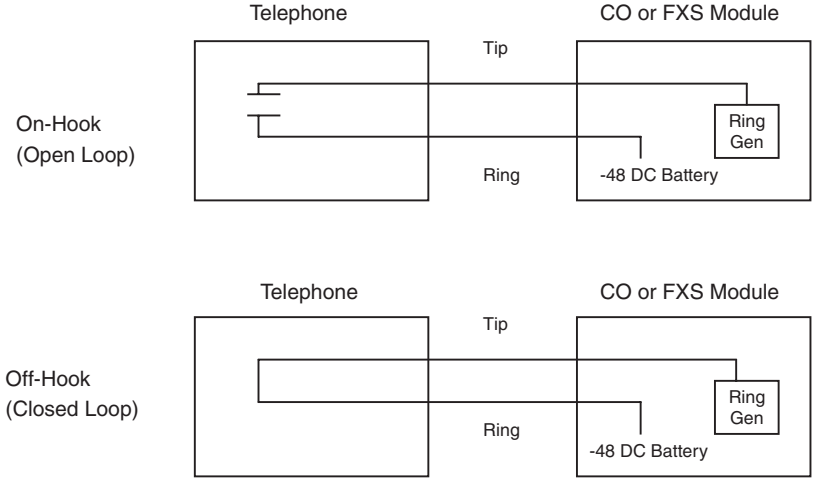
- CO to phone (loop and ground start signaling)
- PBX to PBX (E&M)
- T1/E1 Channel Associated Signaling (CAS)
- ISDN PRI Common Channel Signaling (CCS)

- Q Signaling (Q.SIG)
- SS7 interswitch PSTN signaling

Loop-Start Signaling

Loop-start signaling is an analog signaling technique used to indicate on-hook and off-hook conditions in the network. It is commonly used between the telephone set and the CO, PBX, or FXS module. As shown in Figure 15-3, with loop-start the local loop is open when the phone is on-hook. When the phone is taken off-hook, a –48 direct current (DC) voltage loops from the CO through the phone and back. Loop-start signaling is used for residential lines.

Figure 15-3 *Loop-Start Signaling*

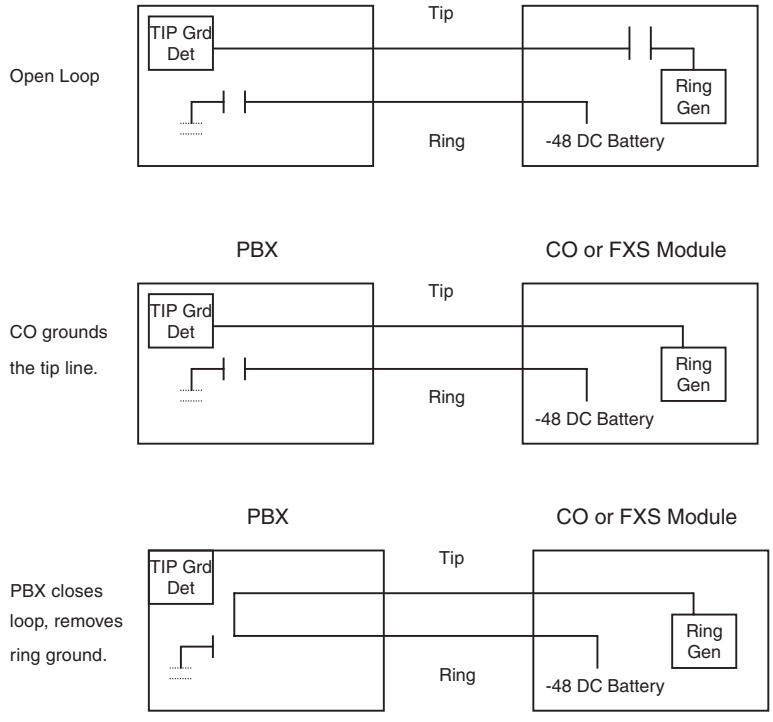


Ground-Start Signaling

Ground-start signaling is an analog signaling technique used to indicate on-hook and off-hook conditions. Ground-start is commonly used in switch-to-switch connections. The difference between ground-start and loop-start is that ground-start requires the closing of the loop at both locations. Ground-start is commonly used by PBXs.

The standard way to transport voice between two telephone sets is to use tip and ring lines. Tip and ring lines are the twisted pair of wires that connect to your phone via an RJ-11 connector. As shown in Figure 15-4, the CO switch grounds the tip line. The PBX detects that the tip line is grounded and closes the loop by removing ground from the ring line.

Figure 15-4 *Ground-Start Signaling*



E&M Signaling

E&M is an analog signaling technique often used in PBX-to-PBX tie-lines. E&M is receive and transmit, or more commonly called ear and mouth. Cisco routers support four E&M signal types: Type I, Type II, Type III, and Type V. Types I and II are most popular on the American continents. Type V is used in the United States and Europe.

There are also three forms of E&M dial supervision signaling to seize the E&M trunk:

- **Immediate start**—This is the most basic protocol. In this technique, the originating switch goes off-hook, waits for a finite period of time (for example, 200 ms), and then sends the dial digits without regard for the far end.
- **Wink start**—Wink is the most commonly used protocol. In this technique, the originating switch goes off-hook, waits for a temporary off-hook pulse from the other end (which is interpreted as an indication to proceed), and then sends the dial digits.
- **Delay dial**—In this technique, the originating side goes off-hook, waits for about 200 ms, and then checks whether the far end is on-hook. If the far end is on-hook, it outputs dial digits. If the far end is off-hook, it waits until it goes on-hook and then outputs dial digits.

CAS and CCS Signaling

Digital signaling has two major forms: Channel Associated Signaling (CAS) and Common Channel Signaling (CCS). The major difference is that with CAS the signaling is included in the same channel as the voice call. With CCS the signaling is provided in a separate channel. Table 15-2 shows the common types of CAS and CCS. They are covered in the following sections.

Table 15-2 *Common CAS and CCS Signaling Types*

From	Signaling Type
CAS	T1 or E1 signaling DTMF
CCS	ISDN PRI or BRI QSIG SS7

T1/E1 CAS

Digital T1 CAS uses selected bits within a selected channel to transmit signaling information. CAS is also called robbed-bit signaling or in-band signaling in the T1 implementation. Robbed-bit CAS works with digital voice because losing an occasional voice sample does not affect the voice quality. The disadvantage of robbed-bit CAS is that it cannot be used on channels that might carry voice or data without reducing the data rate to 56 Kbps to ensure that signaling changes do not damage the data stream.

E1 CAS uses a separate channel in the shared medium for CAS, so it does not have this disadvantage. The E1 signaling bits are channel-associated, but they are not in-band.

ISDN PRI/BRI

ISDN T1 PRI provides 23 64-kbps B (bearer) channels for voice, with a separate 64-kbps D (data signaling) channel for signaling. The ISDN E1 PRI provides 30 B channels. The use of messages in a separate channel, rather than preassigned bits, is also called common-channel signaling. Any bit in the signaling channel is common to all the channels sharing the medium rather than dedicated to a particular single channel. ISDN provides the advantage of not changing bits in the channels and thus is useful for data traffic in addition to voice traffic.

The ISDN BRI interface includes two 64-kbps B channels for voice or data and a separate 16-kbps D channel that provides signaling for the interface.

Q.SIG

Q.SIG is the preferred signaling protocol used between PBX switches. It is a standards-based protocol, based on ISDN, that provides services. It is feature-transparent between PBXs. It is

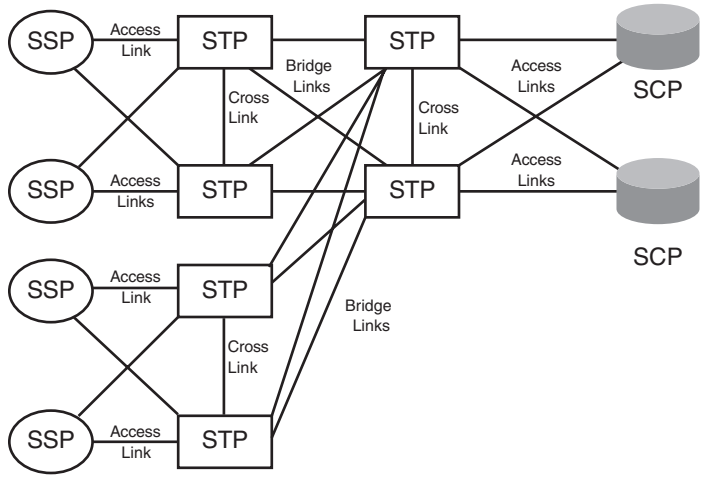
interoperable with public and private ISDN networks and provides no restrictions to private dial plans. QSIG is also used between Cisco's Unified CallManager and enterprise PBX in hybrid implementations.

SS7

SS7 is a global ITU standard for telecommunications control that allows voice-network calls to be routed and controlled by call-control centers. SS7 is used between PSTN switches. SS7 implements call setup, routing, and control, ensuring that intermediate and far-end switches are available when a call is placed. With SS7, telephone companies can implement modern consumer-telephone services such as caller ID, toll-free numbers, call forwarding, and so on.

SS7 provides mechanisms for exchanging control, status, and routing messages on public telephone networks. SS7 messages pass over a separate channel than that used for voice communication. You use Common Channel Signaling 7 (CCS7) when speaking about SS7 signaling. CCS7 controls call signaling, routing, and connections between CO, interexchange carrier, and competitive local exchange carrier switches. Figure 15-5 shows the connectivity between SS7 components.

Figure 15-5 *SS7 Signaling Components*



As shown in Figure 15-5, SS7 has the following system components:

- **Signaling Control Point (SCP)**—Databases that provide the necessary information for special call processing and routing, including 800 and 900 call services, credit-card calls, local number portability, cellular roaming services, and advanced call-center applications.

- **Signaling Transfer Point (STP)**—Receives and routes incoming signaling messages toward their destinations. STPs are deployed in mated pairs and share the traffic between them.
- **Signaling Switching Point (SSP)**—Telephone switches equipped with SS7 software and signaling links. Each SSP is connected to both STPs in a mated pair.

Addressing Digit Signaling

There are two methods for submitting analog address digits to place a call:

- Pulse or rotary dialing
- Dual-tone multifrequency (DTMF) dialing

Pulse dialing uses the opening and closing of a switch at the telephone set. A rotary register at the CO detects the opening and closing of the loop. When the number 5 is dialed on a rotary phone, the dial mechanism opens and closes five times, each one-tenth of a second apart.

DTMF uses two tones simultaneously to indicate the dialed number. Table 15-3 shows the phone keypad and the frequencies used. For example, when the number 5 is dialed, the frequencies 770 Hz and 1336 Hz are sent to the CO.

Table 15-3 *DTMF Frequencies*

Frequency	1209 Hz	1336 Hz	1477 Hz
697 Hz	1	ABC 2	DEF 3
770 Hz	GHI 4	JKL 5	MNO 6
852 Hz	PRS 7	TUV 8	WXY 9
941 Hz	*	OPER 0	#

PSTN Numbering Plan

The PSTN uses the ITU E.164 standard for public network addressing. The E.164 standard uses a maximum of 15 digits and makes each phone unique in the PSTN. Examples of E.164 addresses are the residential, business, IP phones, and cell phones that you use every day. Each country is

assigned a country code to identify it. The country codes can be one to three digits in length. Table 15-4 shows some examples of country codes.

Table 15-4 *E.164 Country Codes*

Country Code	Country
1	United States, Canada
1-787, 1-939	Puerto Rico
55	Brazil
39	Italy
86	China
20	Egypt
91	India
49	Germany
380	Ukraine
44	United Kingdom
81	Japan
52	Mexico
966	Saudi Arabia

The ITU website that lists country codes is located at http://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_763.html.

Each country divides its network into area codes that identify a geographic region or city. The United States uses the North American Numbering Plan (NANP). NANP has the address format of *NXX-NXX-XXXX*, where *N* is any number from 2 to 9 and *X* is any number from 0 to 9. The first three digits are the area code. The address is further divided into the office code (also known as prefix) and line number. The prefix is three digits, and the line number is four digits. The line number identifies the phone.

An example of a PSTN address in the United States is 1-713-781-0300. The 1 identifies the United States; the 713 identifies an area code in the Houston, Texas, geographical region. The 781 identifies a CO in west Houston. The 0300 identifies the phone.

Another example of a PSTN address is 52-55-8452-1110. The country code 52 identifies the country of Mexico. The area code 55 identifies the geographic area of Mexico City. The office code 8452 and line number 1110 follows.

Other PSTN Services

The PSTN provides a suite of services in addition to call setup and routing:

- Centrex
- Voice mail
- Database services
- Interactive voice response (IVR)
- Automatic call distribution (ACD)

Centrex Services

Companies can use the local phone company to handle all their internal and external calls from the CO. In this voice model, the CO acts as the company's voice switch, with PBX features such as four-digit extension dialing, voice mail, and call holds and transfers. The Centrex service gives the company the appearance of having its own PBX network.

Voice Mail

PSTN service providers can enable voice messaging for customers that request the service. Voice mail provides automated call answering and message recording. Users can then retrieve the message and forward it to other extensions.

Database Services

The PSTN must keep call detail records (CDR) in the database systems. CDR information includes all types of call information, such as called party, caller, time, duration, locations, and user service plans. This information is used for billing and reporting.

IVR

IVR systems connect incoming calls to an audio playback system. IVR queues the calls, provides prerecorded announcements, prompts the caller for key options, provides the caller with information, and transfers the call to another switch extension or agent. IVR is used in customer call centers run by companies in all industries to gather and provide information to the customers before transferring them to agents.

ACD

ACD routes calls to a group of agents. ACD keeps statistics on each agent, such as the number of calls and their duration. Based on the statistics, the ACD system then can evenly distribute the calls to the agents or to the appropriate agent skill group. ACD is used by airline reservation systems, customer service departments, and other call centers.

Voice Terminology

You must consider voice traffic requirements when designing a network. The CCDA must be familiar with the following voice engineering terms.

Grade of Service

Grade of service (GoS) is the probability that a call will be blocked when attempting to seize a circuit. If it is determined that a network has a P.02 GoS, the probability is that 2 percent of all attempted calls will be blocked.

Erlangs

An Erlang is a telecommunications traffic unit of measurement representing the continuous use of one voice path for one hour. This means the use of a single voice resource for one hour (3600 seconds). It describes the total traffic volume of one hour. Erlangs determine voice-call usage for bandwidth requirements for voice network designs, including VoIP. It helps determine if a system has been provisioned with enough resources.

If a group of users makes 20 calls in an hour and each call lasts 10 minutes, the Erlangs are calculated as follows:

20 calls per hour * 10 minutes per call = 200 minutes per hour

traffic volume = (200 minutes per hour) / (60 minutes per hour)
= 3.33 Erlangs

There are three common Erlang models:

- **Erlang B** assumes that a blocked call is blocked, not delayed. It is the most common model used.
- **Extended Erlang B** adds a "retry" percentage to the Erlang B model. It assumes that there is an additional load when calls are reattempted after a failed call.
- **Erlang C** assumes that blocked calls are actually delayed. This model is used in call centers where calls are queued for service.

Centum Call Second (CCS)

A Centum Call Second (CCS) represents one call occupying a channel for 100 seconds. It is the equivalent of 1/36th of an Erlang. In other words, 360 CCS equals 1 Erlang (3600 seconds).

Busy Hour

The busy hour is the specific hour within a 24-hour period in which the highest traffic load occurs. Most calls are placed and are of longer durations during this hour. It is also called peak hour.

Busy Hour Traffic (BHT)

BHT is the amount of voice traffic that occurs in the busy hour, expressed in Erlangs. It is calculated by multiplying the average call duration by the number of calls in the hour and then dividing that by 3600.

For example, if 300 calls occurred during the busy hour, with an average duration of 150 seconds, the BHT is calculated as follows:

BHT = (150 seconds * 300 calls per hour) / (3600 seconds per hour)
BHT = 12.5 Erlangs

Blocking Probability

The blocking probability is the probability that a call will be blocked. A blocking probability of 0.02 means that 2 percent of the calls will be blocked.

Call Detail Records

Call detail records include statistical and other information related to all calls placed. Information included in CDRs includes call time, call duration, source phone number, dialed phone number, and the amount billed. For VoIP networks, the CDR may also include source and destination IP addresses.

Integrated Multiservice Networks

The introduction of packet-voice technology allows the convergence of data and voice networks. This lets companies save toll charges on voice telephone calls. It also reduces companies' total cost of ownership by not having to build and operate separate networks for voice, video, and data.

In multiservice networks, digitized (coded) voice is packaged into packets, cells, or frames; sent as data throughout the networks; and converted back to analog voice. The underlying protocols used for these converged services are

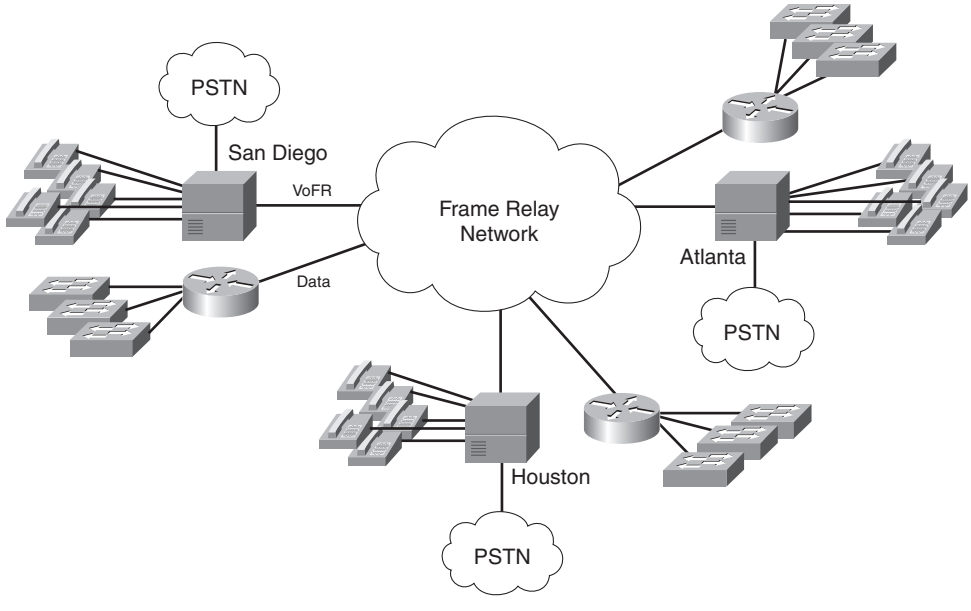
- Voice over Frame Relay (VoFR)
- Voice over Asynchronous Transfer Mode (VoATM)
- Voice over Internet Protocol (VoIP)

Initially, VoFR and VoATM were used but lost ground to VoIP solutions. VoIP is also referred to as IP telephony (IPT) when it is integrated with IP-based signaling and call control. IPT is how almost all new deployments are being implemented.

VoFR

VoFR permits enterprise customers with existing Frame Relay networks to implement packetized voice. Access devices or cards access the Frame Relay network. PBX vendors provide VoFR cards for their switches to support call routing over the Frame Relay network. Figure 15-6 shows three PBXs connected with trunks using VoFR. The PSTN is used for backup if the Frame Relay circuit goes down. The disadvantage of VoFR is that it provides only convergence in the WAN; it still requires local dedicated telephony equipment and networks. It cannot provide convergence to LANs without a network protocol that can span the data link technologies, such as IP.

Figure 15-6 *VoFR Trunks Between PBXs*



One standard for VoFR is Frame Relay Forum (FRF) 11.1. It establishes specifications for call setup, coding types, and packet formats for VoFR service. It provides the basis for interoperability between vendors.

A number of mechanisms can minimize delay and variable delay (jitter) on a Frame Relay network. The presence of long data frames on a low-speed Frame Relay link can cause unacceptable delays for time-sensitive voice frames. To reduce this problem, some vendors implement smaller frame sizes to help reduce delay and delay variation. FRF.12 is an industry-standard approach to doing this, so products from different vendors can interoperate and consumers will know what type of voice quality to expect. To ensure voice quality, you should set the committed information rate (CIR) of each permanent virtual circuit (PVC) to ensure that voice frames are not discarded.

VoATM

VoATM permits enterprise customers to use their existing ATM networks for voice traffic. ATM inherently provides guaranteed QoS for voice traffic that IP protocols alone cannot provide. ATM can provide the service levels and functionality required to support voice traffic for the WAN. For enterprise networks that have ATM, VoATM provides a mechanism to connect enterprise PBXs via ATM and other VoATM applications.

With ATM, constant bit rate (CBR) or variable bit rate–real time (VBR-rt) classes of service (CoS) provide levels of bandwidth and delay guarantees for voice. Chapter 5, "WAN Technologies," covers ATM.

PBX vendors provide VoATM cards for their switches to support call routing over the Frame Relay network. Figure 15-7 shows three PBXs that are connected via trunks using VoATM. The PSTN is used for backup if the ATM circuit goes down. As with VoFR, the disadvantage of VoATM is that it provides only convergence in the WAN. It cannot provide convergence within the LAN without a network protocol that can span the data link technologies, such as IP.

VoIP

VoIP provides transport of voice over the IP protocol family. IP makes voice globally available regardless of the data link protocol in use (Ethernet, ATM, Frame Relay). With VoIP, enterprises do not have to build separate voice and data networks. Integrating voice and data into a single converged network reduces the costs of owning and managing separate networks.

Figure 15-8 shows a company that has separate voice and data networks. Phones connect to local PBXs, and the PBXs are connected using TDM trunks. Off-net calls are routed to the PSTN. The data network uses LAN switches connected to WAN routers. The WAN for data uses Frame Relay.

Separate operations and management systems are required for these networks. Each system has its corresponding monthly WAN charges and personnel, resulting in additional costs.

Figure 15-7 *VoATM Trunks Between PBXs*

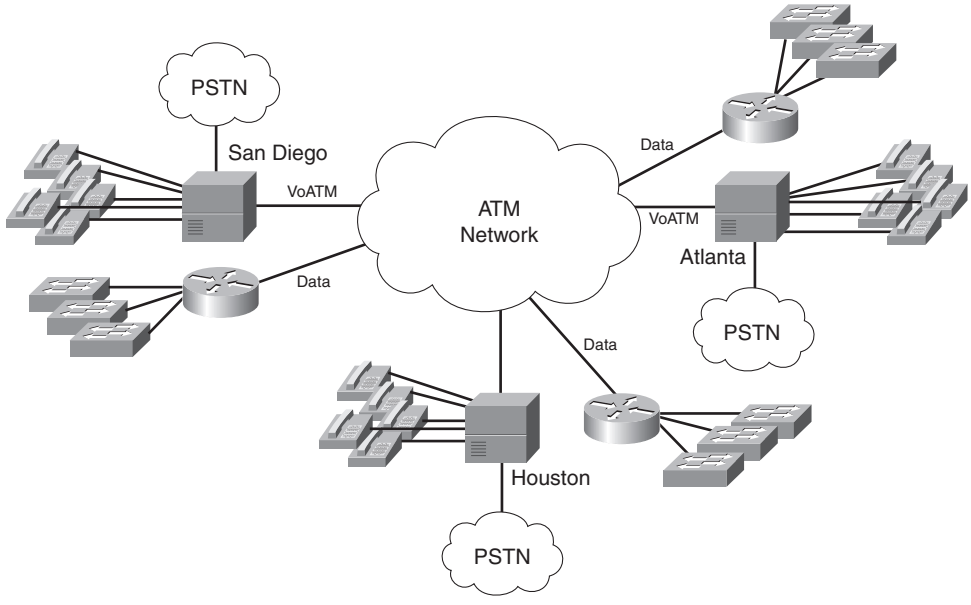
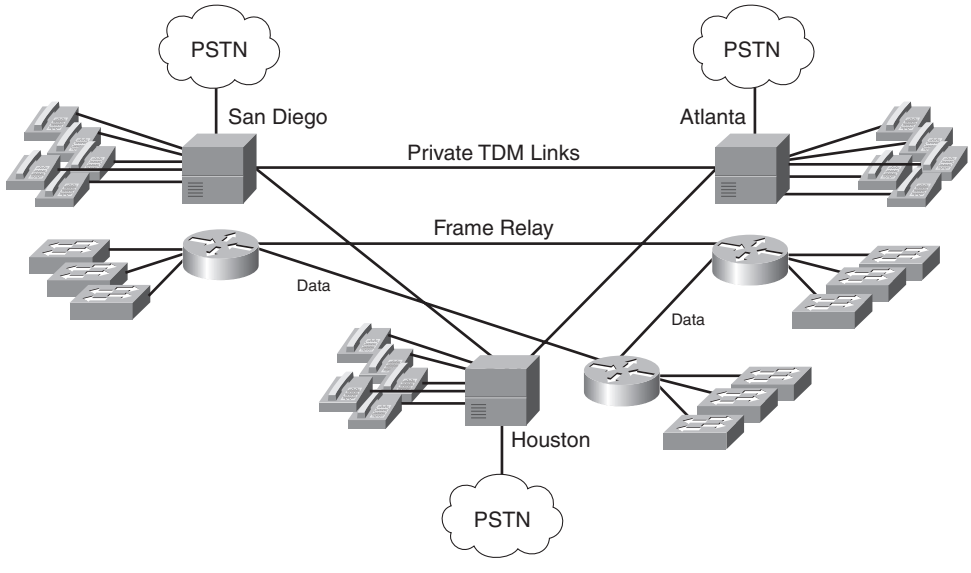
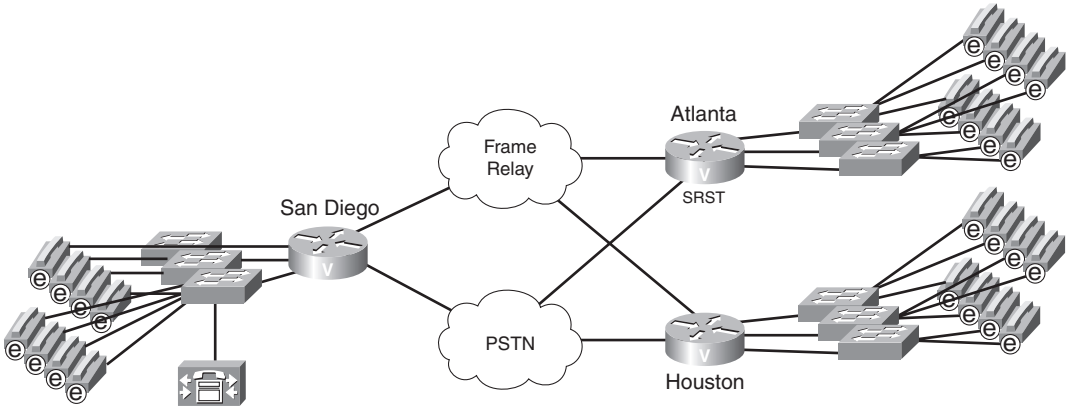


Figure 15-8 *Separate Voice and Data Networks*



With IP telephony, you can reduce the number of systems, circuits, and support personnel. Figure 15-9 shows a multiservice IP telephony network that employs Ethernet-based phones with server-based call processing with gateway routers. Survivable Remote Site Telephony (SRST) is used for failover or backup to the PSTN if WAN failure occurs. On-net calls travel through the Frame Relay network, and off-net calls are forwarded to the PSTN. The PSTN link is also used if voice overflow or congestion occurs on the WAN network. Calls are then routed to the PSTN.

Figure 15-9 *Converged VoIP Network*



IPT Components

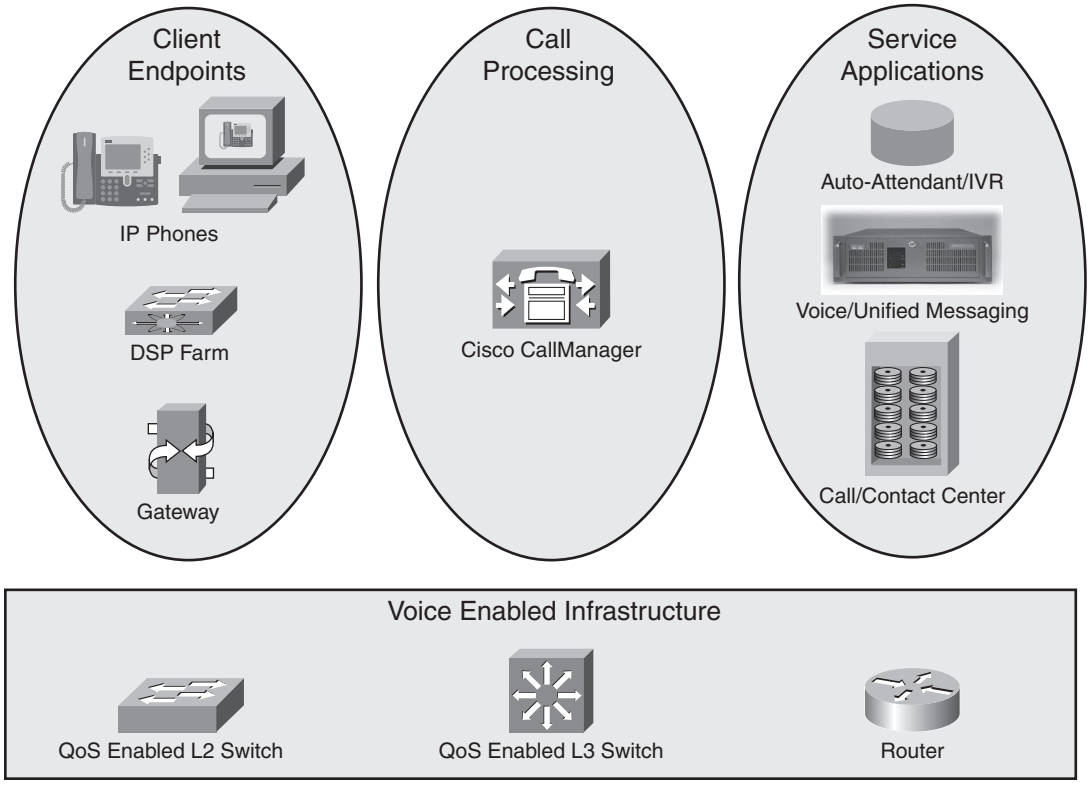
Cisco's IPT architecture divides voice system architectures into four major functional areas, as shown in Figure 15-10:

- Client endpoints
- Call processing
- Service applications
- Voice Enabled Infrastructure

Client endpoints include the IP phones, analog and digital gateways, and digital signal processor (DSP) farms. Included here is Cisco's IP Communicator, which is the software-based IP phone that runs on a PC or laptop. Gateways are used to access PBXs, analog phones, other IP telephony deployments, or the PSTN.

The Cisco Unified CallManager (CM) fulfills the role of call processing. The CM servers are the "brains" of the voice dial plan and are used to establish IPT calls between IP phones.

Figure 15-10 *Cisco IPT Functional Areas*



Service applications include IVR, Auto Attendant, and Unity Unified Messaging System for voice mail. Cisco IP Contact Center (IPCC) is used for enterprise call center applications. In addition, a standards-based Telephony Application Programming Interface (TAPI) allows third-party companies to develop applications for the Cisco Unified CallManager.

The voice-enabled infrastructure includes QoS-enabled devices such as LAN switches and routers. These devices are configured to be IPT-aware and provide service guarantees to the VoIP traffic. For example, LAN switches are configured with voice VLANs and Power over Ethernet (PoE) to service the IP phones. Also, WAN routers are configured with queuing techniques to prioritize VoIP streams over other traffic types.

Design Goals of IP Telephony

The overall goal of IP telephony is to replace traditional TDM-based telephony by deploying IPT components on existing IP networks. IPT should be highly available and as reliable as existing voice networks. IPT should provide greater flexibility and productivity while providing lower cost

of ownership by using a converged network. IPT also allows third-party software providers to develop new applications for IP phones.

IPT Deployment Models

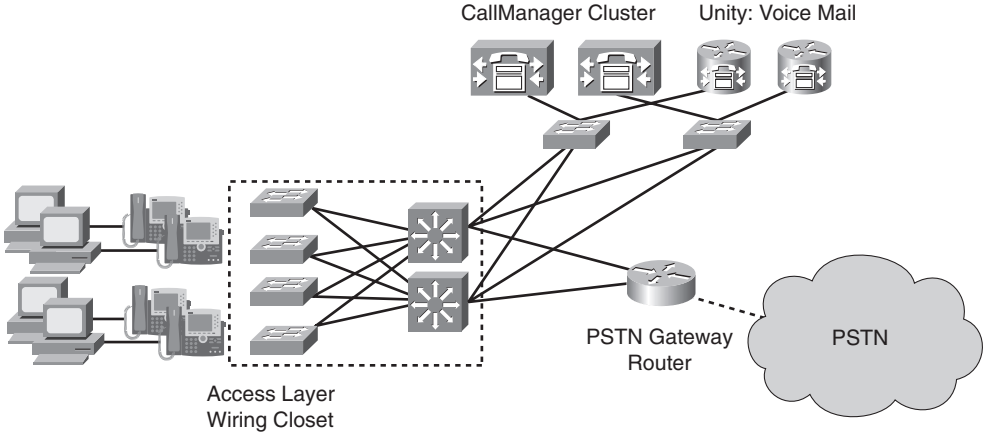
This section covers the Cisco IPT call-processing deployment models:

- Single-site deployment
- Multisite centralized WAN call processing
- Multisite distributed WAN call processing
- CallManager Express deployment

Single-Site Deployment

The single-site deployment model, shown in Figure 15-11, is a solution for enterprises located in a single large building or campus area with no voice on the WAN links. There are no remote sites.

Figure 15-11 *Single-Site Deployment Model*

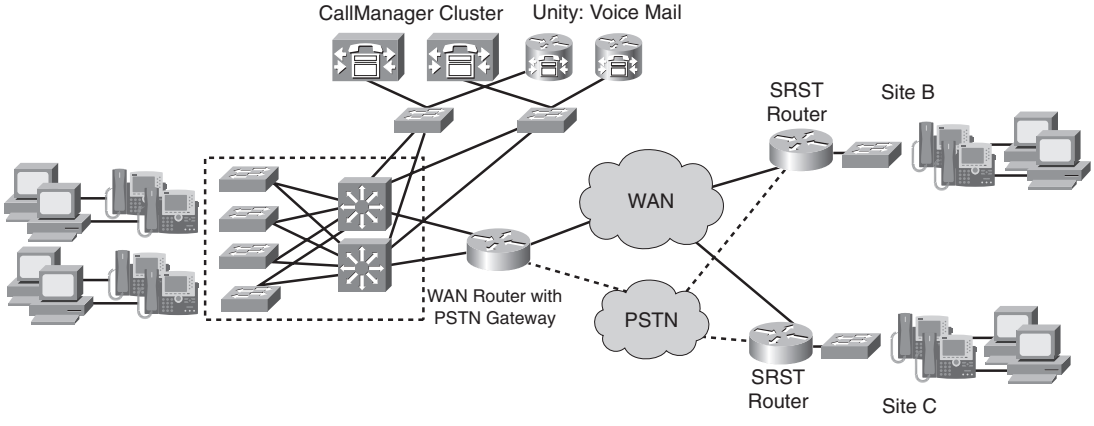


A single CM cluster is deployed for redundancy in the server farm, and Unity is used for voice mail, with or without unified messaging. IP phones are deployed on PoE LAN switches. The Cisco Unified CM supports up to 30,000 IP devices in a cluster. Gateway routers are procured with PRI cards to connect to the enterprise PBX (during migration) or the PSTN.

Multisite Centralized WAN Call-Processing Model

The centralized WAN call-processing model is a solution for medium enterprises with one large location and many remote sites. Figure 15-12 shows the centralized call-processing model. A CM cluster with multiple servers is deployed for redundancy at the large site. Call processing and voice mail servers are located in only the main site. Remote-site IP phones register to the CM cluster located in the main site. PoE switches are used to power all IP phones. Remote sites use voice-enabled gateway routers with SRST for redundancy.

Figure 15-12 *Multisite Centralized WAN CM Deployment Model*



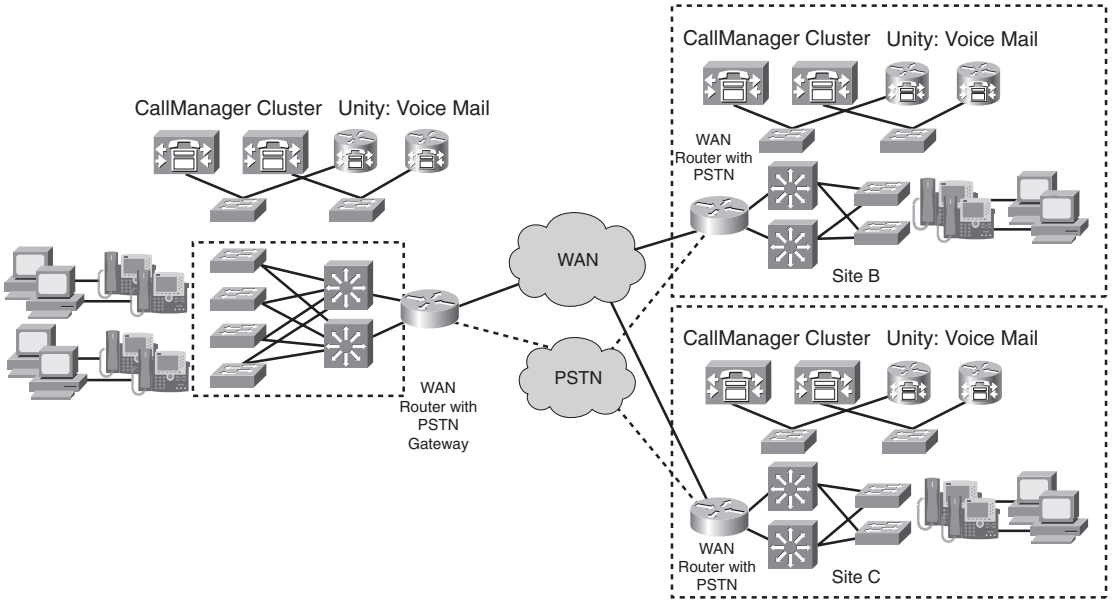
On the WAN, QoS features are configured to prioritize the VoIP packets over other packet types. In the event of WAN failure, SRST configured routers forward calls through the PSTN. The PSTN circuit can be used for local inbound and outbound calls at the remote site. In this model, call admission control (CAC) is configured to impose a limit on the number of on-net calls permitted between sites.

Multisite Distributed WAN Call-Processing Model

The multisite distributed WAN call-processing model is a solution for large enterprises with several large locations. Figure 15-13 shows the distributed WAN model. Up to 30,000 users are supported per CM cluster. Several CM clusters are deployed at the large sites for redundancy, and Unity servers are used for messaging. Intercluster trucks are created to establish communication between clusters. IP phones are deployed on PoE LAN switches.

This model also supports remote sites to be distributed off the large sites. CAC between the CM and Cisco IOS gateway with gatekeeper (GK) is supported. Also, this model supports multiple WAN codecs. Compression of VoIP is done between sites.

Figure 15-13 *Multisite Distributed WAN CM Deployment Model*



Unified CallManager Express Deployments

Cisco provides Express versions of its CallManager, Unity, and IPCC solutions that are installed in a router. CallManager Express (CME) provides the call processing capabilities of CM on a router. Unity Express and IPCC Express also provide the same services on the router. CME deployments support up to 240 Cisco IP phones. It is a lower-cost solution for small branch offices.

Codecs

Because speech is an analog signal, it must be converted into digital signals for transmission over digital systems. The first basic modulation and coding technique was Pulse Code Modulation (PCM). The international standard for PCM is G.711. With PCM, analog speech is sampled 8000 times a second. Each speech sample is mapped onto 8 bits. Thus, PCM produces (8000 samples per second) * (8 bits per sample) = 64,000 bits per second = 64-kbps coded bit rate. Other coding schemes have been developed to further compress the data representation of speech. Most voice compression codes, such as G.729, begin with a G.711-coded voice stream.

Analog-to-Digital Signal Conversion

The steps involved in converting from analog-to-digital signaling are filtering, sampling, and digitizing. First, signals over 4000 Hz are filtered out of the analog signal. Second, the signal is sampled at 8000 times per second using Pulse Amplitude Modulation (PAM). Third, the amplitude samples are converted to a binary code.

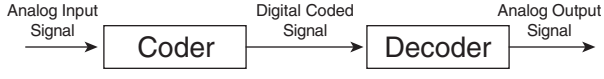
The digitizing process is divided further into two subprocesses:

- **Companding**—This term comes from "compressing and expanding." The analog samples are compressed into logarithmic segments.
- **Quantization and coding**—This process converts the analog value into a distinct value that is assigned a digital value.

Codec Standards

Codecs transform analog signals into a digital bit stream and digital signals back into analog signals. Figure 15-14 shows that an analog signal is digitized with a coder for digital transport. The decoder converts the digital signal into analog form.

Figure 15-14 *Codec*



Each codec provides a certain quality of speech. A measure used to describe the quality of speech is the Mean Opinion Score (MOS). With MOS, a large group of listeners judges the quality of speech from 5 (best) to 1 (bad). The scores are then averaged to provide the MOS for each sample. For example, G.711 has a MOS of 4.1, and G.729 has a MOS of 3.92. The default codec setting for VoIP dial peers in Cisco IOS Software is G.729 (g729r8). Other codec standards are shown in Table 15-5. An explanation of the compression techniques is beyond the scope of the CCDA test.

Table 15-5 *Codec Standards*

Codec	Bit Rate	MOS	Description
G.711u	64 kbps	4.1	PCM. Mu-law version used in North America and Japan. Samples speech 8000 times per second, represented in 8 bits.
G.711a	64 kbps	4.1	PCM. A-law used in Europe and international routes.
G.723.1	6.3 kbps	3.9	Multipulse Excitation–Maximum Likelihood Quantization (MPE-MLQ).
G.723.1	5.3 kbps	3.65	Algebraic Code–Excited Linear Prediction (ACELP).
G.726	16/24/32/40 kbps	3.85	Adaptive Differential Pulse-Code Modulation (AD-PCM).
G.728	16 kbps	3.61	Low-Delay CELP (LDCELP).
G.729	8 kbps	3.92	Conjugate Structure ACELP (CS-ACELP).

VoIP Control and Transport Protocols

You use a number of protocols to set up IP telephony clients and calls and to transport voice packets. Some of the most significant protocols are

- **Dynamic Host Configuration Protocol (DHCP)**—To establish IP configuration parameters
- **Domain Name System (DNS)**—To obtain IP addresses of the Trivial File Transfer Protocol (TFTP) server
- **TFTP**—To obtain configurations
- **Skinny Station Control Protocol (SSCP)**—For call establishment
- **Real-time Transport Protocol (RTP)**—For voice stream (VoIP) station-to-station traffic in an ongoing call
- **Real-time Transport Control Protocol (RTCP)**—For call control
- **Media Gateway Control Protocol (MGCP)**—For call establishment with gateways
- **H.323**—For call establishment with gateways from the ITU
- **Session Initiation Protocol (SIP)**—For call establishment with gateways, defined by the Internet Engineering Task Force (IETF)

DHCP, DNS, and TFTP

IP phones use DHCP to obtain their IP addressing information: IP address, subnet mask, and default gateway. DHCP also provides the IP address of the DNS servers and the name or IP address of the TFTP server. You use TFTP to download the IP phone operating system and configuration. Both DHCP and TFTP run over UDP.

SSCP

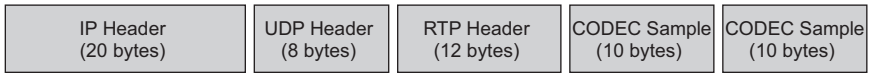
SSCP is a Cisco-proprietary client/server signaling protocol for call setup and control. SSCP runs over TCP. SSCP is called a "skinny" protocol because it uses less overhead than the call-setup protocols used by H.323. IP phones use SSCP to register with CallManager and to establish calls. SSCP is used for VoIP call signaling and for features such as Message Waiting Indicators. This protocol is not used in the voice media streams between IP phones.

RTP and RTCP

In VoIP, RTP transports audio streams. RTP is a transport layer protocol that carries digitized voice in its payload. RTP is defined in RFC 1889. RTP runs over UDP, which has lower delay than TCP. Because of the time sensitivity of voice traffic and the delay incurred in retransmissions, UDP is used instead of TCP. Real-time traffic is carried over UDP ports ranging from 16,384 to 16,624.

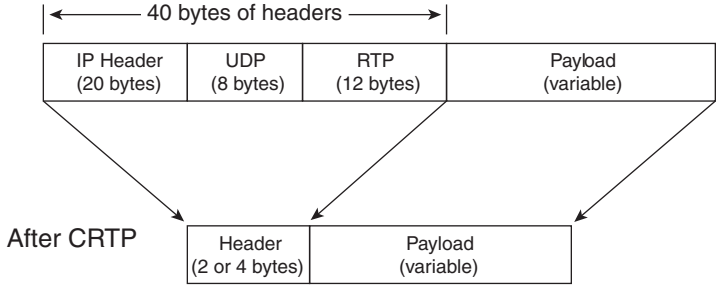
The only requirement is that the RTP data be transported on an even port and that the RTCP data be carried on the next odd port. RTCP is also defined in RFC 1889. RTCP is a session layer protocol that monitors the delivery of data and provides control and identification functions. Figure 15-15 shows a VoIP packet with the IP, UDP, and RTP headers. Notice that the sum of the header lengths is 20 + 8 + 12 = 40 bytes.

Figure 15-15 *IP, UDP, and RTP Headers of a VoIP Packet*



WAN links use RTP header compression to reduce the size of voice packets. This is also called Compressed RTP (CRTP). As shown in Figure 15-16, CRTP reduces the IP/UDP/RTP header from 40 bytes to 2 or 4 bytes—a significant decrease in overhead. CRTP happens on a hop-by-hop basis, with compression and decompression occurring on every link. It must be configured on both ends of the link.

Figure 15-16 *CRTP*



MGCP

MGCP is a client/server signaling protocol used to control gateways in VoIP networks. MGCP is defined in RFC 3435. MGCP's primary function is to control and supervise connection attempts between different media gateways. MGCP gateways handle translation between audio signals and the IP network.

MGCP defines call agents and endpoints. Call agents control the gateways. An endpoint is any gateway interface, such as a PRI trunk or analog interface.

H.323

H.323 is a standard published by the ITU that works as a framework document for multimedia protocols including voice, video, and data conferencing for use over packet-switched networks.

H.323 describes terminals and other entities (such as gatekeepers) to provide multimedia applications. Cisco IOS gateways use H.323 to communicate with Cisco CallManager.

H.323 includes the following elements:

- **Terminals**—Telephones, video phones, and voice mail systems—devices that provide real-time two-way voice.
- **Multipoint Control Units (MCU)**—Responsible for managing multipoint conferences.
- **Gateways**—Composed of a media gateway controller for call signaling and a media gateway to handle media. Provide translation services between H.323 endpoints and non-H.323 devices.
- **Gatekeeper**—Provides call control and signaling services to H.323 endpoints. This function is normally done by an IOS router.

H.323 terminals must support the following standards:

- H.245
- Q.931
- H.225
- RTP/RTCP

H.245 specifies messages for opening and closing channels for media streams and other commands, requests, and indications. It is a conferencing control protocol.

Q.931 is a standard for call signaling used by H.323 within the context of H.225.

H.225 specifies messages for call control, including signaling between endpoints, registration and admissions, and packetization and synchronization of media streams. It performs registration, admission, and status (RAS) signaling for H.323 sessions.

RTP is the transport layer protocol used to transport VoIP packets. RTCP is a session layer protocol.

H.323 includes a series of protocols for multimedia, as shown in Table 15-6.

Table 15-6 *H.323 Protocols*

	Video	Audio	Data	Transport
H.323 protocol	H.261	G.711	T.122	RTP
	H.263	G.722	T.124	H.225
		G.723.1	T.125	H.235
		G.728	T.126	H.245
		G.729	T.127	H.450.1
				H.450.2
				H.450.3
				X.224.0

Gatekeeper Use for Scalability

As a network grows, multiple gateways are placed to communicate with multiple endpoints. Each gateway in a zone needs to be configured with a complete dialing plan. The number of logical connections is calculated with the following formula:

$$L = (N * (N - 1)) / 2$$

where N is the number of gateways in the network.

For example, a network with 7 gateways would have 21 logical connections. With a gatekeeper, simple dial plans are configured on each gateway, and complete dialing is configured on the gatekeeper. This makes network operations and maintenance easier.

SIP

SIP is a protocol defined by the IETF and specified in RFC 2543. It is an alternative multimedia framework to H.323, developed specifically for IP telephony. It is meant to be a replacement to H.323. Cisco now supports SIP on its phones and gateways.

SIP is an application layer control (signaling) protocol for creating, modifying, and terminating Internet multimedia conferences, Internet telephone calls, and multimedia distribution. Communication between members of a session can be via a multicast, a unicast mesh, or a combination.

SIP is designed as part of the overall IETF multimedia data and control architecture that incorporates protocols such as the following:

- Resource Reservation Protocol (RSVP) (RFC 2205) for reserving network resources
- RTP (RFC 1889) for transporting real-time data and providing QoS feedback
- Real-Time Streaming Protocol (RTSP) (RFC 2326) for controlling delivery of streaming media
- Session Announcement Protocol (SAP) (RFC 2974) for advertising multimedia sessions via multicast
- Session Description Protocol (SDP) (RFC 2327) for describing multimedia sessions

SIP supports user mobility by using proxy and redirect servers to redirect requests to the user's current location. Users can register their current locations, and SIP location services provide the location of user agents.

SIP uses a modular architecture that includes the following components:

- **SIP user agent**—Endpoints that create and terminate sessions, SIP phones, SIP PC clients, or gateways
- **SIP proxy server**—Routes messages between SIP user agents
- **SIP redirect server**—Call-control device used to provide routing information to user agents
- **SIP registrar server**—Stores the location of all user agents in the domain or subdomain
- **SIP location services**—Provide logical location of user agents; used by the proxy, redirect, and registrar servers
- **Back-to-back user agent**—Call-control device that allows centralized control of network call flows

IPT Design

This section covers network design issues and solutions that a designer needs to be aware of when designing a network for IPT. Topics such as bandwidth requirements, delay, and QoS schemes should be considered.

Bandwidth

VoIP calls need to meet bandwidth and delay parameters. The amount of bandwidth required depends on the codec used, the Layer 2 protocols, and whether VAD is enabled. For the purpose of call control, you can use the following bandwidth requirements for VoIP design:

- G.729 calls use 26 kbps
- G.711 calls use 80 kbps

When you're designing for VoIP networks, the total bandwidth for voice, data, and video should not exceed 75 percent sustained of the provisioned link capacity during peak times. Use the following formula to provision interface speeds:

> link capacity = [required bandwidth for voice] + [required bandwidth for video] + [required bandwidth for data]

The remaining bandwidth is used by routing, multicast, and management protocols.

NOTE G.729 is the recommended codec for calls over the WAN because of its lower bandwidth requirements and higher Mean Opinion Score.

VAD

As we listen and pause between sentences, typical voice conversations can contain up to 60 percent silence in each direction. In circuit-switched telephone networks, all voice calls use fixed-bandwidth 64-kbps links regardless of how much of the conversation is speech and how much is silence. In multiservice networks, all conversation and silence is packetized. Using Voice Activity Detection (VAD), you can suppress packets of silence. Silence suppression at the source IP telephone or VoIP gateway increases the number of calls or data volumes that can be carried over the links, more effectively utilizing network bandwidth. Bandwidth savings are at least 35 percent in conservative estimates. VAD is enabled by default for all VoIP calls.

Table 15-7 shows how much bandwidth is required based on different parameters. Notice that for G.729, bandwidth is reduced from 26.4 kbps to 17.2 kbps with VAD and to 7.3 kbps with VAD and CRTP enabled.

Table 15-7 *VoIP Bandwidth Requirements with CRTP and VAD*

Technique Codec Bit Rate (kbps)	Payload Size (Bytes)	Bandwidth Multilink PPP (MLP) or FRF.12 (kbps)	Bandwidth with CRTP MLP or FRF.12 (kbps)	Bandwidth with VAD MLP or FRF.12 (kbps)	Bandwidth with CRTP and VAD MLP or FRF.12 (kbps)
G.711 (64)	240	76	66	50	43
G.711 (64)	160 (default)	83	68	54	44
G.726 (32)	120	44	34	29	22
G.726 (32)	80 (default)	50	35	33	23
G.726 (24)	80	38	27	25	17
G.726 (24)	60 (default)	42	27	27	18
G.728 (16)	80	25	18	17	12
G.728 (16)	40 (default)	35	19	23	13
G.729 (8)	40	17.2	9.6	11.2	6.3
G.729 (8)	20 (default)	26.4	11.2	17.2	7.3
G.723.1 (6.3)	48	12.3	7.4	8.0	4.8
G.723.1 (6.3)	24 (default)	18.4	8.4	12.0	5.5
G.723.1 (5.3)	40	11.4	6.4	7.4	4.1
G.723.1 (5.3)	20 (default)	17.5	7.4	11.4	4.8

Cisco has developed a tool, available on its website, that can be used to obtain accurate estimates for IPT design. It also adds an additional 5 percent for signaling overhead. The tool is the Voice Codec Bandwidth Calculator and it is available at http://tools.cisco.com/Support/VBC/do/CodecCalc1.do.

Delay Components

The ITU's G.114 recommendation specifies that the one-way delay between endpoints should not exceed 150 ms to be acceptable commercial voice quality. In private networks, somewhat longer delays might be acceptable for economic reasons. Delay components are one of two major types: fixed delay and variable delay.

Fixed delay includes

- Propagation delay
- Processing delay

- Serialization delay
- Dejitter delay

Propagation delay is how long it takes a packet to travel between two points. It is based on the distance between the two endpoints. You cannot overcome this delay component. The speed of light is the theoretical limit. A reasonable planning figure is approximately 10 ms per 1000 miles, or 6 ms per 1000 km. This figure allows for media degradation and devices internal to the transport network. Propagation delay is noticeable on satellite links.

Processing delay includes coding, compression, decoding, and decompression delays. G.729 has a delay of 15 ms, and G.711 PCM has a delay of 0.75 ms. The delay created by packetization is also a processing delay. Packetization delay occurs in the process of waiting for a number of digital voice samples before sending out a packet.

Serialization delay is how long it takes to place bits on the circuit. Faster circuits have less serialization delay. Serialization delay is calculated with the following formula:

serialization delay = frame size in bits / link bandwidth in bps

A 1500-byte packet takes (1500 * 8) / 64,000 = 187 ms of serialization delay on a 64 Kbps circuit. If the circuit is increased to 512 kbps, the serialization delay changes to (1500 * 8) / 512,000 = 23.4 ms. Data-link fragmentation using Link Fragmentation and Interleaving (LFI) or FRF.12 mechanisms reduces the serialization delay by reducing the size of the larger data packets. This arrangement reduces the delay experienced by voice packets as data packet fragments are serialized and voice packets are interleaved between the fragments. A reasonable design goal is to keep the serialization delay experienced by the largest packets or fragments on the order of 10 ms at any interface.

Packets can take different, redundant paths to reach the destination. Packets might not arrive at a constant rate because they take different paths, and they might experience congestion in the network. This variable delay is called jitter. The receiving end uses dejitter buffers to smooth out the variable delay of received VoIP packets. Dejitter buffers change the variable delay to fixed delay.

The variable-delay component includes queuing delay. As packets cross a network, they pass through several devices. At every output port of these devices, it is possible that other voice and data traffic is sharing the link. Queuing delay is the delay experienced as a result of other traffic sharing the link. It is the sum of the serialization delays of all the packets scheduled ahead of delayed packets. LFI is used as a solution for queuing delay issues. LFI is covered in the next section.

As the traffic load on a network increases, both the probability of delay and the length of the probable delay increase. The actual queuing delay depends on the number of queues, queue lengths, and queue algorithms. Queuing effects in VoIP networks are covered in the next section.

QoS Mechanisms for VoIP Networks

Cisco provides different QoS tools that you should use on edge and backbone routers to support VoIP networks. This section covers several QoS mechanisms and their impact on VoIP networks:

- CRTP
- LFI
- Priority Queue-WFQ (PQ-WFQ)
- LLQ
- Auto QoS

CRTP

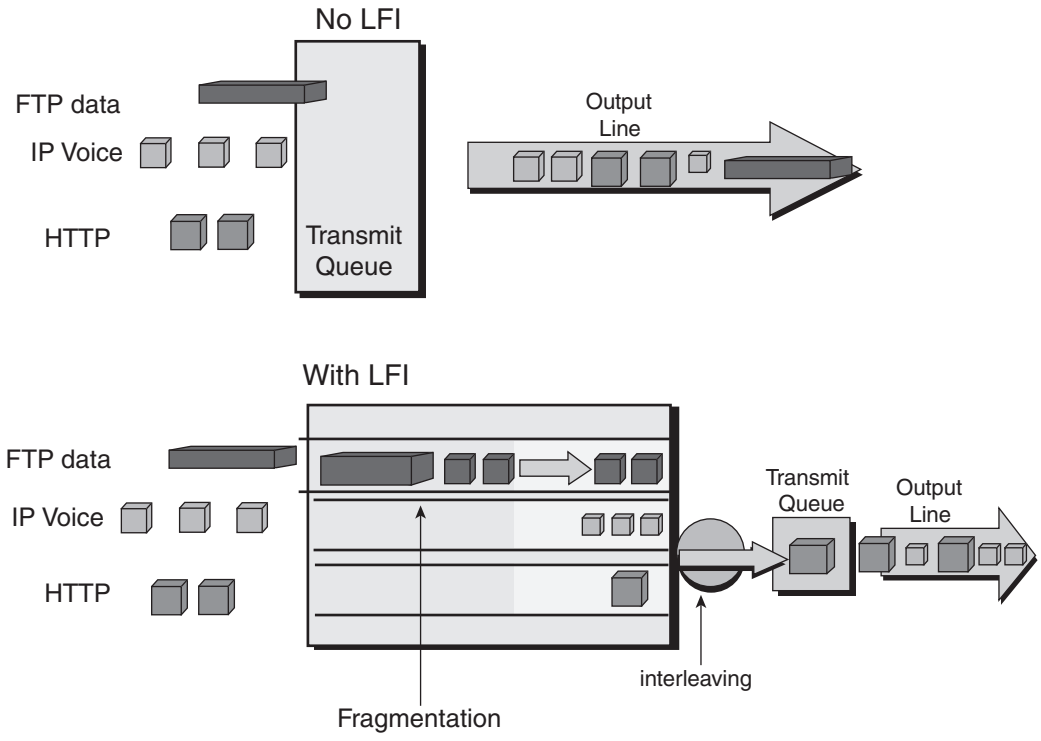
CRTP was covered in an earlier section. It compresses the IP/UDP/RTP headers from 40 bytes to 2 or 4 bytes. It is configured on a link-to-link basis. Cisco recommends using CRTP for links lower than 768 kbps. Do not configure CRTP if the router CPU is above 75 percent utilization.

LFI

LFI is a QoS mechanism used to reduce the serialization delay. In a multiservice network, small VoIP packets have to compete with large data traffic packets for outbound interfaces. If the large data packet arrives at the interface first, the VoIP packet has to wait until the large data packet is serialized. When the large packet is fragmented into smaller packets, the VoIP packets can be interleaved between the data packets. Figure 15-17 shows how LFI works. With no LFI, all VoIP packets and other small packets must wait for the FTP data to be transmitted. With LFI, the FTP data packet is fragmented. The queuing mechanism then can interleave the VoIP packets with the other packets and send them out the interface.

FRF.12 is a fragmentation and interleaving mechanism specific to Frame Relay networks. It is configured on Frame Relay PVCs to fragment large data packets into smaller packets and interleave them with VoIP packets. This process reduces the serialization delay caused by larger packets.

Figure 15-17 *LFI*



PQ-WFQ

PQ-WFQ is also called IP RTP priority. PQ-WFQ adds a single priority queue to WFQ. The priority queue is used for VoIP packets. All other traffic is queued based on the WFQ algorithm. One variation of PQ-WFQ is Frame Relay RTP priority, which allows strict priority for RTP traffic on Frame Relay PVCs.

With IP RTP priority, the router places VoIP RTP packets in a strict priority queue that is always serviced first. All other (data) traffic is serviced by WFQ. If there is no need for differentiated CoS for data traffic, use IP RTP priority instead of LLQ. If you require differentiated CoS for data traffic, use LLQ.

LLQ

LLQ is also known as Priority Queuing–Class-Based Weighted Fair Queuing (PQ-CBWFQ). LLQ provides a single priority queue, as does PQ-WFQ, but it's preferred for VoIP networks because it can also configure guaranteed bandwidth for different classes of traffic. For example, all voice call traffic would be assigned to the priority queue, VoIP signaling and video would be assigned to a

traffic class, FTP traffic would be assigned to a low-priority traffic class, and all other traffic would be assigned to a regular class. With LLQ for Frame Relay, queues are set up on a per-PVC basis. Each PVC has a PQ to support voice traffic. This congestion-management method is considered the most optimal for voice.

If multiple classes are configured for LLQ, they share a single queue but are allocated bandwidth and policed individually. It is recommended that you place only voice in the priority queue, because voice traffic typically is well-behaved, requiring fixed maximum amounts of bandwidth per call. The voice traffic is identified by IP precedence bits set to a value of 5 or a DSCP of Expedited Forwarding (EF) with values of 101xxx. Introducing video or other variable-rate real-time or nonreal-time traffic types could cause unacceptable jitter for the voice traffic. Video traffic normally is set to AF41 (100010). And signaling normally is set to an IP precedence of 3 or a DSCP of 011xxx.

Auto QoS

Auto QoS is a recent Cisco IOS feature that uses a simpler command-line interface (CLI) to enable QoS for VoIP in WAN and LAN environments. Auto QoS significantly reduces the amount of configuration lines necessary to support VoIP in the network.

For the WAN, Auto QoS provides the following capabilities:

- Automatically classifies RTP and VoIP control packets
- Builds VoIP Modular QoS in the Cisco IOS Software
- Provides LLQ for VoIP bearer traffic
- Provides minimum-bandwidth guarantees by using CBWFQ for VoIP control traffic
- Enables WAN traffic shaping where required
- Enables LFI and RTP where required

For the LAN, Auto QoS provides the following capabilities:

- Enforces a trust boundary at the Cisco IP Phone
- Enforces a trust boundary on the Catalyst switch access and uplink and downlink ports
- Enables strict priority queuing and weighted round robin for voice and data traffic
- Modifies queue admission criteria by performing CoS-to-queue mapping
- Modifies queue sizes, as well as queue weights where required
- Modifies CoS-to-DSCP and IP Precedence-to-DSCP mappings

AutoQoS is beneficial for small-to-medium-sized businesses that need to deploy IPT quickly but lack the experience and staffing to plan and deploy IP QoS services.

Auto QoS also benefits large customer enterprises that need to deploy Cisco IPT on a large scale while reducing the costs, complexity, and timeframe for deployment and ensuring that the appropriate QoS for voice applications is being set consistently.

IPT Design Recommendations

The following are some best-practice recommendations when implementing IPT:

- Use separate VLANs/IP subnets for IP phones.
- Use private IP addresses for IP phones.
- Place CallManager and Unity servers on filtered VLAN/IP subnets in the server access in the data center.
- Use IP precedence or DSCP for classification and marking.
- Use LLQ on WAN links.
- Use LFI on slower-speed WAN links.
- Use CAC to avoid oversubscription of priority queues.

IEEE 802.1Q should be configured on the PoE LAN switch ports to allow a voice VLAN for the IP phone and a data VLAN for the PC connected to the IP phone. These VLANs should be on separate IP subnets, and the IP phone should be an RFC 1918 private address subnet. Furthermore, the CallManager servers should be placed on a separate IP subnet in the data center. This lets you restrict access to the IPT environment.

IPT voice packets should be marked with a DSCP of EF (IP precedence 5), and signaling packets should be marked with AF31 (IP precedence 3). This allows QoS schemes to give precedence to the marked packets. LLQ takes the EF marked packets and places them in the strict priority queue, guaranteeing bandwidth for voice. LFI should be configured on WAN links of a size less than 768 kbps to allow smaller IPT packets to get through larger packets. LFI and LLQ also reduce jitter in IPT conversations.

CAC should be used to keep excess voice traffic from the network by rerouting it via alternative network paths or to the PSTN. CAC protects voice traffic from being affected by other voice traffic.

References and Recommended Readings

Andreasen, F., B. Foster, *Media Gateway Control Protocol (MGCP) Version 1.0*, RFC 3435, available from http://www.ietf.org/rfc

Arango, M., A. Dugan, I. Elliott, C. Huitema, S. Pickett, *Media Gateway Control Protocol (MGCP) Version 1.0*, RFC 2705, available from http://www.ietf.org/rfc

Audio-Video Transport Working Group and H. Schulzrinne, *RTP Profile for Audio and Video Conferences with Minimal Control*, RFC 1890, available from http://www.ietf.org/rfc

Audio-Video Transport Working Group, H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, *RTP: A Transport Protocol for Real-Time Applications*, RFC 1889, available from http://www.ietf.org/rfc

Handley, M., H. Schulzrinne, E. Schooler, and J. Rosenberg, *SIP: Session Initiation Protocol*, RFC 2543, available from http://www.ietf.org/rfc

Keagy, S. *Integrating Voice and Data Networks*. Indianapolis: Cisco Press, 2000.

Kotha, S. "Deploying H.323 Applications in Cisco Networks" (white paper); available from http://www.cisco.com/warp/public/cc/pd/iosw/ioft/mmcm/tech/h323_wp.htm

Lovell, D. *Cisco IP Telephony.* Indianapolis: Cisco Press, 2002.

McQuerry, S., K. McGrew, S. Foy, *Cisco Voice over Frame Relay, ATM, and IP.* Indianapolis: Cisco Press, 2001.

Reference Guide, Packet Voice Networking. http://www.cisco.com/warp/public/cc/pd/rt/mc3810/prodlit/pvnet_in.htm

Tech Notes: Voice Network Signaling and Control. http://www.cisco.com/warp/public/788/signalling/net_signal_control.html

Voice over IP: Per Call Bandwidth Consumption. http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.htm

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

This chapter covered the following topics that you need to master for the CCDA exam:

- **Traditional voice architectures**—The architecture of TDM voice networks. You must understand PSTN technologies and limitations.
- **Integrated multiservice networks**—IP telephony architectures and components.
- **IPT design**—Design issues, QoS mechanisms, and IPT best practices.

Table 15-8 summarizes technologies and concepts used in voice network design.

Table 15-8 *Voice Technologies*

Technology	Description
BHT	Busy-hour traffic. Expressed in Erlangs.
CCS	Centum Call Second. One call on a channel for 100 seconds.
CDR	Call Detail Record.
FXS	Foreign Exchange Station.
FXO	Foreign Exchange Office.
E&M	Ear and mouth—analog trunk.
Erlang	Measure of total voice traffic volume in one hour. 1 Erlang = 360 CCS.
VAD	Voice Activity Detection.
RTP	Real-time Transport Protocol. Carries coded voice. Runs over UDP.
RTCP	RTP Control Protocol.
Codec	Coder-decoder. Transforms analog signals into digital bit streams.
H.323	ITU framework for multimedia protocols. Used to control Cisco IOS gateways.
MGCP	Media Gateway Control Protocol. Used to control IOS gateways.

continues

Table 15-8 *Voice Technologies (Continued)*

Technology	Description
SIP	Session Initiation Protocol. IETF framework for multimedia protocols.
SS7	Allows voice and network calls to be routed and controlled by central call controllers. Permits modern consumer telephone services. Protocol used in the PSTN.
PSTN	Public Switched Telephone Network.
DTMF	Dual-Tone Multifrequency dialing.
PBX	Private Branch Exchange.
GoS	Grade of service. The probability that a call will be blocked when attempting to seize a circuit.
Centrex	With Centrex services, the CO acts as the company's voice switch, giving the appearance that the company has its own PBX.
IVR	Interactive Voice Response systems provide recorded announcements, prompt callers for key options, and provide information.
ACD	Automatic Call Distribution systems route calls to a group of agents.

Table 15-9 summarizes the different types of codecs used for voice coding.

Table 15-9 *Codec Standards*

Codec	Bit Rate	MOS	Description
G.711u	64 kbps	4.1	PCM. Mu-law version used in North America and Japan. Samples speech 8000 times per second, represented in 8 bits.
G.711a	64 kbps	4.1	PCM. A-law used in Europe and international routes.
G.723.1	6.3 kbps	3.9	Multipulse Excitation–Maximum Likelihood Quantization (MPE-MLQ).
G.723.1	5.3 kbps	3.65	Algebraic Code–Excited Linear Prediction (ACELP).
G.726	16/24/32/ 40 kbps	3.85	Adaptive Differential Pulse-Code Modulation (AD-PCM).
G.728	16 kbps	3.61	Low-Delay CELP (LDCELP).
G.729	8 kbps	3.92	Conjugate Structure ACELP (CS-ACELP).

Table 15-10 summarizes the IPT functional areas.

Table 15-10 *IPT Functional Areas*

IPT Functional Area	Description
Service applications	Unity, IVR, TAPI interface
Call processing	Cisco CM
Client Endpoints	IP phones, digital and analog gateways
Voice Enabled Infrastructure	Layer 2 and Layer 3 switches and routers

Table 15-11 summarizes protocols used in VoIP networks.

Table 15-11 *Significant Protocols in VoIP Networks*

Protocol	Description
DHCP	Dynamic Host Control Protocol. Provides IP address, mask, gateway, DNS address, and TFTP address.
DNS	Domain Name System. Provides the IP address of the TFTP server.
TFTP	Trivial File Transfer Protocol. Provides the IP phone configuration and operating system.
SSCP	Skinny Station Control Protocol. Establishes calls between IP phones and CM.
RTP	Real-time Transport Protocol. Carries codec voice streams.
RTCP	Real-time Transport Control Protocol. Controls RTP streams.
H.323	ITU framework standard. Used to control Cisco IOS gateways.
SIP	Session Initiation Protocol. An IETF replacement for H.323.

Table 15-12 summarizes the different schemes used for QoS.

Table 15-12 *QoS Scheme Summary*

QoS Scheme	Description
CRTP	RTP header compression. Reduces header overhead from 40 bytes to 2 to 4 bytes.
LFI	Link Fragmentation and Interleaving. Fragments large data packets and interleaves VoIP packets between them.
PQ-WFQ	Also known as IP RTP priority. Uses a single strict queue for RTP traffic. All other traffic in WFQ.

continues

Table 15-12 *QoS Scheme Summary (Continued)*

QoS Scheme	Description
LLC	Also known as PQ-CBWFQ. Uses a single strict queue for RTP traffic. Differentiated CoS available for all other traffic.
CAC	Call Admission Control. Reroutes voice calls to the PSTN.

Q&A

As mentioned in the Introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. True or false: LLQ is recommended for VoIP networks.
2. True or false: H.323 is an IETF standard, and SIP is an ITU standard for multimedia protocols.
3. True or false: An Erlang is a unit that describes the number of calls in an hour.
4. What do you implement to stop packets from being transmitted when there is silence in a voice conversation?
5. The variable delay of received VoIP packets is corrected with what kind of buffers?
6. True or false: Common Channel Signaling uses a separate channel for signaling.
7. True or false: FXO ports are used for phones, and FXS ports connect to the PSTN.
8. True or false: SS7 provides mechanisms for exchanging control and routing messages in the PSTN.
9. An organization uses what kind of system to gather and provide information for the customer before transferring her to an agent?
10. An organization uses what kind of system to route calls to agents based on the agent skill group or call statistics?
11. In addition to codec selection, both _____ and _____ can be used to reduce the bandwidth of VoIP calls.
12. Label each of the following delays as fixed or variable:
    a. Processing
    b. Dejitter buffer
    c. Serialization
    d. Queuing
    e. Propagation

13. How can you reduce serialization delay?
14. Which two queuing techniques use a strict priority queue for RTP traffic?
15. True or false: The maximum one-way delay in the G.114 recommendation for acceptable voice is 200 ms.
16. True or false: FRF.12 is an LFI standard used in networks with VoFR and VoIP over Frame Relay.
17. An assessment of a network determines that the average round-trip time between two sites is 250 ms. Can an IPT solution be implemented between the sites?
18. Match each protocol with its description:

    i. DHCP

    ii. SSCP

    iii. RTP

    iv. H.323

    v. TFTP

    a. Transports coded voice streams

    b. Controls Cisco IOS gateways

    c. Provides call signaling between Cisco IP phones and CM

    d. Provides IP address

    e. Provides phone configuration
19. Match each CM deployment model with its description:

    i. Single-site deployment

    ii. Distributed WAN

    iii. Centralized WAN

    a. Single CM cluster with SRST at remote sites

    b. Single CM cluster implemented in a large building

    c. Multiple CM clusters

20. Match each component with its Cisco IPT functional area:

i. ICM

ii. Layer 3 switch

iii. Digital gateway

iv. Unity

a. Service applications

b. Call processing

c. Client Endpoint

d. Infrastructure

21. Which standard establishes specifications for call setup and packet formats for VoFR?

22. Which protocol is preferred for inter-PBX trunks?

a. SS7

b. RTP

c. Q.SIG

d. DTMF

23. CRTP compresses the IP/UDP/RTP header to what size?

a. 2 or 4 bytes

b. 2 or 5 bytes

c. 40 bytes

d. It compresses the RTP header only

24. The steps of converting an analog signal to digital format occur in which order?

a. Sampling, filtering, digitizing

b. Filtering, sampling, digitizing

c. Digitizing, filtering, sampling

d. Sampling, digitizing, filtering

25. Digitizing is divided into which two processes?

a. Filtering and sampling

b. Expanding and filtering

c. Companding, and quantizing and coding

d. Sampling, and quantizing and coding

26. Which of the following are goals of IP telephony?

- **a.** Use the existing IP infrastructure
- **b.** Provide lower cost of ownership
- **c.** Provide greater flexibility in voice communications
- **d.** All of the above

27. An analysis of a 384-kbps WAN link shows IPT calls being delayed when large file transfers take place. The circuit is running at 45 percent utilization. What QoS scheme(s) should be implemented to alleviate this?

- **a.** CQ and cRTP
- **b.** LFI and cRTP
- **c.** LLQ
- **d.** All of the above

28. Which codec is recommended for use in WAN links?

- **a.** G.711
- **b.** G.723
- **c.** G.726
- **d.** G.729

29. Which technology reduces the amount of bandwidth used? (Choose all that apply.)

- **a.** QoS
- **b.** LFI
- **c.** cRTP
- **d.** VAD

30. Which of the following statements is true?

- **a.** CAC prevents voice calls from affecting other voice calls.
- **b.** CAC prevents voice calls from affecting data bandwidth.
- **c.** CAC prevents data from affecting voice calls.
- **d.** CAC prevents data from affecting other data traffic.

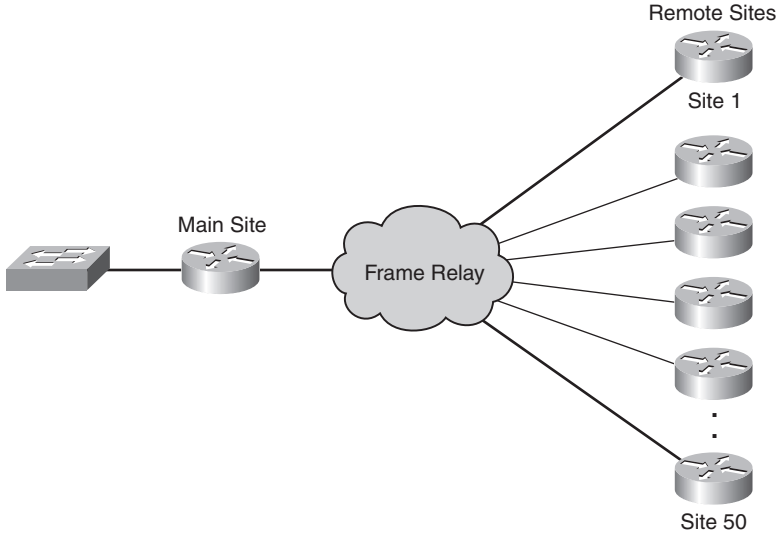
31. What IPT component contains the dial plan and is used to register IP phones?

- **a.** Gateway
- **b.** Unity server
- **c.** Gatekeeper
- **d.** Cisco Unified CallManager

Use both the scenario described in the following paragraph and Figure 15-18 to answer the following questions.

The client has an existing Frame Relay network, as shown in Figure 15-18. The network has a large site and 50 small remote sites. The client wants a design for a VoIP network. The client wants to provide differentiated CoS for the voice, Systems Network Architecture (SNA), FTP, and other traffic.

Figure 15-18 *Client's Current Frame Relay Network*



32. Based on the current network diagram, which Cisco IPT deployment model should you recommend?

33. What feature should you recommend to provide call processing in the event of a WAN failure?

34. Which queuing technique should you recommend?

35. For Site 1, the current data traffic is 512 kbps, and video traffic is 0. What is the minimum bandwidth required to support four concurrent VoIP G.729 calls plus the data traffic to the site?

36. Should you implement a CallManager cluster?

37. What feature can you use to reduce bandwidth over the WAN links?

38. Which LFI technique should you use to reduce the serialization delay?

This chapter covers the following subjects:

- SNMP
- Other Network Management Technologies

CHAPTER 16

Network Management Protocols

This chapter introduces the following network management protocols and components: Simple Network Management Protocol (SNMP), Management Information Base (MIB), Remote Monitoring (RMON) protocol, Cisco Discovery Protocol (CDP), and the use of NetFlow and system logging (syslog).

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

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

Table 16-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 16-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
SNMP	1, 2, 3, 4, 6, 8
Other Network Management Technologies	5, 7, 9, 10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure, you should mark this question wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might give you a false sense of security.

1. Which version of SNMP introduces security extensions for authentication and encryption?
   a. SNMPv1
   b. SNMPv2
   c. SNMPv3
   d. SNMPv4
2. SNMP runs over which protocol?
   a. TCP
   b. UDP
   c. IP
   d. MIB
3. Which SNMP component contains an agent?
   a. Managed device
   b. Agent
   c. NMS manager
   d. MIB
4. Which SNMP component is a collection of information that is stored on the local agent?
   a. Managed device
   b. Agent
   c. NMS manager
   d. MIB
5. CDP is an acronym for which Cisco function?
   a. Collection Device Protocol
   b. Cisco Device Protocol
   c. Campus Discovery Protocol
   d. Cisco Discovery Protocol
6. Which SNMP operation obtains full table information from an agent?
   a. Get
   b. GetNext
   c. GetBulk
   d. Inform

7. RMON1 provides information at what levels of the OSI model?
   a. Data link and physical
   b. Network, data link, physical
   c. Transport and network
   d. Application to network
8. Which of the following is not an SNMP operation?
   a. Get
   b. Community
   c. Set
   d. Trap
9. Which solution gathers information that can be used for accounting and billing applications?
   a. RMON
   b. NetFlow
   c. CDP
   d. Syslog
10. What is CDP?
   a. Client/server protocol
   b. Hello-based protocol
   c. Network management agent
   d. Request-response protocol

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. It includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

After a new network is designed, installed, and configured, it must be managed by the operations team. Network management tools are used to gather operating statistics and to manage devices. Statistics are gathered on WAN bandwidth utilization, router CPU and memory utilization, and interface counters. Configuration changes are also made through network management tools such as CiscoWorks. The ISO defines five types of network management processes that are commonly known as FCAPS. These processes are as follows:

- **Fault management**—Refers to detecting and correcting network fault problems
- **Configuration management**—Refers to baselining, modifying, and tracking configuration changes
- **Accounting management**—Refers to keeping track of circuits for billing of services
- **Performance management**—Measures the network's effectiveness at delivering packets
- **Security management**—Tracks the authentication and authorization information

The protocols and tools described is this chapter perform some of these functions. SNMP is the underlying protocol used for network management. Agents are configured in managed devices (routers) that allow the network management system to manage the device. RMON is used for advanced monitoring of routers and switches. CDP is a Cisco proprietary protocol that allows the discovery of Cisco devices. NetFlow is a network monitoring solution that allows for greater scalability than RMON. Syslog allows system messages and error events to be gathered for review.

SNMP

SNMP is an IP application layer protocol that has become the standard for the exchange of management information between network devices. SNMP was initially described in RFC 1157. It is a simple solution that requires little code to implement, which allows vendors to build SNMP agents on their products.

SNMP runs over User Datagram Protocol (UDP) and thus does not inherently provide for sequencing and acknowledgment of packets, but it still reduces the amount of overhead used for management information.

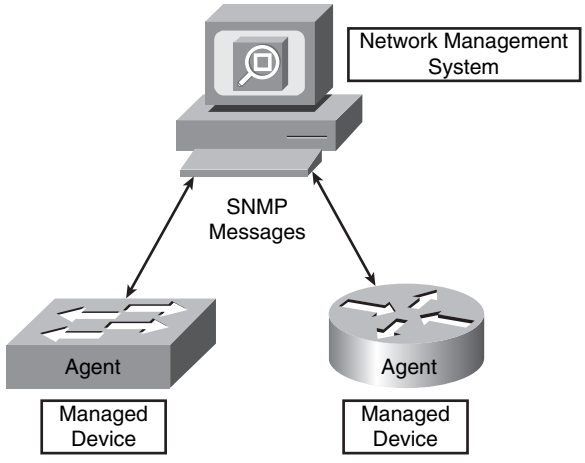
SNMP Components

SNMP has three network-managed components:

- The managed device
- The agent that resides on the managed device
- The network management system (NMS)

Figure 16-1 shows the relationship of these components.

Figure 16-1 *SNMP Components*



A managed device is a router or LAN switch or any other device that contains an SNMP agent. These devices collect and store management information and make this information available to the NMS. SNMP community strings (passwords) are configured on routers and switches to allow for SNMP management.

The agent is the network management software that resides in the managed device. The agent gathers the information and puts it in SNMP format. It responds to the manager's request for information and also generates traps.

The NMS has applications that are used to monitor and configure managed devices. It is also known as the manager. The NMS provides the bulk of the processing resources used for network management.

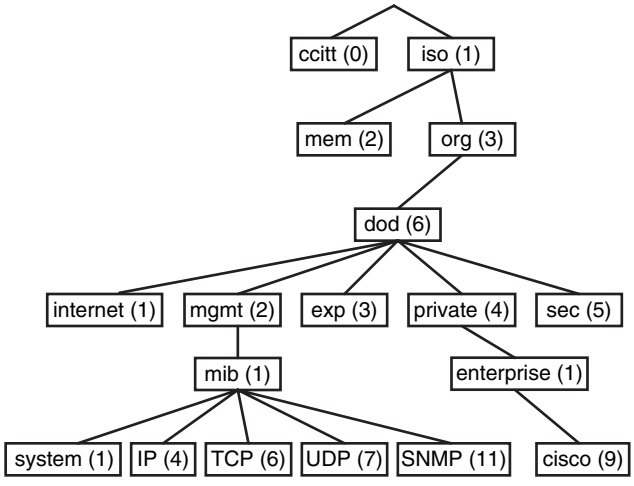
MIB

A Management Information Base (MIB) is a collection of information that is stored on the local agent of the managed device. MIBs are organized hierarchically and are accessed by the NMS. MIBs are organized in a treelike structure, with each branch containing similar objects. Each object has a unique object identifier (number) that uniquely identifies the managed object of the MIB hierarchy.

The top-level MIB object IDs belong to different standards organizations, and lower-level object IDs are allocated to associated organizations. Vendors define private branches that include

managed objects for their products. Figure 16-2 shows a portion of the MIB tree structure. RFC 1213 describes the MIBs for TCP/IP. Cisco defines the MIBs under the Cisco head object. For example, a Cisco MIB can be uniquely identified by either the object name, *iso.org.dod.private.enterprise.cisco*, or the equivalent object descriptor, *1.3.6.1.4.1.9*.

Figure 16-2 *MIB Tree Structure*



Each individual manageable feature in the MIB is called a MIB variable. The MIB module is a document that describes each manageable feature that is contained in an agent. The MIB module is written in Abstract Syntax Notation 1 (ASN.1). Three ASN.1 data types are required: name, syntax, and encoding. The name serves as the object identifier. The syntax defines the object's data type (integer or string). The encoding data describes how information associated with a managed object is formatted as a series of data items for transmission on the network. More specific information about Cisco MIBs can be found at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

SNMP Message Types

SNMPv1 was initially defined by RFC 1157. Since then, SNMP has evolved with a second and third version, each adding new message types. The CCDA should understand each message type and the version associated with each.

SNMPv1

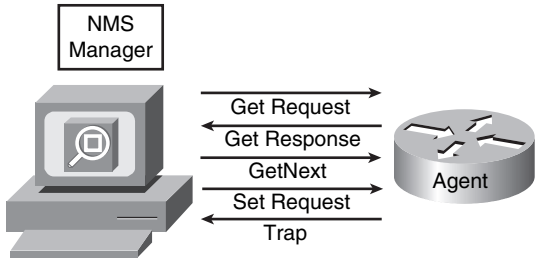
SNMPv1 is defined by RFC 1157. It is a simple request-and-response protocol. The NMS manager issues a request, and managed devices return responses. The date types are limited to

32-bit values. SNMPv1 uses four protocol operations, with five message types to carry out the communication:

- Get Request
- GetNext Request
- Get Response
- Set Request
- Trap

Figure 16-3 shows the SNMPv1 message types.

Figure 16-3 *SNMPv1 Message Types*



The NMS manager uses the Get operation to retrieve the value-specific MIB variable from an agent. The GetNext operation is used to retrieve the next object instance in a table or list within an agent. The Get Response contains the value of the requested variable.

The NMS manager uses the Set operation to set values of the object instance within an agent. For example, the Set operation can be used to set an IP address on an interface or to bring an interface up or down. Agents use the Trap operation to inform the NMS manager of a significant alarm event. For example, a trap is generated when a WAN circuit goes down.

SNMPv2

SNMPv2 is an evolution of the initial SNMPv1 and is defined in RFCs 1901 and 1902. SNMPv2 offers improvements to SNMPv1, including additional protocol operations. The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv1. The SNMP Trap operation serves the same function as in SNMPv1, but it uses a different message format.

SNMPv2 defines two new protocol operations:

- GetBulk
- Inform

The NMS manager uses the GetBulk operation to retrieve large blocks of data, such as multiple rows in a table. This is more efficient than repeating GetNext commands. If the agent responding to the GetBulk operation cannot provide values for all the variables in a list, it provides partial results. The Inform operation allows one NMS manager to send trap information to other NMS managers and to receive information. Another improvement is that data type values can be 64 bits.

SNMPv3

SNMPv3 was developed to correct several deficiencies in the earlier versions of SNMP, security being a primary reason. SNMPv3 is defined in RFCs 3410 through 3415. SNMPv3 provides authentication and privacy by using usernames and access control by using key management. Security levels are implemented to determine which devices a user can read, write, or create. SNMPv3 also verifies each message to ensure that it has not been modified during transmission.

SNMPv3 introduces three levels of security:

- noAuthNoPriv
- authNoPriv
- authPriv

The noAuthNoPriv level provides no authentication and no privacy (encryption). At the authNoPriv level, authentication is provided but not encryption. The authPriv level provides authentication and encryption.

Authentication for SNMPv3 is based on HMAC-MD5 or HMAC-SHA algorithms. The Cipher Block Chaining-Data Encryption Standard (CBC-DES) standard is used for encryption.

Other Network Management Technologies

This section covers RMON, NetFlow, CDP, and syslog technologies used to gather network information.

RMON

RMON is a standard monitoring specification that enables network monitoring devices and console systems to exchange network monitoring data. RMON provides more information than

SNMP, but more sophisticated data collection devices (network probes) are needed. RMON looks at MAC-layer data and provides aggregate information on the statistics and LAN traffic.

Enterprise networks deploy network probes on several network segments; these probes report back to the RMON console. RMON allows network statistics to be collected even if a failure occurs between the probe and the RMON console. RMON1 is defined by RFCs 1757 and 2819, and additions for RMON2 are defined by RFC 2021.

The RMON MIB is located at *iso.org.dod.internet.mgt.mib.rmon* or by the equivalent object descriptor, *1.3.6.1.2.1.16*. RMON1 defines nine monitoring groups; each group provides specific sets of data. One more group is defined for Token Ring. Each group is optional, so vendors do not need to support all the groups in the MIB. Table 16-2 shows the RMON1 groups.

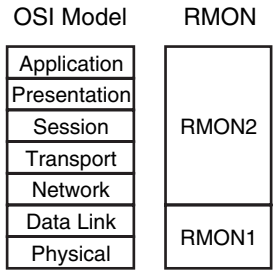
Table 16-2 *RMON1 Groups*

ID	Name	Description
1	Statistics	Contains real-time statistics for interfaces: packets sent, bytes, CRC errors, fragments
2	History	Stores periodic statistic samples for later retrieval
3	Alarm	An alarm event is generated if a statistic sample crosses a threshold
4	Host	Host-specific statistics
5	HostTopN	Most active hosts
6	Matrix	Stores statistics for conversations between two hosts
7	Filters	Allows packets to be filtered
8	Packet Capture	Allows packets to be captured for subsequent analysis
9	Events	Generates notification of events
10	Token Ring	Token Ring RMON extensions

RMON2

RMON1 is focused on the data link and physical layers of the OSI model. As shown in Figure 16-4, RMON2 provides an extension for monitoring upper-layer protocols.

Figure 16-4 *RMON1 and RMON2 Compared to the OSI Model*



Defined by RFC 2021, RMON2 extends the RMON group with the MIB groups listed in Table 16-3.

Table 16-3 *RMON2 Groups*

ID	Name	Description
11	Protocoldir	Lists the protocols the device supports
12	Protocoldis	Traffic statistics for each protocol
13	Addressmap	Contains network-to-MAC layer address mapping (IP-to-MAC)
14	nlHost	Contains statistics for traffic sent to or from network layer hosts
15	nlMatrix	Contains statistics for conversations between two network layer hosts
16	alHost	Contains Application layer statistics for traffic sent to or from each host
17	alMatrix	Contains Application layer statistics for conversations between pairs of hosts
18	Usrhistory	Contains periodic samples of specified variables
19	Probeconfig	Probe parameter configuration

NetFlow

Cisco's NetFlow allows the tracking of IP flows as they are passed through routers and multilayer switches. NetFlow information is forwarded to a network data analyzer, network planning tools, RMON applications, or accounting and billing applications. NetFlow allows for network planning, traffic engineering, billing, accounting, and application monitoring. NetFlow consists of three major components:

- Network accounting
- Flow collector engines
- Data analyzers

Routers and switches are the network accounting devices that gather the statistics. These devices aggregate data and export the information. Each unidirectional network flow is identified by both source and destination IP addresses and transport layer port numbers. NetFlow can also identify flows based on IP protocol number, type of service, and input interface.

The NetFlow export or transport mechanism sends the NetFlow data to a collection engine or network management collector. Flow collector engines perform data collection and filtering. They aggregate data from several devices and store the information. Different NetFlow data analyzers can be used based on the intended purpose. NetFlow data can be analyzed for performance and planning purposes, security monitoring, RMON monitoring, application monitoring, and billing and accounting.

NetFlow Compared to RMON

NetFlow lets you gather more statistical information than RMON with fewer resources. It provides more data, with date and time stamping. NetFlow has greater scalability and does not require network probes. It can be configured on individual layer 3 interfaces on routers and layer 3 switches. NetFlow provides detailed information on the following:

- Source and destination IP addresses
- Source and destination interface identifiers
- TCP/UDP source and destination port numbers
- Number of bytes and packets per flow
- IP type of service (ToS)

CDP

CDP is a Cisco-proprietary protocol that can be used to discover Cisco network devices. CDP is media- and protocol-independent, so it works over LAN, Frame Relay, ATM, and other media. The requirement is that the media support Subnetwork Access Protocol (SNAP) encapsulation. CDP runs at the data link layer of the OSI model. CDP uses hello messages; packets are exchanged between neighbors, but CDP information is not forwarded.

Being protocol- and media-independent is CDP's biggest advantage over other network management technologies. CDP provides plenty of neighbor information, which is significant for network discovery. It is very useful when SNMP community strings are unknown when performing a network discovery.

When displaying CDP neighbors, you can obtain the following information:

- **Local port**—Local port to connect to the network
- **Device ID**—Name of the neighbor device and MAC address
- **Device IP address**—IP address of the neighbor
- **Hold time**—How long to hold the neighbor information
- **Device capabilities**—Type of device discovered: router, switch, transparent bridge, host, IGMP, repeater
- **Version**—IOS or switch OS version
- **Platform**—Router or switch model number
- **Port ID**—Interface of the neighboring device

Network management devices can obtain CDP information for data gathering. CDP should be disabled on interfaces that face the Internet and other secure networks. CDP works on only Cisco devices.

NOTE Disable CDP on interfaces for which you do not want devices to be discovered, such as Internet connections.

Syslog

The syslog protocol is currently defined in RFC 3164. Syslog transmits event notification messages over the network. Network devices send the event messages to an event server for aggregation. Network devices include routers, servers, switches, firewalls, and network appliances. Syslog operates over UDP, so messages are not sequenced or acknowledged. The syslog messages are also stored on the device that generates the message and can be viewed locally.

Syslog messages are generated in many broad areas. These areas are called facilities. Cisco IOS has more than 500 facilities. Common facilities include

- IP
- CDP
- OSPF
- TCP

- Interface
- IPsec
- SYS operating system
- Security/authorization
- Spanning Tree Protocol (STP)

Each syslog message has a level. The syslog level determines the event's criticality. Lower syslog levels are more important. Table 16-4 lists the syslog levels.

Table 16-4 *Syslog Message Levels*

Syslog Level	Severity	Level
0	Emergency	System is unusable
1	Alert	Take action immediately
2	Critical	Critical conditions
3	Error	Error messages
4	Warning	Warning conditions
5	Notice	Normal but significant events
6	Informational	Informational messages
7	Debug	Debug level messages

Common syslog messages are interface up and down events. Access lists can also be configured on routers and switches to generate syslog messages when a match occurs. Each syslog message includes a time stamp, level, and facility. Syslog messages have the following format:

mm/*dd*/*yy*:*hh*/*mm*/*ss*:*FACILITY-LEVEL-mnemonic*:*description*

Syslog messages can create large amounts of network bandwidth. It is important to enable only syslog facilities and levels that are of particular importance.

References and Recommended Reading

"NetFlow Performance Analysis," http://www.cisco.com/en/US/tech/tk812/technologies_white_paper0900aecd802a0eb9.shtml

MIBs Supported by Product, http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1441, *Introduction to Version 2 of the Internet-standard Network Management Framework*

RFC 1757, *Remote Network Monitoring Management Information Base*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 Using SMIv2*

RFC 2576, *Coexistence Between Version 1, Version 2, and Version 3 of the Internet Standard Network Management Framework*

RFC 3164, *The BSD syslog Protocol*

RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 3414, *User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3416, *Protocol Operations for SNMPv2*

RFC 3418, *Management Information Base for SNMPv2*

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on the CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

The CCDA exam requires that you be familiar with the following topics covered in this chapter:

- **SNMP**—Underlying protocol for network management
- **MIB**—Stores management information
- **RMON**—Uses network probes for proactive remote monitoring
- **CDP**—Cisco's proprietary protocol for network discovery
- **NetFlow**—More efficient than RMON; collects flow data for performance, billing, planning, and QoS applications
- **Syslog**—Reports state information based on facilities and severity levels

Table 16-5 lists SNMP components.

Table 16-5 *SNMP Components*

SNMP Component	Description
Managed device	Collects and stores management information and contains an agent
Agent	Network management software that gathers information and puts it in SNMP format
NMS	Application used to monitor and configure managed devices

Table 16-6 summarizes SNMP messages.

Table 16-6 *SNMP Messages*

SNMP Message	Description
Get	Retrieves MIB variables from an agent
GetNext	Retrieves the next object instance in a table
Get Response	Response to Get operation commands

continues

Table 16-6 *SNMP Messages (Continued)*

SNMP Message	Description
Set Request	Sets values of the object within an agent
Trap	Sent by the agent to inform the NMS manager of a significant event
GetBulk	SNMPv2 operation to retrieve large blocks of data
Inform	SNMPv2 operation for NMS managers to send trap information to other managers

Table 16-7 summarizes the RMON1 and RMON2 groups.

Table 16-7 *RMON1 and RMON2 Groups*

ID	Name	Group	Description
1	Statistics	RMON1	Contains real-time statistics for interfaces: packets sent, bytes, CRC errors, fragments
2	History	RMON1	Stores periodic statistic samples for later retrieval
3	Alarm	RMON1	An alarm event is generated if a statistic sample crosses a threshold
4	Host	RMON1	Host-specific statistics
5	HostTopN	RMON1	Most active hosts
6	Matrix	RMON1	Stores statistics for conversations between two hosts
7	Filters	RMON1	Allows packets to be filtered
8	Packet capture	RMON1	Allows packets to be captured for subsequent analysis
9	Events	RMON1	Generates notification of events
10	Token Ring	RMON1	Token Ring RMON extensions
11	Protocoldir	RMON2	Lists the protocols the device supports
12	Protocoldis	RMON2	Traffic statistics for each protocol
13	Addressmap	RMON2	Contains network-to-MAC layer address mapping (IP-to-MAC)
14	nlHost	RMON2	Contains statistics for traffic sent to or from network layer hosts
15	nlMatrix	RMON2	Contains statistics for conversations between two network layer hosts

Table 16-7 *RMON1 and RMON2 Groups (Continued)*

ID	Name	Group	Description
16	alHost	RMON2	Contains application layer statistics for traffic sent to or from each host
17	alMatrix	RMON2	Contains application layer statistics for conversations between pairs of hosts
18	Usrhistory	RMON2	Contains periodic samples of specified variables
19	Probeconfig	RMON2	Probe parameter configuration

Table 16-8 summarizes other network management technologies.

Table 16-8 *NetFlow, CDP, and Syslog*

Technology	Description
NetFlow	Collects network flow data for network planning, performance, accounting, and billing applications
CDP	Proprietary protocol for network discovery that provides information on neighboring devices
Syslog	Reports state information based on facility and severity levels

Q&A

As mentioned in the introduction, you have two choices for review questions: here in the book or the exam questions on the CD-ROM. The answers to these questions appear in Appendix A.

For more practice with exam format questions, use the exam engine on the CD-ROM.

1. What does the acronym FCAPS stand for?
2. CDP runs at what layer of the OSI model?
3. Syslog level 5 is what level of severity?
4. True or false: RMON provides more scalability than NetFlow.
5. True false: NetFlow provides detailed information on the number of bytes and packets per conversation.
6. What information can be obtained from a neighbor using CDP?
7. What SNMP message is sent by an agent when an event occurs?
   a. Get
   b. Set
   c. GetResponse
   d. Trap
8. What SNMP message is sent to an agent to obtain an instance of an object?
   a. Get
   b. Set
   c. GetResponse
   d. Trap
9. What SNMP message is used to configure a managed device?
   a. Get
   b. Set
   c. GetResponse
   d. Trap

10. About how many facilities are available for syslog in Cisco routers?

    a. 25

    b. 100

    c. 500

    d. 1000

11. Which SNMPv3 level provides authentication with no encryption?

    a. authPriv

    b. authNoPriv

    c. noAuthNoPriv

    d. noauthPriv

12. What encryption standard does SNMPv3 use?

    a. 3DES

    b. CBC-DES

    c. HMAC-MD5

    d. MD5

13. Which technologies can you use to assess a network and create documentation? (Select two.)

    a. RMON

    b. MIB

    c. CDP

    d. NetFlow

14. Which of the following are true about CDP? (Select three.)

    a. It uses UDP.

    b. It is a data-link protocol.

    c. It provides information on neighboring routers and switches.

    d. It is media- and protocol-independent.

    e. It uses syslog and RMON.

15. RMON2 provides information at what levels of the OSI model?

    a. Data link and physical

    b. Network, data link, and physical

    c. Transport and network only

    d. Application to network

16. Which network management technology operates over TCP?
    a. SNMP
    b. RMON
    c. NetFlow
    d. None of the above
17. Which statement is correct?
    a. SNMPv1 uses GetBulk operations and 32-bit values.
    b. SNMPv2 uses 32-bit values, and SNMPv3 uses 64-bit values.
    c. SNMPv1 uses 32-bit values, and SNMPv2 uses 64-bit values.
    d. SNMPv1 uses GetBulk operations, and SNMPv2 uses Inform operations.
18. Which SNMPv3 level provides authentication and privacy?
    a. authPriv
    b. authNoPriv
    c. noAuthNoPriv
    d. noauthPriv
19. Match the RMON group with its description.

    i. Statistics

    ii. Matrix

    iii. alHost

    iv. protocoldir

    a. Stores statistics for conversations between two hosts

    b. Lists the protocols that the device supports

    c. Contains real-time statistics for interfaces: packets sent, bytes, CRC errors, fragments

    d. Contains application layer statistics for traffic sent to or from each host

The comprehensive scenarios in this part draw on many different CCDA exam topics to test your overall understanding of the material you will see on the CCDA exam.

Part V: Comprehensive Scenarios

This chapter covers four comprehensive scenarios that draw on several design topics covered in this book:

- Scenario One: Pearland Hospital
- Scenario Two: Big Oil and Gas
- Scenario Three: Beauty Things Store
- Scenario Four: Falcon Communications

The case studies and questions in this chapter draw on your knowledge of CCDA exam topics. Use these exercises to help master the topics as well as to identify areas you still need to review for the exam.

Understand that each scenario presented encompasses several exam topics. Each scenario, however, does not necessarily encompass all the topics. Therefore, you should work through all the scenarios in this chapter to cover all the topics.

CHAPTER 17

Comprehensive Scenarios

Your CCDA exam will probably contain questions that require you to analyze a scenario. This chapter contains four case studies that are similar in style to the ones you might encounter on the CCDA exam. Read through each case study and answer the corresponding questions. You will find the answers to the case study questions at the end of each scenario. Sometimes more than one solution can satisfy the customer's requirements. In these cases, the answers presented represent recommended solutions developed using good design practices. An explanation accompanies the answer where necessary.

Scenario One: Pearland Hospital

Mr. Robertson, the IT director at Pearland Hospital, is responsible for managing the network. Mr. Robertson has requested your help in proposing a network solution that will meet the hospital's requirements. The hospital is growing, and the management has released funds for network improvements.

The medical staff would like to be able to access medical systems using laptops from any of the patient rooms. Doctors and nurses should be able to access patient medical records, x-rays, prescriptions, and recent patient information. Mr. Robertson purchased new servers and placed them in the data center. The wireless LAN (WLAN) has approximately 30 laptops, and about 15 more are due in six months. The servers must have high availability.

Patient rooms are on floors 6 through 10 of the hospital building. Doctors should be able to roam and access the network from any of the floors. A radio-frequency report mentions that a single access point located in each communication closet can reach all the rooms on each floor. The current network has ten segments that reach a single router that also serves the Internet. The router is running Routing Information Protocol Version 1 (RIPv1). The back-end new servers are located in the same segment as those used on floor 1. Mr. Robertson mentions that users have complained of slow access to the servers. He also hands you a table with current IP addresses (see Table 17-1).

Table 17-1 *Current IP Addresses*

Floor	Servers	Clients	IP Network
1	15	40	200.100.1.0/24
2	0	43	200.100.2.0/24
3	0	39	200.100.3.0/24
4	0	42	200.100.4.0/24
5	0	17	200.100.5.0/24
6	0	15	200.100.6.0/24
7	0	14	200.100.7.0/24
8	0	20	200.100.8.0/24
9	0	18	200.100.9.0/24
10	0	15	200.100.10.0/24

Mr. Robertson would like a proposal to upgrade the network with fast switches and to provide faster access to the servers. The proposal should also cover secure WLAN access on floors 6 through 10. Include an IP addressing scheme that reduces the number of Class C networks the hospital uses. Mr. Robertson wants to reduce the number of networks leased from the Internet service provider (ISP).

Scenario One Questions

The following questions refer to Scenario One:

1. What are Pearland Hospital's business requirements?
2. Are there any business-cost constraints?
3. What are the network's technical requirements?
4. What are the network's technical constraints?
5. Prepare a logical diagram of the current network.
6. Does the hospital use IP addresses effectively?
7. What would you recommend to improve the switching speed between floors?
8. Based on the number of servers and clients provided, what IP addressing scheme would you propose?
9. What routing protocols would you recommend?

10. What solution would you recommend for WLAN access and the network upgrade?
11. Draw the proposed network solution.

Scenario One Answers

1. The hospital needs to provide access to patient records, prescriptions, and information from patient rooms.
2. No cost restrictions were discussed.
3. The technical requirements are as follows:

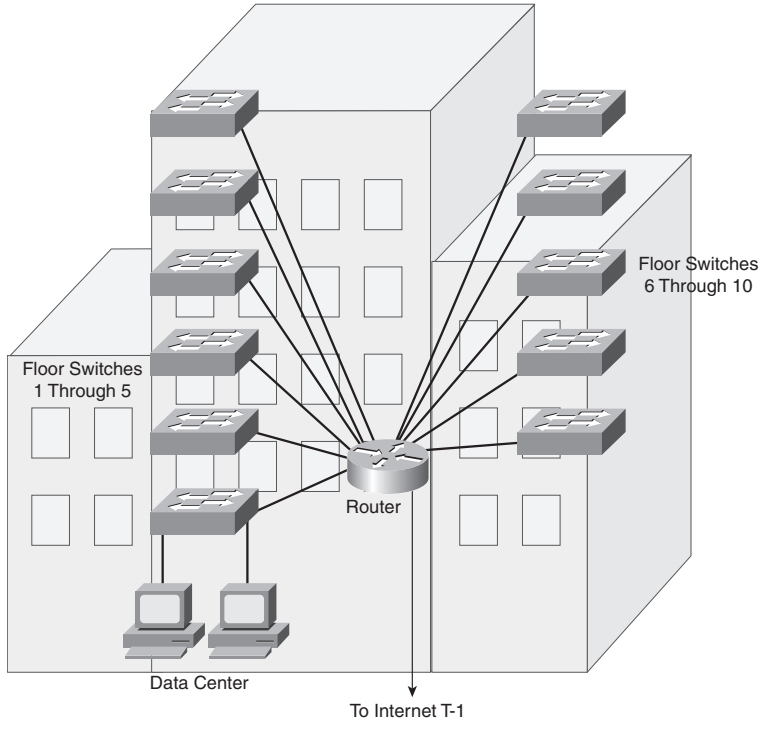
   WLAN access from rooms on floors 6 through 10

   Redundant access to servers in the data center

   Fast switching between LAN segments
4. The technical constraint is as follows:

   Servers must be located in the first floor data-center rooms.
5. Figure 17-1 shows the logical diagram of the current network.

Figure 17-1 *Pearland Hospital Current Network*



6. The hospital does not use IP addresses effectively. It uses Class C networks on each floor. Each floor wastes more than 200 IP addresses, because each Class C network provides up to 254 IP addresses.

7. Recommend using a high-speed Layer 3 switch for the building LANs. They can use the router for Internet and WAN access.

8. The primary recommendation is to use private addresses for the network. Using private addresses has been a best-practice policy for private internal networks since 1996. With private addresses, the hospital could release eight of the Class C networks to the ISP, retaining two for ISP connectivity.

   With private addresses, the hospital can choose to use 172.16.0.0/16 for private addressing. The addressing scheme shown in Table 17-2 provides sufficient address space for each network.

Table 17-2 *IP Addressing Scheme Using Private Addresses*

Floor	Servers	Clients	IP Network
1	15	0	172.16.0.0/24
1	0	40	172.16.1.0/24
2	0	43	172.16.2.0/24
3	0	39	172.16.3.0/24
4	0	42	172.16.4.0/24
5	0	17	172.16.5.0/24
6	0	15	172.16.6.0/24
7	0	14	172.16.7.0/24
8	0	20	172.16.8.0/24
9	0	18	172.16.9.0/24
10	0	15	172.16.10.0/24
WLAN: 6, 7, 8, 9, 10	0	40	172.16.20.0/24

Another solution is to retain the public addresses and use them in the internal network. This solution is less preferred than private addressing. Table 17-3 shows the recommended address scheme that would reduce the number of Class C networks.

Table 17-3 *IP Addressing Scheme Using Public Address Space*

Floor	Servers	Clients	IP Network
1	0	40	200.100.1.0/26
1	15	—	200.100.1.64/26
2	0	43	200.100.1.128/26
3	0	39	200.100.1.192/26
4	0	42	200.100.2.0/26
5	0	17	200.100.2.64/26
6	0	15	200.100.2.128/26
7	0	14	200.100.2.192/26
8	0	20	200.100.3.0/26
9	0	18	200.100.3.64/26
10	0	15	200.100.3.128/26
WLAN: 6, 7, 8, 9, 10	0	40	200.100.3.192/26

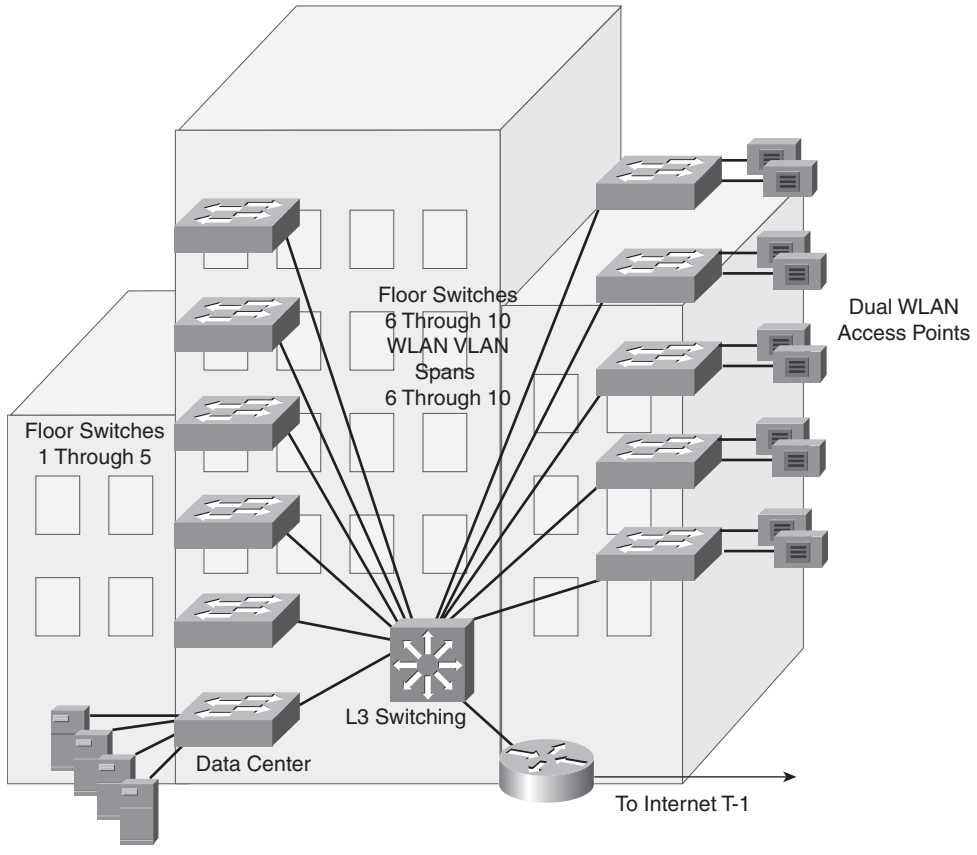
Each subnet has 62 IP addresses for host addressing. Based on the preceding IP addressing scheme, Pearland Hospital does not need networks 200.100.4.0/24 through 200.100.10.0/24.

9. Recommend routing protocols that support variable-length subnet masks (VLSM). The network is small. Recommend RIPv2 or Enhanced Interior Gateway Routing Protocol (EIGRP). Do not recommend Open Shortest Path First (OSPF) because of its configuration complexity.

10. Recommend using two access points on each floor for redundancy. Use a VLAN that spans floors 6 through 10. Change the router to a high-speed Layer 3 switch. Use the router for Internet or WAN access.

11. Figure 17-2 shows the diagram. The router is replaced by the L3 switch to provide high-speed switching between LANs. Each floor has an IP subnet plus a subnet for the WLAN and another for the data center. Each floor has two access points for redundancy. Servers can connect using Fast EtherChannel or Gigabit Ethernet.

Figure 17-2 *Pearland Hospital Proposed Network Solution*



Scenario Two: Big Oil and Gas

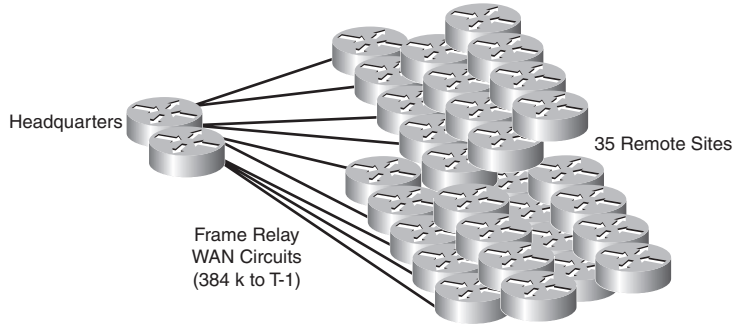
Mr. Drew is an IT director at Big Oil and Gas, a medium-sized petrochemical company based in Houston. It also has operations in the Gulf and in South America. Mr. Drew is in charge of the network infrastructure, including routers and switches. His group includes personnel who can install and configure Cisco routers and switches.

The Big Oil and Gas CIO wants to begin migrating from the voice network to an IP telephony solution to reduce circuit and management costs. Existing data WAN circuits have 50 percent utilization or less but spike up to 80 percent when sporadic FTP transfers occur.

Mr. Drew hands you the diagram shown in Figure 17-3. The exiting data network includes 35 sites with approximately 30 people at each site. The network is hub-and-spoke, with approximately 200 people at the headquarters. The WAN links range from 384 kbps circuits to T1 speeds.

Remote-site applications include statistical files and graphical-site diagrams that are transferred using FTP from remote sites to the headquarters.

Figure 17-3 *Big Oil and Gas Current Network*



Mr. Drew wants an IP telephony solution that manages the servers at headquarters but still provides redundancy or failover at the remote site. He mentions that he is concerned that the FTP traffic might impact the VoIP traffic. He wants to choose a site to implement a test before implementing IP telephony at all sites.

Scenario Two Questions

The following questions refer to Scenario Two:

1. What are the business requirements for Big Oil and Gas?
2. Are there any business-cost constraints?
3. What are the network's technical requirements?
4. What are the network's technical constraints?
5. Approximately how many IP phones should the network support?
6. What type of IP telephony architecture should you propose?
7. What quality of service (QoS) features would you propose for the WAN?
8. Would you propose a prototype or a pilot?
9. What solution would you suggest for voice redundancy at the remote sites?
10. Diagram the proposed solution.

Scenario Two Answers

1. The company wants to provide voice services in a converged network.
2. The solution should provide reduced costs over the existing separate voice and data networks.
3. The technical requirements are as follows:

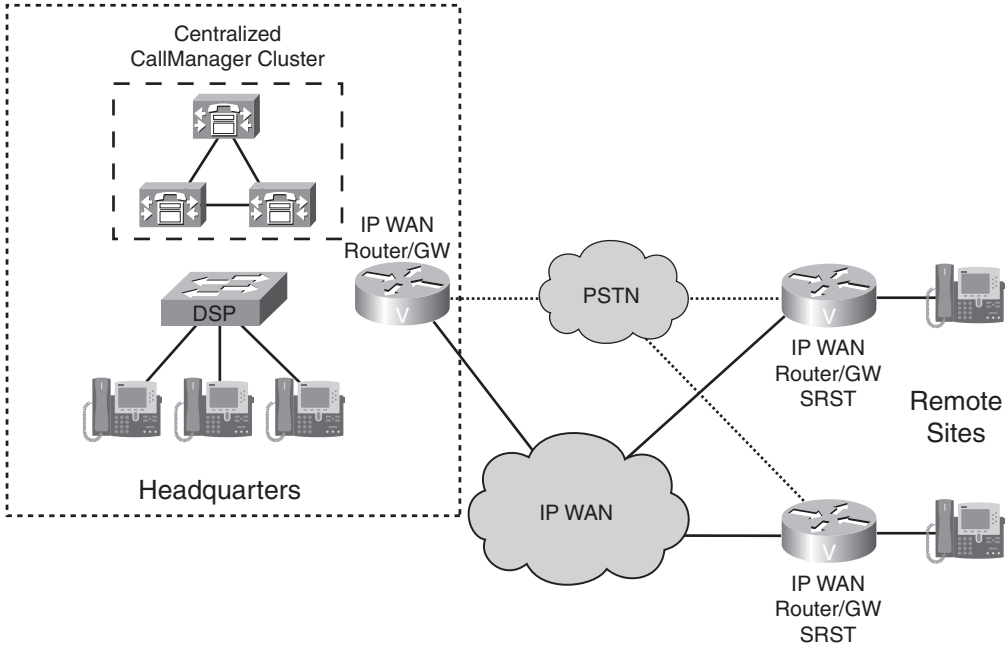
   Provide IP telephony over the data network.

   Provide voice redundancy or failover for the remote sites.

   Prevent FTP traffic from impacting the voice traffic.
4. The technical constraint is as follows:

   Call-processing servers need to be located at headquarters.
5. There are 200 IP phones at headquarters, and 35 * 30 = 1050 remote IP phones, for a total of 1250 IP phones.
6. Propose the WAN centralized call-processing architecture with a CallManager (CM) cluster at headquarters.
7. Use low-latency queuing (LLQ) on the WAN links to give the highest priority to voice traffic. Then define traffic classes for regular traffic and FTP traffic. Make bandwidth reservations for the voice traffic and maximum bandwidth restrictions for the FTP traffic. Call Admission Control (CAC) is recommended to limit the number of calls from and to a remote site.
8. To prove that calls can run over the WAN links, implement a pilot site. The pilot would test the design's functionality over the WAN with or without FTP traffic.
9. Recommend the use of Survivable Remote Site Telephony (SRST) to provide voice services in the event of WAN failure, and reroute calls to the Public Switched Telephone Network (PSTN).
10. Figure 17-4 shows the diagram, which shows headquarters and two remote sites for clarity. This architecture is duplicated for all remote sites. Each site uses a voice router that is connected to both the IP WAN and the PSTN. SRST provides voice survivability in the case of WAN failure. A CM cluster is implemented at the headquarters. The CM servers are in the data center in a redundant network.

Figure 17-4 *Headquarters and Two Remote Sites for Clarity*



Scenario Three: Beauty Things Store

Beauty Things is a chain of stores that sell beauty supplies. Headquarters is in Houston, Texas, and more than 60 stores are located throughout the U.S. The CIO tells you that they are in the middle of a WAN migration from Frame Relay to MPLS. It will be completed in two months. Most WAN links are less than 384 kbps.

After the WAN migration is complete, the CIO wants to use VoIP for voice calls between stores. He wants to complete the VoIP project within the next six months and within the established budget. Each store will have five concurrent calls back to headquarters.

The WAN provider has four priority queues for traffic: blue, red, green, and yellow. Each is assigned the DSCP codepoints listed in Table 17-4.

Table 17-4 *DSCP Codepoints for Beauty Things*

Priority Queue	DSCP Codepoint
Blue	AF31
Red	EF
Green	AF21
Yellow	Default

Scenario Three Questions

The following questions refer to Scenario Three:

1. What are the business constraints for this project?
2. Is MPLS technology appropriate for VoIP?
3. Assuming a g.729 codec, how much bandwidth must be allocated for VoIP packets per store?
4. Assuming a g.729 codec, how much bandwidth must be reserved for VoIP traffic on the WAN link of the headquarters router?
5. Which MPLS priority queue is assigned for VoIP traffic?
   a. Blue
   b. Red
   c. Green
   d. Yellow
6. Which MPLS priority queue is assigned for FTP traffic?
   a. Blue
   b. Red
   c. Green
   d. Yellow
7. What WAN interface solution must be used to prevent large file transfers from interfering and causing delays of VoIP packets?
   a. Priority queuing
   b. Policy routing
   c. Link fragmentation and interleaving
   d. Serialization delay

8. What is the recommended queuing technique for the WAN interfaces?
   a. PQ
   b. Policy queuing
   c. LLQ
   d. Custom queuing

Scenario Three Answers

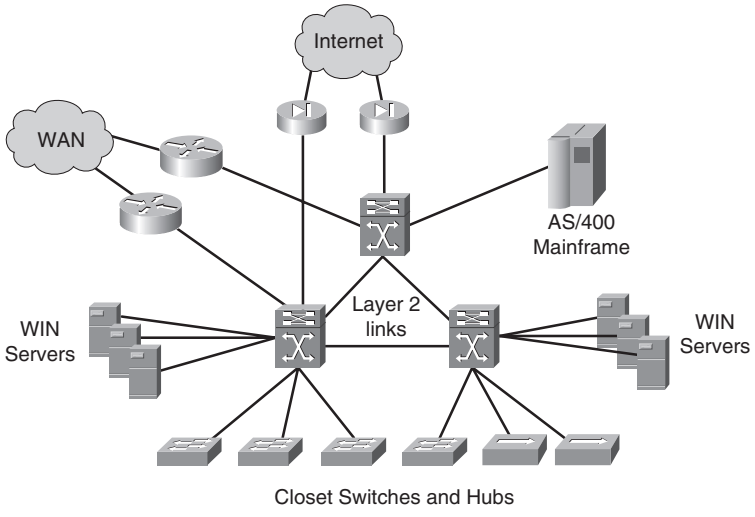
1. The WAN project is to be completed in two months. The VoIP project is to be completed in six months and within budget.
2. Yes, MPLS technology is the preferred WAN technology to support VoIP packets. MPLS provides QoS prioritization and guarantees.
3. 130 kbps. This is calculated by taking five concurrent calls times 26 kbps per call.
4. 7.8 Mbps. This is the sum of VoIP traffic per store multiplied by 60 remote stores.
5. B. VoIP traffic is marked with DSCP expedited forwarding, which corresponds to the Red queue.
6. D. FTP traffic does not require prioritization and thus is assigned to the default Yellow queue.
7. C. LFI should be used on WAN links that are less than 768 kbps. It is used to reduce the serialization delay of large packets.
8. C. LLQ is the recommended queuing technique when VoIP packets are present on WAN links.

Scenario Four: Falcon Communications

Falcon Communications has requested an assessment of its current network infrastructure. You are given the diagram shown in Figure 17-5. The current infrastructure contains three 6500 Catalyst switches connected using Layer 2 links. Building access switches, WAN routers, Internet firewalls, the mainframe, and Windows servers all connect to the 6500 switches. Some Fast Ethernet hubs are used on the network.

The IT manager mentions that they experience sporadic network outages several times during the day, and users are complaining that the network is slow. The CIO states that they want to prepare the network, because the company expects to double in size in three years. They also want to prepare the network for IP telephony.

Figure 17-5 *Falcon Communications Current Network*



Scenario Four Questions

The following questions refer to Scenario Four:

1. Is this network scalable?
2. What would you recommend for the core switches?
3. What changes are required in the closet switches and hubs?
4. What would you recommend for the WAN routers and Internet firewalls?
5. What would you recommend for the AS/400 and WIN server?
6. What is the role of the distribution layer in the architecture?
7. What are your recommendations for IP addressing?
8. Falcon Communications has a VLAN with a /22 IP subnet that is experiencing network delays. What would you recommend?
9. Diagram your proposed solution.

Scenario Four Answers

1. No. The current Falcon network is not scalable. It is a flat network architecture using Layer 2 links in the core with no hierarchy. It does not have core, distribution, and access layers.
2. Recommend inserting a distribution layer to create a hierarchy between the core and access layers. Use Layer 3 links instead of Layer 2 links to prevent spanning-tree loop broadcast storms.
3. All hubs need to be replaced with switches. All switches should be replaced with PoE switches to provide power to future IP phones and wireless access points. All new switch purchases should be PoE-capable LAN switches.

4. Create an enterprise edge layer that separates the campus LAN and the enterprise edge.
5. Create a server distribution and access layer on which to place all servers and the AS/400 mainframe.
6. The distribution layer has several functions:

   Address summarization

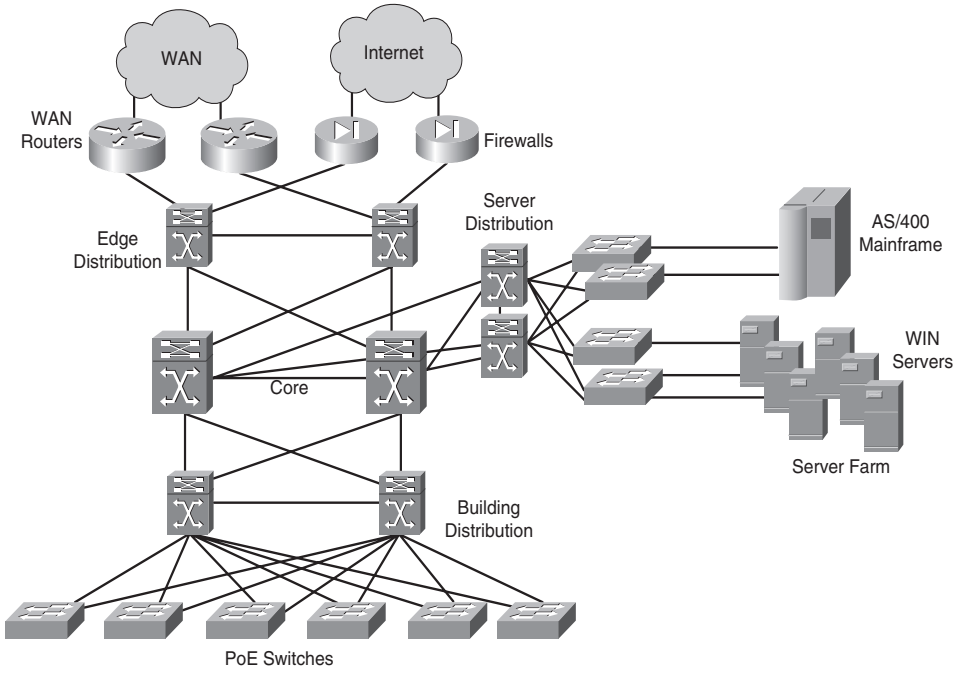
   Security access lists

   Broadcast domain definition

   VLAN routing

   Media translation
7. Recommend allocating /30 subnets for the links between the core and distribution switches. Allocate separate IP subnets for the future IP phones and servers. This lets you apply security policies. Also allocate separate IP subnets for wireless LAN networks.
8. Recommend splitting the IP subnet into four separate /24 IP subnets.
9. The solution shown in Figure 17-6 is a hierarchical network with core, distribution, and access layers. Building access and separate server farms are used. Distribution switches are used to allocate security policies and route summarization. The solution is scalable and will support Falcon Communications' growth plans. PoE switches are deployed to support the future IP telephony deployment.

Figure 17-6 *Falcon Communications Proposed Network Solution*



Appendix B provides a review of the OSI model and TCP/IP architecture. Understanding these frameworks will help you comprehend many concepts covered throughout the book. Numeric conversion will help with understanding binary and hexadecimal numbers.

Part VI: Appendixes

APPENDIX A

Answers to Chapter "Do I Know This Already?" Quizzes and Q&A Sections

Chapter 1

"Do I Know This Already?"

1. B. Integrated Transport, Integrated Service, and Integrated Application are the three phases of IIN.
2. A. Application, Interactive Services, and Network Infrastructure are the layers of SONA.
3. C. Virtualization services occur in the Interactive Service layer of SONA.
4. B. IPCC is a collaboration application. All the others are business applications.
5. A.
6. A, B, C. The PPDIOO methodology has three steps.
7. D. The primary sources of network audits are existing documentation, management software, and new management tools.
8. D. The top-down design approach starts the design from the application layer.
9. B. The examples are organization constraints.
10. C. The examples are technical goals.

Q&A

1. Network Infrastructure layer, Interactive Service layer, and Application layer.
2. Integrated Transport, Integrated Service, and Integrated Application.
3. Identity, Mobility, Storage, Compute, Security, and Voice and Collaboration.
4. Application growth, IT evolution, and increased business expectations from networks.
5. Application-Oriented Network (AON).

6. Prepare, Plan, Design, Implement, Operate, Optimize.
7. i = B, ii = A, iii = C
8. C. SONA evolves enterprise networks to IIN.
9. i = D, ii = F, iii = C, iv = B, v = E, vi = A
10. i = D, ii = A, iii = E, iv = B, v = F, vi = C
11. B. A pilot site is an actual live location for testing.
12. A. A prototype network is a subset of the design in an isolated environment.
13. B.
14. A. Monitoring commands are not SNMP tools.
15. A and B.
16. C and D. The other answers are technical constraints.
17. A, C, E.
18. B, D, F. The other answers are organizational goals.
19. A, B, D, E. Answers C and F are not usually included in the design document.
20. i = D, ii = C, iii = B, iv = F, v = E, vi = A, vii = G
21. C. The network health analysis is based on statistics obtained from the existing network.
22. B. Networks should not contain shared hub segments, and collisions over 1 percent represent an unhealthy segment.
23. C. WAN circuits with sustained utilization of more than 70 percent should have their provisioned bandwidth increased.
24. A, B, C, D, E. All these items are included in a network audit report.
25. C, E, F.

Chapter 2

"Do I Know This Already?"

1. B. The core layer of the hierarchical model is responsible for fast transport.
2. C. The Enterprise Edge consists of e-commerce, Internet connectivity, VPN/remote access, and WAN modules. The Enterprise Edge modules connect to SPs.

3. C. The distribution layer of the hierarchical model is responsible for security filtering, address and area aggregation, and media translation.
4. D. HSRP provides default gateway redundancy. Hosts participating in RIP can find alternative gateways.
5. F. The network-management module monitors all components and functions except the SP Edge.
6. A. The SP Edge includes Internet, PSTN, and WAN modules.
7. C. The server farm hosts campus servers including Cisco CallManager servers.
8. D. The access layer functions are high availability, port security, rate limiting, ARP inspection, virtual access lists, and trust classification.

Q&A

1. False.
2. True.
3. The server farm.
4. True.
5. The Internet submodule.
6. Enterprise Campus, Enterprise Edge, Enterprise WAN, Enterprise Branch, Enterprise Data Center, and Enterprise Teleworker.
7. True.
8. False. A full-mesh network increases costs.
9. Use $n(n – 1)/2$, where $n = 6$. $6(6 – 1)/2 = 30/2 = 15$.
10. Option 1: Single router, dual links to one ISP

    Option 2: Single router, dual links to two ISPs

    Option 3: Dual routers, dual links to one ISP

    Option 4: Dual routers, dual links to two ISPs

    Option 4 provides the most redundancy, with dual local routers, dual links, and dual ISPs.
11. The SP Edge Internet submodule connects to the Enterprise Edge Internet submodule.
12. Cost savings, ease of understanding, easy network growth (scalability), and improved fault isolation.

13. IP phones reside in the building-access layer of the campus infrastructure. The CallManagers are placed in the server farm of the Enterprise Campus.

14. i = C , ii = D, iii = B, iv = A

15. False. Small campus networks can have collapsed core and distribution layers and implement a two-layer design. Medium campus networks can have two-tier or three-tier designs.

16. Use the formula $n(n – 1)/2$, where $n = 10$. $10(10 – 1)/2 = 90/2 = 45$ links.

17. B. The distribution layer provides routing between VLANs and security filtering.

18. E-commerce, Internet, VPN/remote access, and WAN.

19. Internet services, WAN services, and PSTN services.

20. Firewalls, Internet routers, FTP/HTTP servers, SMTP mail servers, and DNS servers.

21. B. The VPN/Remote Access submodule contains firewalls, VPN concentrators, and ASAs.

22. D and E. The access layer concentrates user access and provides PoE to IP phones.

23. B and C. The distribution layer concentrates the network access switches and routers and applies network policies with access lists.

24. A and F. The core layer provides high-speed data transport without manipulating the data.

25. D. The Campus Core connects to the server farm, the Enterprise Edge, and the Building Distribution.

26. E. The infrastructure at the remote site usually consists of a WAN router and a small LAN switch.

27. A, B, C. Web, application, and database servers are placed in the e-commerce submodule.

28. Block 4.

29. Block 1.

30. Block 6.

31. Block 2.

32. Block 5.

33. Block 3.

Chapter 3

"Do I Know This Already?"

1. F. Routers and Layer 3 switches are Layer 3 devices that control and filter network broadcasts.
2. C. The maximum distance of 100BASE-T is 100 meters.
3. G. Every port of a Layer 2 switch, Layer 3 switch, or LAN port on a router is a collision domain.
4. B. Routes are summarized at the distribution layer.
5. B. Layer 3 switches are recommended for the backbone of campus networks.
6. B. CGMP controls multicast traffic at Layer 2.
7. C. Marking is also known as coloring. Marking sets class-of-service (CoS) bits at Layer 2 or type-of-service (ToS) bits at Layer 3.
8. B. Each port on a switch is a separate collision or bandwidth domain. All ports on a hub share the same bandwidth domain.

Q&A

1. False. Layer 2 switches only limit the collision domain.
2. CGMP.
3. True.
4. True.
5. Inter-Switch Link (ISL) and IEEE 802.1p/802.1Q.
6. A. IP phone-to-IP phone communication is an example of peer-to-peer communication.
7. A, C, E. Network applications, infrastructure devices, and environmental characteristics affect network design.
8. C. Multimode fiber provides the necessary connectivity at the required distance. UTP can reach only 100 m. Single-mode fiber would be more expensive.
9. B. The DC aggregation layer is similar to the campus distribution layer.
10. C. Disabling trunking on host ports and using RPVST+ are best practices at the access layer.
11. B. The use of HSRP and summarization of routes are best practices in the distribution layer.
12. A. Best practices for the core is the use of triangle connections to reduce switch peering and use routing to prevent network loops.

13. D. Load balancers, SSL offloading, firewalls, and intrusion detection devices are deployed in the DC aggregation layer.

14. D. All are threats to the Enterprise Edge distribution.

15. C. Create a server farm that allows the enforcement of security policies.

16. B. These are design considerations for the distribution layer.

17. D. All are server connectivity options.

18. A. The core and the distribution should be connected using redundant Layer 3 triangular links.

19. B. The building subnets are too large and should be further segmented to reduce the broadcast domain.

20. B. Broadcasts are not forwarded by routers and are controlled by VLANs.

21. i = C, ii = A, iii = B, iv = E, v = D

22. True. Layer 3 switches and routers control both the collision and broadcast domains.

23. i = A, ii = C, iii = B

24. i = E, ii = A, iii = C, iv = D, v = B

25. i = B, ii = A, iii = D, iv = C

26. i = B, ii = D, iii = C, iv = A

27. True. IP phones reclassify incoming frames from the PC. Switches can accept or reclassify incoming frames.

28. CGMP and IP snooping control multicast traffic at Layer 2. The switch and local router exchange CGMP messages. With IGMP snooping, the switch listens to IGMP messages between the host and the router.

29. ISL and IEEE 802.1p/Q are two methods for CoS. ISL was created by Cisco and uses an external tag that contains 3 bits for marking. IEEE 802.1p specifies 3 bits for marking that is carried in the internal tag of IEEE 802.1q. The IEEE 802.1p specification is not included in the IEEE 802.1D-1998 standard.

30. False. You can configure the CGMP only if both the router and switch are Cisco devices.

31. The campus backbone should have high-speed links. Recommend Gigabit Ethernet links.

32. The IP phones should remap the workstation traffic to a value less than the value assigned to voice. Typically, it is recommended that you configure the IP phone to set the CoS to 5 for VoIP traffic.

33. Inspect them at the Layer 3 switches in Building A. Packets should be marked and accepted as close as possible to the source.

34. No. There is no redundancy to the WAN module. A separate link to another building would provide that redundancy.

35. No. There is no redundancy to the Internet module. A separate link from another building would provide that redundancy.

36. Yes. The network uses Layer 2 switches at the building-access layer and Layer 3 switches at the building-distribution and campus-backbone layers.

Chapter 4

"Do I Know This Already?"

1. C. Only 802.11a uses UNII frequencies.

2. B. The Industrial, Scientific, and Medical (ISM) band of frequencies provides 11 channels for wireless LANs.

3. D. Lightweight Access Point Protocol (LWAPP) is a draft Internet Engineering Task Force (IETF) standard for control messaging for setup, authentication, and operations between access points (AP) and wireless LAN controllers (WLC).

4. B. The service-port interface is an optional interface that is statically configured for out-of-band management.

5. B. The Cisco Catalyst 3750 Integrated WLC supports up to 50 APs.

6. C. With N+N+1 redundancy, an equal number of controllers back up each other, as with N+N. Plus, a backup WLC is configured as the tertiary WLC for the access points.

7. B. The recommended best practice is up to 20 WLAN clients.

8. D. Mesh Access Points (MAP) connect to the RAP to connect to the wired network.

Q&A

1. 54 Mbps

2. 200 Mbps

3. Having to configure SSIDs, frequency channels, and power settings for dispersed APs.

4. Advanced Encryption Standard (AES)

5. Reduced TCO
   Enhanced visibility control
   Dynamic RF management
   WLAN security

Unified wired and wireless network
Enterprise mobility
Enhanced productivity and collaboration

6. False. With Split-MAC, control and data traffic frames are split. LWAPs communicate with the WLCs with control messages over the wired network. LWAPP data messages are encapsulated and forwarded to and from wireless clients.

7. True. Controller MAC functions are association requests, resource reservation, and authentication and key management.

8. C. Layer 3 LWAPP tunnels are the preferred solution.

9. B. Layer 2 intercontroller roaming is the preferred intercontroller roaming option.

10. B. The WLC places the user data on the appropriate VLAN and forwards the frame to the wired network.

11. C. Each 4400 series WLC supports 100 APs. 100 APs times 24 controllers in a mobility group equals 2400.

12. D. The recommended number of data devices per AP is 20.

13. B. The recommended number of voice over wireless devices per AP is seven for g.711 and eight for g.729.

14. C. Cisco Radio Resource Management controls AP radio frequency and power settings.

15. A. Typically, there is a 2- to 3-ms latency per hop.

16. C. The RTT between the AP and WLC should not exceed 100 ms.

17. D. Cisco recommends deterministic controller redundancy.

18. D. EoIP is the recommended method for guest services.

19. A. H-REAP with centralized controllers is recommended for branch WLAN design.

20. B and D. Recommended practices are minimizing intercontroller roaming and centralizing controller placement.

21. D. The Cisco 6500 WLC module supports 300 access points.

22. i = D, ii = E, iii = A, iv = F, v = B, vi = C

23. i = E, ii = D, iii = C, iv = B, v = A

24. i = B, ii = A, iii = C

25. i = B, ii = A, iii = E, iv = C, v = D

26. i = C, ii = D, iii = A, iv = B

27. B. For best performance, 20 MAP nodes are recommended per RAP.

28. D. Only answer D has the correct order.

29. B. Radio Resource Management (RRM) functions include radio resource monitoring, dynamic channel assignment, interference detection and avoidance, dynamic transmit power control, coverage hole detection and correction, and client and network load balancing.

30. B. Channels 1, 6, and 11 of the ISM frequencies do not overlap.

31. A. Only answer A is correct.

32. C. LEAP uses mutual authentication between the client and the network server and uses IEEE 802.1X for 802.11 authentication messaging. LEAP uses a RADIUS server to manage user information.

Chapter 5

"Do I Know This Already?"

1. C. DMZ/E-Commerce, Internet, Remote Access VPN, and WAN/MAN are all network modules found in the Enterprise Edge.

2. B. The singling protocol used between the Frame Relay switch and the router is called Local Management Interface (LMI).

3. D. A TDM T1 circuit provides 1.5.44 Mbps of bandwidth.

4. C. The Cisco PPDIOO methodology is used when designing the Enterprise Edge.

5. C. The architecture of Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) is circuit-based and delivers high-speed services over an optical network.

6. B. With ASDL, the downstream bandwidth is asymmetric, or higher than the upstream bandwidth, and is very popular in residential environments.

7. B. Frame Relay network discards frames marked with the DE bit of 1 before those marked with 0.

8. D. Frame Relay technology supports full mesh configurations when connecting multiple sites together.

9. D. The window size defines the upper limit of frames that can be transmitted without getting a return acknowledgment.

10. A. Low-Latency Queuing (LLQ) adds a strict priority queue to CBWFQ.

Q&A

1. D. After analyzing the customer requirements, the next step is to characterize the existing network.
2. B. The Enterprise Edge modules connect to the enterprise campus via the campus core module.
3. D. The high speeds and relatively low cost of DSL make this a very popular internet access technology for the enterprise telecommuter.
4. C and D. DMZ/E-Commerce, Internet, Remote Access VPN, and WAN/MAN are modules that are found in the Enterprise Edge.
5. A. The window size defines the upper limit of frames that can be transmitted without getting a return acknowledgement. The larger the window size, the smaller number of acknowledgement that need to take place.
6. B. WFQ is the default QoS mechanism on interfaces below 2.0 Mbps.
7. A, B, D. The PPDIOO design methodology includes the process of analyzing network network requirements, characterizing the existing network, and designing the topology.
8. D. DMZ/E-Commerce, Internet, Remote Access VPN, and WAN/MAN are modules that are found in the Enterprise Edge.
9. C and D. DMZ/E-Commerce and Internet are modules that are found in the Enterprise Edge.
10. A. The remote access/vpn module connects to PSTN type connectivity.
11. B. WAN/MAN are modules that use Frame Relay and ATM and are found in the Enterprise Edge.
12. B. After you analyze the network requirements and characterize the existing network, the design of the topology occurs which includes the implementation planning.
13. D. The WAN/MAN functional area or module provides connectivity to the remote sites via Frame Relay, TDM, ATM, or MPLS services.
14. D. The framing for dark fiber is determined by the enterprise not the provider.
15. D. Low Latency Queuing (LLQ) adds a strict priority queue to CBWFQ.
16. 24
17. False. Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD).
18. False. DSL uses digital technology over phone lines.
19. True. SONET/SDH uses a ring topology by connecting sites together and providing automatic recovery capabilities and has self-healing mechanisms.

20. False. During periods of congestion, the Frame Relay network will discard frames marked with the DE bit of 1 first before those marked with zero.

21. C. Wireless bridges are used to connect two separate wireless network together typically located in two separate buildings.

22. DWDM. DWDM maximizes the use of the installed base of fiber used by service providers and is a critical component of optical networks.

23. CMTS. The equipment used on the remote access side is the cable modem which connects to the Cable Modem Termination System or (CMTS) on the Internet Service provider side.

24. A. The WAN/MAN module provides connectivity to the remote sites via Frame Relay, TDM, ATM, or SONET network services.

25. True. Designing WANs use two primary design goals which include application availability and cost and usage.

26. True. A common use for dial-up is with remote or teleworker using it as a backup network solution in the event that their DSL or cable connection goes down.

27. False. PVCs are used more predominately due to the permanent nature of the connections.

28. True. With ASDL, the downstream bandwidth is asymmetric or higher than the upstream bandwidth.

29. DOCSIS. The Data Over Cable Service Interface Specifications (DOCSIS) protocol defines the cable procedures that the equipment need to support.

Chapter 6

"Do I Know This Already?"

1. A. Frame Relay and ATM are commonly used to connect to WAN services in the Enterprise Edge.

2. A, B, C. Typical remote access requirements include best-effort interactive traffic patterns, connections to Enterprise Edge via Layer 2 WAN technologies, and voice and VPN support.

3. C. Extranet VPN infrastructure uses private and public networks to support business partner connectivity.

4. B. Secondary WAN links offer both backup and load-sharing capabilities.

5. C. The goal of high availability is to remove the single points of failure in the design, either by software, hardware, or power. Redundancy is critical in providing high levels of availability.

6. C. SP MPLS MPLS/IP VPN has excellent growth support and high availability services.
7. B. Cisco IOS S Releases 12.2SB and 12.2SR are designed for the Enterprise and SP edge networks.
8. A, B, D. Common components used when designing Enterprise Branch Architecture are routers, switches, and IP phones.
9. B. The dual-tier design is recommended for branch offices of 50 to 100 users, with an additional access router in the WAN edge allowing for redundancy services.
10. C. The multi-tier profile supports between 100 to 1000 users, dual routers, dual firewalls, and multiple distribution switches for aggregation to the access layer switches.

Q&A

1. B. Leased lines are dedicated network connections provided by the service provider.
2. A. A major disadvantage of the hub and spoke topology is that the hub router represents a single point of failure.
3. B. Full-mesh topologies require that each site has a connection to all other sites in the WAN cloud.
4. A. Circuit-switched data connections, such as ISDN service, can be brought up when needed and terminated when finished.
5. C. Access VPN connections give users connectivity over shared networks such as the Internet to their corporate intranets.
6. True. Overlay VPNs are built using traditional WAN technologies such as Frame Relay and ATM.
7. B. With peer-to-peer VPNs, the server provider plays an active role in enterprise routing.
8. B. Service providers can offer shadow PVCs, which provide additional permanent virtual circuit (PVC) for use if needed.
9. C. A secondary WAN links provide advantages that include backup WAN services and load sharing.
10. True. Fast switching is enabled on WAN links that are faster than 56 kbps, and per-destination load balancing is preferred.
11. True. IPsec protocols protect data being transport over the Internet, such as with WAN backup services.

12. A and C. IPsec and GRE are methods that exist for tunneling private networks over a public IP network.

13. C. Factors for WAN architecture selection include ongoing expenses, ease of management, and high availability.

14. A. This approach is simple Layer 3 tunneling for basic IP VPNs without using encryption.

15. True. IPsec encrypted connectivity over the private WAN is optional.

16. B. ISP service uses Internet-based site-to-site VPNs.

17. False. Hardware selection involves modularity of add-on hardware and port densities.

18. False. Redundany and modularity are both considerations when selecting Enterprise Edge hardware.

19. False. The Cisco IOS software family IOS XR is designed for the service provider core.

20. False. The Cisco IOS software family IOS T is designed for access routing platforms for the enterprise.

21. B. A private WAN with self-deployed MPLS is usually reserved for very large enterprises that are willing to make substantial investments in equipment and training to build out the MPLS network.

22. IP Base.

23. True. At the top is the premium package, Advanced Enterprise Services. It combines all features and supports all routing protocols with voice, security, and VPN technologies.

24. D. The IOS package IP Voice supports converged voice and data.

25. True. The Cisco 2970, 3560, and 3750 series switches provide low-end to midrange LAN switching for enterprise access and distribution deployments.

26. False. Cisco Enterprise Branch Architecture is based on Cisco's Service-Oriented Network Architecture (SONA), which includes plug-in modules that provide remote connectivity to network endpoints.

27. True. Common components used when designing Enterprise Branch Architecture are routers, switches, PCs, and IP phones.

28. i = A, ii = C, iii = D, iv = B

Chapter 7

"Do I Know This Already?"

1. C. IPv4 private addresses are contained within 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
2. B. There are 5 host bits: $2^5 - 2 = 30$ hosts.
3. D. Loopback addresses should have a /32 mask so that address space is not wasted.
4. C. The precedence bits are located in the type-of-service field of the IPv4 header.
5. B. Multicast addresses range from 224.0.0.1 to 239.255.255.255.
6. B. ARP maps IPv4 addresses to Layer 2 MAC addresses.
7. D. Point-to-point links need only two host addresses; use a /30 mask, which provides $2^2 - 2 = 2$ host addresses.
8. C. DHCP assigns IP addresses dynamically.
9. B. NAT translates between IPv4 private addresses and public addresses.
10. C. The DS field allocates 6 bits in the ToS field, thus making it capable of 64 distinct codepoints.

Q&A

1. 10/8, 172.16/12, and 192.168/16
2. You use VLSM to subdivide a network into subnets of various sizes, whereas CIDR permits the aggregation of classful networks.
3. DNS
4. True. You can use DHCP to specify several host IP configuration parameters, including IP address, mask, default gateway, DNS servers, and TFTP server.
5. False. The bit-number representation of 255.255.255.248 is /29. /28 is the same mask as 255.255.255.240.
6. True.
7. 20 (bytes)
8. DSCP uses 6 bits, which provides 64 levels of classification.
9. True.
10. False. The header checksum field only includes a checksum of the IP header; it does not check the data portion.

11. The subnet is 172.56.4.0/22, the address range is from 172.56.4.1 to 172.56.7.254, and the subnet broadcast is 172.56.7.255.
12. The IP layer in the destination host.
13. B. DHCP configures the IP address, subnet mask, default gateway, and other optional parameters.
14. C. Class B networks have 16 bits for host addresses with the default mask: $2^{16} - 2 = 65{,}534$.
15. B. A /26 mask has 26 network bits and 6 host bits.
16. C. Network 192.170.20.16 with a prefix of /29 summarizes addresses from 192.170.20.16 to 192.170.20.23.
17. B. AF Class 3 is backward-compatible with IP precedence priority traffic with a binary of 011.
18. A. IPv4 packets can be fragmented by the sending host and routers.
19. B. Multicast addresses are received to a set of hosts subscribed to the multicast group.
20. Unicast, multicast, and broadcast.
21. B. The networks in answer B provide 126 addresses for hosts in each LAN at Site B.
22. A. Network 192.168.15.0/25 provides 126 addresses for LAN 1, network 192.168.15.128/26 provides 62 addresses for LAN 2, and network 192.168.15.192/27 provides 30 addresses for LAN 3.
23. D. You need only two addresses for the WAN link, and the /30 mask provides only two.
24. A. Private addresses are not announced to Internet service providers.
25. B. NAT translates internal private addresses to public addresses.
26. D. VLSM provides the ability to use different masks throughout the network.

Chapter 8

"Do I Know This Already?"

1. C. IPv6 uses 128 bits for addresses, and IPv4 uses 32 bits. The difference is 96.
2. C. The IPv6 header is 40 bytes in length.
3. C. The defining first hexadecimal digits for link-local addresses are FE8.
4. D. IPv6 addresses can be unicast, anycast, or multicast.
5. B. Answers A and C are incorrect because you cannot use the double colons (::) twice. Answers C and D are also incorrect because you cannot reduce b100 to b1.

6. C. NAT-PT translates between IPv4 and IPv6 addresses.
7. B. The IPv6 multicast address type handles broadcasts.
8. B. The IPv6 loopback address is ::1.
9. A. IPv4-compatible IPv6 addresses have the format ::d.d.d.d.
10. C. The DNS maps fully qualified domain names to IPv6 addresses using (AAAA) records.

Q&A

1. False. OSPFv3 supports IPv6. OSPFv2 is used in IPv4 networks.
2. True.
3. ARP
4. 16
5. 0110. The first field of the IPv6 header is the version field. It is set to binary 0110 (6).
6. False.
7. 0xFF (1111 1111 binary)
8. FE8/10
9. True.
10. Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, IPv6 Source Address, IPv6 Destination Address.
11. B. IPv6 address types are unicast, anycast, and multicast.
12. True. Both compressed representations are valid.
13. 2001:1:0:ab0::/64
14. 32
15. It is a multicast address. All IPv6 multicast addresses begin with hexadecimal FF.
16. C. Answers A, B, and D are incorrect because 0100 does not compact to 01. Answer B is also incorrect because 0010 does not compact to 001.
17. A. The dual-stack backbone routers handle packets between IPv4 hosts and IPv6 hosts.
18. B. DNS indicates which stack to use. DNS A records return IPv4 addresses. DNS AAAA records return IPv6 addresses.

19. IPv6 over dedicated links
IPv6 over IPv4 tunnels
IPv6 using dual-stack backbones
Protocol-translation mechanisms

20. A and D.

21. D. IPv4 packets can be fragmented by the sending host and routers. IPv6 packets are fragmented by the sending host only.

22. A. Anycast addresses reach the nearest destination in a group of hosts.

23. D

24. Implement a dual-stack backbone, or implement IPv4 tunnels between the sites.

25. NAT-PT is required to provide network address translation and protocol translation between IPv6 and IPv4 hosts.

26. If a dual-stack backbone is implemented, only the WAN routers require an IPv6-IPv4 dual stack. End hosts do not need a dual stack.

27. No. All WAN routers still run the IPv4 stack, with two exceptions: the WAN routers at Sites A and B. These routers speak IPv6 within their sites and speak IPv4 to the WAN.

Chapter 9

"Do I Know This Already?"

1. D. Only RIPv1 is a classful routing protocol. EIGRP, OSPF, IS-IS, and RIPv2 are classless routing protocols.

2. C. You use an exterior gateway protocol (EGP) to receive Internet routes from a service provider.

3. A. RIPv2 is a classless distance-vector routing protocol.

4. B. Distance-vector routing protocols send periodic updates.

5. B. RIPng is a distance-vector routing protocol that is used in IPv6 networks.

6. B. If bandwidth is used, the path with the highest bandwidth is selected. If cost is used, the path with the lowest cost is selected.

7. B. OSPF has an administrative distance of 110. EIGRP has an administrative distance of 90. The route with the lower administrative distance is selected: EIGRP.

8. D. EIGRP, RIPv2, IS-IS, and OSPF are all classless routing protocols.

Q&A

1. RIPv1 and IGRP. These protocols are classful.
2. False. Distance-vector routing protocols send periodic routing updates.
3. False. RIPng is used with IPv6 networks.
4. True.
5. True. The higher value for reliability is preferred.
6. False. The link with the lower load is preferred.
7. The EIGRP route. EIGRP routes have an administrative distance of 90, and OSPF routes have an administrative distance of 100. The lower administrative distance is preferred.
8. The IS-IS route. IS-IS routes have an administrative distance of 115, and RIP routes have an administrative distance of 120. The lower administrative distance is preferred.
9. The OSPF route, because it has a more specific route.
10. A. The best reliability is 255/255 (100 percent), and the best load is 1/255 (~0 percent).
11. G. IS-IS and OSPF permit an explicit hierarchical topology.
12. Delay measures the amount of time a packet takes to travel from one end to another in the internetwork.
13. OSPF cost. The Cisco default metric is 10^8/BW.
14. The metric is 10^8/BW. If BW = 100 Mbps = 10^8, the metric = $10^8/10^8 = 1$.
15. i = C, ii = A, iii = D, iv = B.
16. True.
17. B, D, E, F.
18. B. OSPFv3 is the only standards-based routing protocol in the list that supports large networks. RIPng has limited scalability.
19. C. IS-IS is deployed by ISPs, not in enterprise networks.
20. C, D, E. Link-state routing protocols plus EIGRP's hybrid characteristics converge faster.
21. C. EIGRP supports large networks and does not require a hierarchical network.
22. B, C, D, E. RIPv1 does not support VLSMs.
23. F. BGP is used to connect to ISPs.
24. C. EIGRP is supported only on Cisco routers.

25. D. OSPFv3 is the only correct answer. RIPv2 is for IPv4 networks. EIGRP is not standards-based. BGPv6 and RIPv3 do not exist.

26. CDP. Cisco Discovery Protocol (CDP) provides for communication between hub and stub routers when using ODR.

27. C.

28. A is EIGRP for IPv6, B is OSPF, C is RIPv2, D is EIGRP, E is OSPFv3.

29. A. The minimum bandwidth via Route 1 is 384 kbps. The minimum bandwidth via Route 2 is 128 kbps. The route with the higher minimum bandwidth is preferred, so the router chooses Route 1.

30. B. Route 2 has fewer router hops than Route 1.

31. A. Route 2 has a higher cost than Route 1. The Route 2 cost is 10^8/128 kbps = 781.25. The Route 1 cost is 10^8/512 kbps + 10^8/384 kbps + 10^8/512 kbps = 195.31 + 260.41 + 195.31 = 651.03. Route 1 is preferred.

Chapter 10

"Do I Know This Already?"

1. C. RIPv1 and RIPv2 are limited to 15 router hops.

2. A. RIPv2 broadcasts every 30 seconds.

3. B. RIPv2 implements support for VLSMs and an authentication mechanism for route updates and can multicast rather than broadcast updates.

4. D. EIGRP routers maintain adjacencies with their neighboring routers. The adjacencies are kept in a topology table.

5. B. RIPng and EIGRP are the only distance-vector routing protocols that support IPv6.

6. B. By default, EIGRP uses bandwidth and delay in its composite metric.

7. D. RIPv2, EIGRP, OSPF, and IS-IS support VLSMs.

8. C. Only EIGRP implements DUAL. DUAL selects the best path and second-best path to a destination.

Q&A

1. False. RIPv2 multicasts its routing table to 224.0.0.9. It does not send a broadcast to all nodes in the segment.

2. False. By default, EIGRP uses bandwidth and delay to calculate the composite metric.

3. True. EIGRP routers build a table of adjacent EIGRP neighbors.
4. True.
5. False. Both RIPv1 and RIPv2 have a 15-router-hop limit.
6. RIP uses UDP port 520.
7. RIPng uses UDP port 521.
8. EIGRP uses IP protocol 88.
9. EIGRP is preferred for large networks.
10. You would use RIPv2 because IGRP and EIGRP are available only on Cisco devices.
11. EIGRP uses DUAL for fast convergence and loop prevention.
12. i = D, ii = B, iii = A, iv = C
13. EIGRP combines characteristics commonly associated with both distance-vector and link-state routing protocols.
14. C. To reduce the broadcast traffic, use EIGRP for IPv4 as the routing protocol for the network. RIPv2 still generates periodic broadcasts. EIGRP for IPv6 and RIPng are used in IPv6 networks.
15. RIPng does not include authentication. It uses the authentication schemes of IPv6.
16. i = C, ii = B, iii = D, iv = A, v = E
17. i = B, ii = D, iii = A, iv = C
18. Equal-cost load balancing is a feature of RIPv1 and RIPv2 with Cisco routers.
19. Unequal-cost load balancing is a feature of IGRP and EIGRP with Cisco routers.
20. B. EIGRP does not require a hierarchical topology. RIPv2 does not scale for large networks. OSPF and IS-IS require a hierarchical topology. IS-IS is not recommended in enterprise networks.
21. i = C, ii = A, iii = D, iv = B
22. B. The EIGRP route has a lower administrative distance.
23. H. EIGRP is proprietary.

24.

Characteristic	RIPv1	RIPv2	RIPng	EIGRP	EIGRP for IPv6
Authentication	No	Yes	No	Yes	Yes
Protocol/port	UDP 520	UDP 520	UDP 521	IP 88	Next Header 88
Administrative distance	120	120	120	90	90
IP version	IPv4	IPv4	IPv6	IPv4	IPv6

25. A. From Router A, Path 1 is one router hop, and Path 2 is three router hops. RIPv2 selects Path 1 because of the lower metric.

26. A. From Router A, Path 1 is one router hop, and Path 2 is three router hops. RIPng selects Path 1 because of the lower hop count metric.

27. B. From Router A, the lowest bandwidth (BW_{min1}) in Path 1 is 256 kbps; the lowest bandwidth in Path 2 (BW_{min2}) is 512 kbps. With the default delay values, the EIGRP metric calculation would be more sensitive to the bandwidth component of the metric calculation. EIGRP selects the path with the greatest minimum bandwidth.

28. C. By default, EIGRP load-balances using equal-cost paths. EIGRP does unequal load balancing when you use the variance command.

29. B. Regardless of IPv4 or IPv6, EIGRP uses the fastest bandwidth (and lowest delay) for best path calculations. From Router A, the lowest bandwidth (BW_{min1}) in Path 1 is 256 kbps; the lowest bandwidth in Path 2 (BW_{min2}) is 512 kbps. With the default delay values, EIGRP selects the path with the greatest minimum bandwidth: 512 kbps (path 2) is selected over 256 kbps (path 1).

Chapter 11

"Do I Know This Already?"

1. B. OSPF defines ABRs that connect areas to the OSPF backbone.

2. G. EIGRP, OSPF, and IS-IS support VLSMs.

3. D. IS-IS is a common alternative to EIGRP and OSPF for Service Provider networks.

4. B. OSPF defines the ASBR as the router that injects external routes into the OSPF autonomous system.

5. B. The default IS-IS cost metric for any interface type is 10.

6. E. OSPFv2 Type 5 LSAs are AS external LSAs.

7. C. OSPFv2 routers use 224.0.0.6 to communicate with DRs.
8. A. Type 1 LSAs (router LSAs) are forwarded to all routers within an OSPF area.
9. D. IS-IS does not define BDRs.
10. D. Intra-Area-Prefix LSAs carry IPv6 prefixes associated with a router, a stub network, or an associated transit network segment.

Q&A

1. False. A router with one or more interfaces in Area 0 is considered an OSPF backbone router.
2. True.
3. 224.0.0.5 for ALLSPFRouters and 224.0.0.6 for ALLDRouters.
4. FF02::5 for ALLSPFRouters and FF02::6 for ALLDRouters.
5. The administrative distance of OSPF is 110, and the administrative distance of IS-IS is 115.
6. True. By default, IS-IS assigns a cost metric of 10 to all interfaces.
7. OSPF ABRs generate the Type 3 summary LSA for ABRs.
8. OSPF DRs generate Type 2 network LSAs.
9. Included are the router's links, interfaces, state of links, and cost.
10. True.
11. False. The router with the highest priority is selected as the OSPF designated router.
12. i = C, ii = B, iii = A, iv = D
13. OSPF DRs produce OSPF network LSAs for broadcast multi-access networks.
14. False. IS-IS uses Layer 2 OSI PDUs to communicate between routers.
15. Cost is calculated as 10^8/BW, and BW = 100 Mbps = 10^8 bps for Fast Ethernet. Cost = $10^8/10^8 = 1$.
16. OSPF and IS-IS are the only link-state routing protocols, and they both support VLSMs.
17. OSPF. Although RIPv2 and EIGRP support VLSMs, you should use RIPv2 only on the edge. EIGRP is not supported on non-Cisco routers.
18. True. L1/L2 routers maintain separate link-state databases for Level 1 and Level 2 routes. ABRs maintain separate link-state databases for each area they are connected to.
19. Virtual links. You use virtual links to temporarily connect an OSPF area to the backbone.
20. You do not need to flood external LSAs into the stub area, which reduces LSA traffic.

21. All traffic from one area must travel through Area 0 (the backbone) to get to another area.
22. False. For Fast Ethernet, the OSPF cost is 1 and the IS-IS cost is 10.
23. OSPFv3 is identified as IPv6 Next Header 89.
24. F. EIGRP and OSPFv2 are recommended for large enterprise networks.
25. C. Link LSAs are flooded to the local link.
26. F.
27. E. EIGRP and OSPFv2 have fast convergence.
28. E. EIGRP for IPv6 and OSPFv3 have fast convergence for IPv6 networks.
29. H. RIPv1 and RIPv2 generate periodic routing traffic. IS-IS is used in SP networks. BGP is used for external networks.
30. B. OSPFv3 is used in IPv6 networks.
31. A. From Router A, Path 1 has an IS-IS cost of 10 + 10 = 20. Path 2 has an IS-IS cost of 10 + 10 + 10 + 10 = 40. Path 1 is selected.
32. B. From Router A, the OSPF cost for Path 1 is 10^8/256 kbps = 390. The OSPF cost for Path 2 is (10^8/1536 kbps) + (10^8/1024 kbps) + (10^8/768 kbps) = 65 + 97 + 130 = 292. OSPF selects Path 2 because it has a lower cost.
33. Router A = Internal
    Router B = ABR
    Router C = Backbone
    Router D = ASBR
    Router E = ABR
    Router F = Internal

Chapter 12

"Do I Know This Already?"

1. B. You use External Border Gateway Protocol (eBGP) to exchange routes between autonomous systems.
2. C. The current version of BGP is Version 4. BGPv4 includes support for CIDR.
3. B. It is a best practice to summarize routes on the distribution routers toward the core.
4. D. PBR changes packets' routes based on configured policies.
5. B. You use IGMP between hosts and local routers to register with multicast groups.

6. B. The lower 23 bits of the IP multicast address are mapped to the last 23 bits of the Layer 2 MAC address.
7. A. The administrative distance of eBGP routes is 20. The administrative distance of internal BGP (iBGP) routes is 200.
8. D. CIDR provides the capability to forward packets based on IP prefixes only, with no concern for IP address class boundaries.

Q&A

1. False. You use eBGP to exchange routes between different autonomous systems.
2. True. BGPv4 added support for Classless Interdomain Routing (CIDR), which provides the capability of forwarding packets based on IP prefixes only, with no concern for the address class.
3. True.
4. PBR
5. 20, 200
6. True.
7. False. PIM does not have a hop-count limit. DVMRP has a 32 hop-count limit.
8. True.
9. False. BGP uses several attributes in the BGP decision process.
10. RIPv2, OSPF, and EIGRP.
11. FF02::A
12. i =D, ii = B, iii = A, iv = C
13. i = B, ii = C, iii = D, iv = A
14. Weight. Weight is configured locally and not exchanged in BGP updates. On the other hand, the local preference attribute is exchanged between iBGP peers and is configured at the gateway router.
15. Route reflectors reduce the number of iBGP logical mesh connections.
16. External peers see the confederation ID. The internal private AS numbers are used within the confederation.
17. BGP confederations, route reflectors.
18. B. Only answer B has the correct order of BGP path selection, which is weight, local preference, AS path, origin, MED, and lowest IP.

19. CIDR was first implemented in BGPv4.
20. C.
21. i = E, ii = C, iii = A, iv = B, v = D
22. B.
23. C.
24. B. BGP should be configured between AS 100 and AS 500.
25. C. Both Routers A and B perform the redistribution with route filters to prevent route feedback.
26. B. The OSPF routes are redistributed into EIGRP. Then you can redistribute EIGRP routes into BGP.
27. D. You should use filters on all routers performing redistribution.

Chapter 13

"Do I Know This Already?"

1. C. The U.S. Health Insurance Portability and Accountability Act (HIPAA) applies to the protection of private health information that is used electronically.
2. B. Reconnaissance techniques are used to gather information from hosts attached to the network.
3. A. Denial of service (DoS) attacks aim to overwhelm resources such as memory, CPU, and bandwidth, thus impacting the target system and denying legitimate users access.
4. D. Rate limiting can control the rate of bandwidth that is used for incoming traffic such as ARPs and DHCP requests.
5. C. When an attacker changes sensitive data without the proper authorization, this is called an integrity violation.
6. B. The incident-handling policy defines the processes and procedures for managing incidents and emergency type scenarios.
7. D. Identification of assets, definitions of roles and responsibilities, and a description of permitted behaviors should be included in a security policy.
8. A, B, C. Authentication of an identity is based on something the subject knows, has, or is, such as password, token, and fingerprint, respectively.
9. A. Asymmetric cryptography uses two different keys for encryption and relies on PKI.

10. A, B, C. Threat Defense has three main areas of focus that include enhancing the security of the existing network, adding full security services to network endpoints, and enabling integrated security in routers, switches, and appliances.

Q&A

1. C. Encryption can protect data transported between sites over the Internet.
2. A and C. Firewalls and host-based security have the capabilities to protect database servers, such as in a DMZ segment.
3. D. Encryption is a security technique for protecting the data confidentiality of information.
4. A and B. The use of ACLs and rate limiting can alleviate the effects of a DoS attack being preformed.
5. A and D. DoS, reconnaissance, and gaining unauthorized access are security threats.
6. True. IPsec can ensure data integrity and confidentiality across the Internet.
7. C. SOX focuses on the accuracy and controls imposed on a company's financial records.
8. A, B, C. Managing the security infrastructure has components that include the overall security management policy, incident-handling policy, and network access control policy.
9. C. EU Data Protection Directive calls for the protection of the people's right to privacy with respect to the processing of personal data.
10. False. HIPAA applies to the protection of private health information that is used electronically.
11. True. Distributed DoS attacks are when multiple sources work together to deliver an attack.
12. True. Social engineering involves manipulating users into giving out confidential information.
13. D. Attackers can use password-cracking utilities, capture network traffic, and use social engineering to obtain sensitive information.
14. D. Data integrity allows only authorized users to modify data, ensuring that the data is authentic.
15. Some targets that are used for attacks include routers, switches, firewalls, and servers.
16. B. Accounting provides an audit trail of activities by logging the actions of the user.
17. DHCP snooping authenticates valid DHCP servers, thereby preventing rouge DHCP servers from interfering with real production servers.
18. True. Unicast RPF is used to prevent unknown source addresses from using the network as a transport.

19. Rate limiting can control the rate of traffic that is allowed into the network.
20. The security policy contains the organization's procedures, guidelines, and standards.
21. D. Access control can be enforced by restricting access using VLANs, OS-based controls, and encryption techniques.
22. Acceptable-use policy.
23. True. The network access control policy defines the general access control principles used and how data is classified, such as confidential, top-secret, or internal.
24. D. Secure—Identification, authentication, ACLs, stateful packet inspection (SPI), encryption, and VPNs

    Monitor—Intrusion and content-based detection and response

    Test—Assessments, vulnerability scanning, and security auditing

    Improve—Security data analysis, reporting, and intelligent network security
25. True. The Cisco Self-Defending Network Trust and Identity Management defines who and what can access the network, as well as when, where, and how that access can occur.
26. True. Tokens such as a six-digit PIN and a token code are used in the two-factor authentication technique.
27. i = B, ii = C, iii = A, iv = D

Chapter 14

"Do I Know This Already?"

1. A, B, C. Critical components of the Cisco Self-Defending Network include Trust and Identity Management, Threat Defense, and Secure Connectivity.
2. C. The Cisco ASAs provide high-performance firewall, IPS, anti-X, IPsec, and VPN services.
3. B. 802.1x is an IEEE media-level access control standard that permits and denies admission to the network and applies traffic policy based on identity.
4. A. Network Access Control (NAC) protects the network from security threats by enforcing security compliance on all devices attempting to access the network.
5. D. The Cisco ASA, FWSM, and PIX security appliances all support firewall filtering with ACLs.
6. A. The Cisco Security Agent is software that is installed on hosts to perform host-based intrusion prevention (HIPS).

7. A. CSM is an integrated solution for configuration management of firewall, VPN, router, switch module, and IPS devices.
8. A, B, C. Cisco IOS, PIX, and ASA can all be used to integrate security into the network.
9. B. Netflow provides information for detecting and mitigating threats.
10. C. Cisco ACS is a security management platform for controlling administrative access for Cisco devices and security applications.

Q&A

1. B. Integrated Services Router (ISR) combines IOS firewall, VPN, and IPS services.
2. C. The 802.1X protocol is a standards-based protocol for authenticating network clients by permitting or denying access to the network.
3. D. The NAC Framework is an integrated solution led by Cisco that incorporates the network infrastructure and third-party software to impose security policies on the attached endpoints.
4. A. Cisco Security MARS (CS-MARS) is an appliance-based solution for network security administrators to monitor, identify, isolate, and respond to security threats.
5. A, B, C. Cisco IOS Trust and Identity is a set of services that include AAA, SSH, SSL, 802.1x, and PKI.
6. False. SSH provides encrypted router access.
7. B. Cisco IOS IPsec offers data encryption at the IP packet level using a set of standards-based protocols.
8. True. PKI provides strong authentication services for e-commerce applications.
9. D. High-Performance advanced integration module (AIM) is a hardware module for terminating large numbers of VPN tunnels.
10. False. Integrated Content Modules for 2800/3800 series routers are used for content networking.
11. False. Cisco VPN 3000 concentrators provide businesses with IPsec and SSL VPN connectivity.
12. A, B. Cisco Catalyst 6500 switches support FWSM and IDSM2 services modules.
13. B. The Anomaly Guard Module provides attack responses by blocking malicious traffic at Gbps line rates.
14. A, B, C. Some identity and access control protocols include 802.1X, ACLs, and NAC. NetFlow collects stats on packets flowing through the router.
15. True. The Cisco Security Agent protects server and desktop endpoints from the latest threats caused by malicious network attacks.

16. D. CSA MC is an SSL web-based tool for managing Cisco Security Agent configurations.
17. True. IDM is a web-based application that configures and manages IPS sensors.
18. True. NetFlow is used for threat detection and mitigation.
19. C. The three phases of the Cisco Self-Defending Network include Integrating Security, Adaptive Threat Defense, and Collaborative Security.
20. True. Cisco ASAs, PIX security appliances, FWSM, and IOS firewall are part of Infection Containment.
21. D. IOS intrusion prevention system (IPS) offers inline deep-packet inspection to successfully diminish a wide range of network attacks.
22. IPS. The 4200 IPS sensor appliances can identify, analyze, and block unwanted traffic from flowing on the network.
23. B. Cisco Secure Access Control Server (ACS) provides centralized control for administrative access to Cisco devices and security applications.
24. True. ASDM provides management of Cisco ASAs, PIX, and FWSMs.
25. False. IPS 4255 delivers 1000 Mbps of performance and can be used to protect partially utilized Gigabit connected subnets.
26. True. FWSM is a high-speed firewall module for use in the Cisco Catalyst 6500 and 7600 series routers.
27. i = D, ii = C, iii = B, iv = A

Chapter 15

"Do I Know This Already?"

1. C. H.323 is the ITU standard that provides a framework for the transport of voice, video, and data over packet-switched networks.
2. D. The default codec in Cisco VoIP dial peers is G.729, which has an 8-kbps bit rate.
3. C. RTP operates at the transport layer of the OSI model.
4. C. The H.225 standard defines the procedures for call setup and signaling.
5. B. An Erlang is a unit that describes the number of calls in an hour.
6. B. VAD reduces traffic by not transmitting packets when there is silence in voice conversations.
7. C. CRTP compresses the RTP, UDP, and IP headers.

8. B. LLQ is recommended for VoIP networks.
9. A. The local loop is located between the traditional phone and the CO switch.
10. C. Jitter is the variable delay of packets at the receiving end of a connection, including an IP telephony voice call.

Q&A

1. True. Cisco recommends Low-Latency Queuing for VoIP networks.
2. False. H.323 is an ITU standard, and SIP is an IETF standard for multimedia.
3. True. An Erlang is a telecommunications traffic unit of measurement representing the continuous use of one voice path for one hour.
4. VAD. Voice Activity Detection suppresses packets when there is silence.
5. Dejitter buffers are used at the receiving end to smooth out the variable delay of received packets.
6. True. With CCS, a separate channel (from the bearer channels) is used for signaling.
7. False. You use FXS ports to connect to phones and FXO ports to connect to the PSTN.
8. True. SS7 implements call setup, routing, and control, ensuring that intermediate and far-end switches are available when a call is placed.
9. Interactive Voice Response (IVR) System. IVR systems connect incoming calls to an audio playback system that queues the calls, provides prerecorded announcements, prompts the caller for key options, provides the caller with information, and transfers the call to another switch extension or agent.
10. Automatic Call Distribution (ACD) system. ACD is used by airline reservation systems, customer service departments, and other call centers.
11. CRTP and VAD. Both CRTP and VAD reduce the amount of bandwidth used by VoIP calls. G.729 calls can be reduced from 26.4 kbps to 11.2 with CRTP and to 7.3 with CRTP and VAD.
12. A, B, C, and E are fixed; D is variable. Fixed-delay components include processing, serialization, dejitter, and propagation delays. Variable-delay components include only queuing delays.
13. You reduce the frame size with fragmentation or increase the link bandwidth. The formula is serialization delay = frame size/link bandwidth.
14. PQ-WFQ and LLQ. Both of these queuing techniques use a strict priority queue. LLQ also provides class-based differentiated services.
15. False. The G.114 recommendation specifies 150-ms one-way maximum delay.

16. True. FRF.12 specifies LFI for Frame Relay networks.

17. Yes. An RTT of 250 ms means that the average one-way delay is 125 ms, which is less than the recommended maximum of 150 ms.

18. i = D, ii = C, iii = A, iv = B, v = E

19. i = B, ii = C, iii = A

20. i = B, ii = D, iii = C, iv = A

21. FRF.11

22. C. Q.SIG is the preferred protocol for inter-PBX trunks.

23. A. CRTP compresses the IP/UDP/RTP headers from 40 bytes to 2 or 4 bytes.

24. B. The analog signal is filtered and then sampled, and then samples are digitized.

25. C. The digitizing process is divided into companding, and quantization and coding.

26. D. All answers are correct.

27. B. LFI and cRTP should be implemented to help with the serialization delay on slow-speed WAN circuits. LLQ will not help, because the circuit has no congestion.

28. D. The G.729 codec is recommended on WAN links because of its lower bandwidth requirements and relatively high MOS.

29. C and D. cRTP and VAD reduce the amount of IP bandwidth used in IPT calls.

30. A. CAC prevents new voice calls from affecting existing voice calls.

31. D. The Cisco Unified CallManager performs the call processing functions of the Cisco IPT solution.

32. Multisite centralized WAN call processing with a CM cluster at the main site and SRST routers at the remote sites.

33. SRST enables the remote routers to provide call-handling support for IP phones when they lose connectivity to the CallManagers because of a WAN failure.

34. LLQ provides a strict queue for RTP (VoIP) traffic and differentiated class of service for all other traffic.

35. The minimum bandwidth is approximately 640 kbps. Each call is 30 kbps times four, which equals 120 kbps. The exiting 512 kbps of data traffic equals 640 kbps. The circuit should be provisioned at a higher speed to prevent the sustained peak utilization from being higher than 70 percent.

36. Yes, a CM cluster should be implemented at the main site.

37. CRTP compresses the RTP/UDP/IP headers from 40 bytes to 2 to 4 bytes.
38. FRF.12 is the link and fragmentation technique used in frame relay networks.

Chapter 16

"Do I Know This Already?"

1. C. SNMPv3 introduces authentication and encryption for SNMP.
2. B. SNMP runs over UDP.
3. A. Managed devices contain SNMP agents.
4. D. A MIB is a collection of information that is stored on the local agent of the managed device.
5. D. CDP is Cisco Discovery Protocol.
6. C. The NMS manager uses the GetBulk operation to retrieve large blocks of data, such as multiple rows in a table.
7. A. RMON1 is focused on the data link and physical layers of the OSI model.
8. B. Community is not an SNMP operation.
9. B. NetFlow allows for network planning, traffic engineering, billing, accounting, and application monitoring.
10. B. CDP is a hello-based protocol.

Q&A

1. Fault management, configuration management, accounting management, performance management, and security management.
2. Data link layer.
3. Notice level.
4. False.
5. True.
6. Device ID, IP address, capabilities, OS version, model number, port ID.
7. D. A trap message is sent by the agent when a significant event occurs.
8. A. The NMS manager uses the Get operation to retrieve the value-specific MIB variable from an agent.

9. B. The NMS manager uses the Set operation to set values of the object instance within an agent.
10. C. More than 500 syslog facilities can be configured on Cisco IOS.
11. B. At the authNoPriv level, authentication is provided, but not encryption.
12. B. CBC-DES is the encryption algorithm used by SNMPv3.
13. C and D. Both CDP and NetFlow can be used to discover and document a network.
14. B, C, D.
15. D. RMON2 provides monitoring information from the network to the application layers.
16. D.
17. C.
18. A. The authPriv level provides authentication and encryption.
19. i = C, ii = A, iii = D, iv = B

APPENDIX B

The OSI Reference Model, TCP/IP Architecture, and Numeric Conversion

The Open Systems Interconnection (OSI) model is a mandatory topic in any internetworking book. The CCDA candidate should understand the OSI model and identify which OSI layers host the different networking protocols. The OSI model provides a framework for understanding internetworking. This appendix provides an overview and general understanding of the OSI reference model.

The Transmission Control Protocol/Internet Protocol (TCP/IP) architecture provides the practical implementation of a layered model. This appendix provides an overview of the TCP/IP layers and how they map to the OSI model.

Also covered in this appendix is the numeric conversion of binary, decimal, and hexadecimal numbers. The ability to covert between binary, decimal, and hexadecimal numbers helps you manipulate IP addresses in binary and dotted-decimal format. Quickly converting these numbers will help you answer test questions.

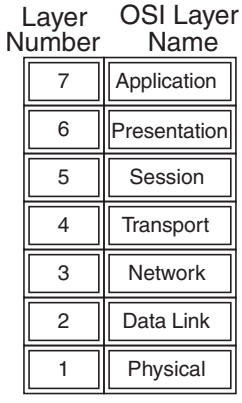
OSI Model Overview

The International Organization for Standardization (ISO) developed the OSI model in 1984, and revisited it in 1994, to coordinate standards development for interconnected information-processing systems. The model describes seven layers that start with the physical connection and end with the application. As shown in Figure B-1, the seven layers are physical, data link, network, transport, session, presentation, and application.

The OSI model divides the tasks involved in moving data into seven smaller, more manageable layers. Each layer provides services to the layer above, performs at least the functions specified by the model, and expects the defined services from the layer below. The model does not define the precise nature of the interface between layers or the protocol used between peers at the same layer in different instantiations of a protocol stack. The model's design encourages each layer to be implemented independently. For example, you can run an application over IP (Layer 3), Fast Ethernet (Layer 2), Frame Relay (Layer 2), or Gigabit Ethernet (Layer 2). As the packets route through the Internet, the Layer 2 media change independently from the upper-layer protocols. The OSI model helps standardize discussion of the design and construction of

networks for developers and hardware manufacturers. It also provides network engineers and analysts with a framework useful in understanding internetworking.

Figure B-1 *Seven-Layer OSI Model*



Layered implementations of internetworking technologies do not necessarily map directly to the OSI model. For example, the TCP/IP architecture model describes only four layers, with the upper layer mapping to the three upper layers of the OSI model (application, presentation, and session). The development of IP predates the OSI model. For a more thorough discussion of the TCP/IP model, see Chapter 7, "Internet Protocol Version 4."

The following sections describe and provide sample protocols for each OSI layer.

Physical Layer (OSI Layer 1)

The physical layer describes the transportation of raw bits over physical media. It defines signaling specifications and media types and interfaces. It also describes voltage levels, physical data rates, and maximum transmission distances. In summary, it deals with the electrical, mechanical, functional, and procedural specifications for links between networked systems.

Examples of physical layer specifications are

- EIA/TIA-232 (Electronic Industries Association/ Telecommunications Industry Association)
- EIA/TIA-449
- V.35
- IEEE 802 LAN and metropolitan-area network (MAN) standards

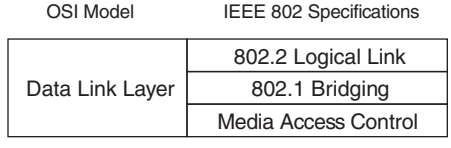
- Physical layer (PHY) groups Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH)
- Maximum cable distances of the Ethernet family, Token Ring, and Fiber Distributed Data Interface (FDDI)

Data Link Layer (OSI Layer 2)

This layer is concerned with the reliable transport of data across a physical link. Data at this layer is formatted into frames. Data link specifications include frame sequencing, flow control, synchronization, error notification, physical network topology, and physical addressing. This layer converts frames into bits when sending information and converts bits into frames when receiving information from the physical media. Bridges and switches operate at the data link layer.

Because of the complexity of this OSI layer, the IEEE subdivides the data link layer into three sublayers for LANs. Figure B-2 shows how Layer 2 is subdivided. The upper layer is the logical link sublayer, which manages communications between devices. The bridging layer, defined by IEEE 802.1, is the middle layer. The lowest layer is the Media Access Control (MAC) sublayer, which manages the protocol access to the physical layer and ultimately the actual media. Systems attached to a common data link layer have a unique address on that data link layer. Be aware that you might find some references describing this layer as having two sublayers: the Logical Link Control (LLC) sublayer and the MAC sublayer.

Figure B-2 *IEEE Data Link Sublayers*



Examples of data link layer technologies are

- Frame Relay
- ATM
- Synchronous Data Link Control (SDLC)
- High-Level Data Link Control (HDLC)
- Point-to-Point Protocol (PPP)
- Ethernet implementations (IEEE 802.3)
- Token Ring (IEEE 802.5)
- Wireless LAN (IEEE 802.11)

Network Layer (OSI Layer 3)

The network layer is concerned with routing information and methods to determine paths to a destination. Information at this layer is called packets. Specifications include routing protocols, logical network addressing, and packet fragmentation. Routers operate at this layer.

Examples of network layer specifications are

- Routed protocols
  - IP
  - Internetwork Packet Exchange (IPX)
  - Connectionless Network Protocol (CLNP)
- Routing protocols
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Intermediate System-to-Intermediate System (IS-IS)

Transport Layer (OSI Layer 4)

The transport layer provides reliable, transparent transport of data segments from upper layers. It provides end-to-end error checking and recovery, multiplexing, virtual circuit management, and flow control. Messages are assigned a sequence number at the transmission end. At the receiving end, the packets are reassembled, checked for errors, and acknowledged. Flow control manages the data transmission to ensure that the transmitting device does not send more data than the receiving device can process.

Examples of transport layer specifications are

- Transmission Control Protocol (TCP)
- Real-Time Transport Protocol (RTP)
- Sequenced Packet Exchange (SPX)
- User Datagram Protocol (UDP)

NOTE Although UDP operates in the transport layer, it does not perform the reliable error-checking functions that other transport layer protocols do.

Session Layer (OSI Layer 5)

The session layer provides a control structure for communication between applications. It establishes, manages, and terminates communication connections called sessions. Communication sessions consist of service requests and responses that occur between applications on different devices.

Examples of specifications that operate at the session layer are

- AppleTalk's Zone Information Protocol (ZIP)
- DECnet's Session Control Protocol (SCP)
- H.245 and H.225

Presentation Layer (OSI Layer 6)

The presentation layer provides application layer entities with services to ensure that information is preserved during transfer. Knowledge of the syntax selected at the application layer allows selection of compatible transfer syntax if a change is required. This layer provides conversion of character-representation formats, as might be required for reliable transfer. Voice coding schemes are specified at this layer. Furthermore, compression and encryption can occur at this layer.

An example of a specification that operates at the presentation layer is Abstract Syntax Notation 1 (ASN.1).

Application Layer (OSI Layer 7)

The application layer gives the user or operating system access to the network services. It interacts with software applications by identifying communication resources, determining network availability, and distributing information services. It also provides synchronization between the peer applications residing on separate systems.

Examples of application layer specifications are

- Telnet
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

- Network File System (NFS)
- Association Control Service Element (ACSE)

TCP/IP Architecture

The suite of TCP/IP protocols was developed for use by the U.S. government and research universities. The suite is identified by its most widely known protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). As mentioned, the ISO published the OSI model in 1984. However, the TCP/IP protocols had been developed by the Department of Defense's Advanced Research Projects Agency (DARPA) since 1969. The TCP/IP uses only four layers (as described in RFC 791) versus the seven layers used by OSI. The TCP/IP layers are

- Application
- Host-to-host transport
- Internet
- Network interface

Figure B-3 shows how the TCP/IP layers map to the OSI model.

Figure B-3 *The TCP/IP Architecture and the OSI Model*

<table>
<tr><th>OSI Model</th><th>TCP/IP Architecture</th><th>TCP/IP Protocols</th></tr>
<tr><td>Application</td><td rowspan="3">Application</td><td rowspan="3">Telnet, SMTP, SNMP, FTP, TFTP, HTTPS, DNS</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Host-to-Host Transport</td><td>TCP, UDP</td></tr>
<tr><td>Network</td><td>Internet</td><td>IP, ARP, OSPF, ICMP</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Interface</td><td rowspan="2">Use of lower layer protocols such as Ethernet and Frame Relay.</td></tr>
<tr><td>Physical</td></tr>
</table>

Network Interface Layer

The TCP/IP network interface (also known as network access) layer maps to the OSI data link and physical layers. TCP/IP uses the lower-layer protocols for transport.

Internet Layer

The Internet layer is where IP resides. IP packets exist at this layer. It directly maps to the network layer of the OSI model. Other TCP/IP protocols at this layer are Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Reverse ARP (RARP). These protocols are covered in Chapter 7.

Host-to-Host Transport Layer

The host-to-host transport layer of TCP/IP provides two connection services: TCP and UDP. TCP provides reliable transport of IP packets, and UDP provides transport of IP packets without verification of delivery. This layer maps to the OSI transport layer, but the OSI model only defines reliable delivery at this layer.

Application Layer

The TCP/IP application layer maps to the top three layers of the OSI model: application, presentation, and session. This layer interfaces with the end user and provides for authentication, compression, and formatting. The application protocol determines the data's format and how the session is controlled. Examples of TCP/IP application protocols are Telnet, FTP, and Hypertext Transfer Protocol Secure (HTTPS).

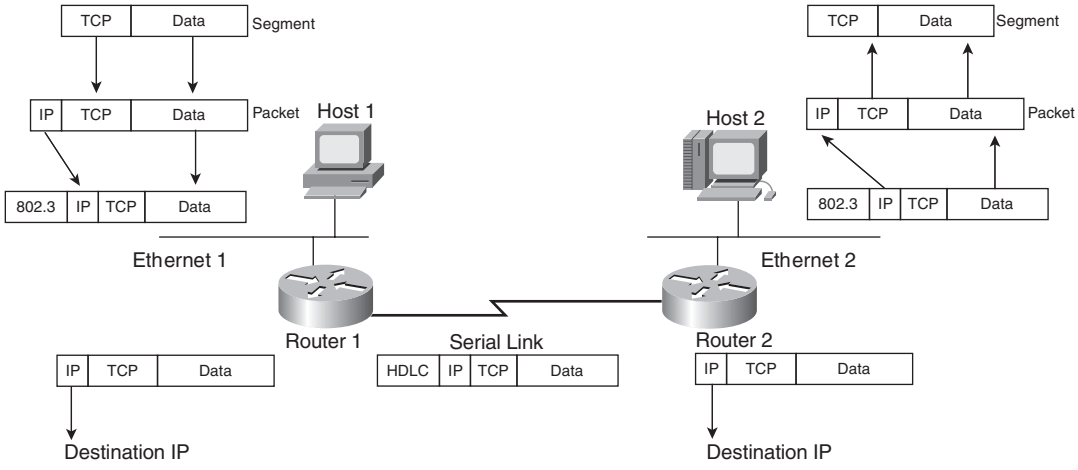
The TCP/IP protocols are covered further in Chapter 7.

Example of Layered Communication

Suppose that you use a Telnet application. Telnet maps to the top three layers of the OSI model. In Figure B-4, a user on Host 1 enables the Telnet application to access a remote host (Host 2). The Telnet application provides a user interface (application layer) to network services. As defined in RFC 854, ASCII is the default code format. No session layer is defined for Telnet (not an OSI protocol). Per the RFC, Telnet uses TCP for connectivity (transport layer). The TCP segment is placed in an IP packet (network layer) with a destination IP address of Host 2. The IP packet is placed in an Ethernet frame (data link layer), which is converted into bits and sent onto the wire (physical layer).

When the frame arrives at Router 1, it converts the bits into a frame; removes the frame headers (data link); checks the destination IP address (network); places a serial link header on the packet, making it a serial frame; and forwards the frame to the serial link (data link), which sends it as bits.

Figure B-4 *Telnet Example*



Router 2 receives the bits and converts them into a frame; removes the serial encapsulation headers; checks the destination IP address (network); adds an Ethernet header to the packet, making it a frame; and places the frame on Ethernet 2 (data link). Host 2 receives bits (physical) from the Ethernet cable and converts the bits into a frame (data link). Then, the IP protocol is examined and the packet data is forwarded to TCP, which checks the segment number for errors and then forwards the segment to TCP port 23 (Telnet), which is the application.

Numeric Conversion

This section focuses on the techniques for converting between decimal, binary, and hexadecimal numbers. Although the exam might not have a specific question about converting a binary number to decimal, you need to know how to convert these numbers to do problems on the test. IPv6 addresses are shown in hexadecimal. An IPv4 address could be shown as binary or in traditional dotted-decimal format. MAC addresses and IPv6 addresses are represented in hexadecimal. Some **show** commands have output information in hexadecimal or binary formats.

Hexadecimal Numbers

The hexadecimal numeric system uses 16 digits instead of the 10 digits used by the decimal system. Table B-1 shows the hexadecimal digits and their decimal equivalent values.

Table B-1 *Hexadecimal Digits*

Hexadecimal Digit	Decimal Value
0	0
1	1

Table B-1 *Hexadecimal Digits (Continued)*

Hexadecimal Digit	Decimal Value
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
A	10
B	11
C	12
D	13
E	14
F	15
10	16
11	17
12	18
13	19
14	20

Hexadecimal Representation

It is common to represent a hexadecimal number with "0x" before the number so that it is not confused with a decimal number. The hexadecimal number of decimal 16 is written as 0x10, not 10. Another method is to put a subscript h to the right of the number, such as 10_h. It is also common to use the term "hex" when speaking of hexadecimal. Much of the following text uses "hex."

Converting Decimal to Hexadecimal

First things first: memorize Table B-1. There are two ways to convert larger numbers. The first method is to convert decimal to binary and then convert binary to hex. The second method is to divide the decimal number by 16—the residual is the rightmost hexadecimal digit—and then keep dividing until the number is not divisible anymore. For the first method, use the schemes described in later sections. For the second method, follow the examples described here.

First, divide the decimal number by 16. The remainder of the division is the least-significant (first) hexadecimal digit. Continue to divide the quotients (answer) of the divisions by 16 until the quotient is 0. The remainder value of each later division is converted to a hexadecimal digit and prepended to the previous value. The final remainder is the most-significant digit of the hexadecimal equivalent. For large numbers, you might have to divide many times. This process will be clearer in the following examples.

Conversion Example B-1 *Convert 26 to Its Hex Equivalent*

Divide by 16:

```
    1
16 | 26
   -16
    10 = Ah
```

Answer: **$1A_h$**

Conversion Example B-2 *Convert 96 to Its Hex Equivalent*

Not divisible by 256; divide by 16:

```
    6
16 | 96
   -96
    0 = 0h
```

Answer: **60_h**

Conversion Example B-3 *Convert 375 to Its Hex Equivalent*

Divide by 16 first:

```
    23
16 | 375
   -32
    55
   -48
     7
```

Now divide 23 by 16:

```
    1
16 | 23
   -16
     7
```

Now take the residual from the first division (7) and concatentate it with the residual from the second division (7), plus the result of the second division (1), and the answer is 177_h.

Conversion Example B-4 *Convert 218 to Its Hex Equivalent*

Divide by 16:

$$\begin{array}{r|l} & \mathbf{13 = D_h} \\ \hline 16 & 218 \\ & -16 \\ & \overline{58} \\ & -48 \\ & \overline{\mathbf{10 = A_h}} \end{array}$$

Answer: $\mathbf{DA_h}$

Converting Hexadecimal to Decimal

To convert a hex number to decimal, take the rightmost digit and convert it to decimal (for example, 0xC = 12). Then add this number to the second rightmost digit times 16 and the third rightmost digit times 256. Don't expect to convert numbers larger than 255 on the CCDA exam, because the upper limit of IP addresses in dotted-decimal format is 255 (although Token Ring numbers reach 4096). Some examples follow.

Conversion Example B-5 *Convert 177_h to Decimal*

$$\begin{array}{r} 1 \times 256 = 256 \\ 7 \times 16 = 112 \\ 7 \times 1 = \underline{7} \\ \mathbf{375_d} \end{array}$$

Conversion Example B-6 *Convert 60_h to Decimal*

$$\begin{array}{r} 6 \times 16 = 96 \\ 0 \times 1 = \underline{0} \\ \mathbf{96_d} \end{array}$$

Conversion Example B-7 *Convert 100_h to Decimal*

$$\begin{array}{r} 1 \times 256 = 256 \\ 0 \times 16 = 0 \\ 0 \times 1 = \underline{0} \\ \mathbf{256_d} \end{array}$$

Conversion Example B-8 *Convert $1DA_h$ to Decimal*

$$\begin{array}{r} 1 \times 256 = 256 \\ 13 \times 16 = 208 \\ 10 \times 1 = \underline{10} \\ \mathbf{474_d} \end{array}$$

Alternative Method for Converting from Hexadecimal to Decimal

Another way is to convert from hex to binary and then from binary to decimal. The following sections discuss converting from binary to decimal.

Binary Numbers

The binary number system uses two digits: 1 and 0. Computer systems use binary numbers. IP addresses and MAC addresses are represented by binary numbers. The number of binary 1s or 0s is the number of *bits*, short for binary digits. For example, 01101010 is a binary number with 8 bits. An IP address has 32 bits, and a MAC address has 48 bits. As shown in Table B-2, IPv4 addresses are usually represented in dotted-decimal format; therefore, it is helpful to know how to convert between binary and decimal numbers. MAC addresses are usually represented in hexadecimal numbers; therefore, it is helpful to know how to convert between binary and hexadecimal.

Table B-2 *Binary Representation of IP and MAC Addresses*

IPv4 Address in Binary	**IPv4 Address in Dotted Decimal**
00101000 10001010 01010101 10101010	= 40.138.85.170
MAC Address in Binary	**MAC Address in Hexadecimal**
00001100 10100001 10010111 01010001 00000001 10010001	= 0C:A1:97:51:01:91

The CCDA candidate should memorize Table B-3, which shows numbers from 0 to 16 in decimal, binary, and hexadecimal formats.

Table B-3 *Decimal, Binary, and Hexadecimal Numbers*

Decimal Value	**Hexadecimal**	**Binary**
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001

Table B-3 *Decimal, Binary, and Hexadecimal Numbers (Continued)*

Decimal Value	Hexadecimal	Binary
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111
16	10	10000

Converting Binary to Hexadecimal

To convert binary numbers to hex, put the bits in groups of 4, starting with the right-justified bits. Groups of 4 bits are often called *nibbles*. Each nibble can be represented by a single hexadecimal digit. A group of two nibbles is an octet, 8 bits. Examples follow.

Conversion Example B-9 *Convert 0010011101 to Hex*

Group the bits:
00 1001 1101
Answer: **$09D_h$**

Conversion Example B-10 *Convert 00101010010110010000010110001 to Hex*

Group the bits:
0010 1010 0101 1001 0000 1011 0001
Answer: **$2A590B1_h$**

Converting Hexadecimal to Binary

This procedure is also easy. Simply change the hex digits into their 4-bit equivalents. Examples follow.

Conversion Example B-11 *Convert 0DEAD0 to Hex*

Hex: 0 D E A D 0
Binary: 0000 1101 1110 1010 1101 0000
Answer: **000011011110101011010000**

Conversion Example B-12 *Convert AA0101 to Hex*

Hex: A A 0 1 0 1
Binary: 1010 1010 0000 0001 0000 0001
Answer: **101010100000000100000001**

Converting Binary to Decimal

To convert a binary number to decimal, multiply each instance of 0 or 1 by the power of 2 associated with the position of the bit in the binary number. The first bit, starting from the right, is associated with $2^0 = 1$. The value of the exponent increases by 1 as each bit is processed, working leftward. As shown in Table B-4, each bit in the binary number 10101010 has a decimal equivalent from 0 to 128 based on the value of the bit multiplied by a power of 2 associated with the bit position. This is similar to decimal numbers, in which the numbers are based on powers of 10: 1s, 10s, 100s, and so on. In decimal, the number 111 is (1*100) + (1*10) + (1*1). In binary, the number 11111111 is the sum of $(1*2^7) + (1*2^6) + (1*2^5) + (1*2^4) + (1*2^3) + (1*2^2) + (1*2^1) + (1*2^0) = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$. For 10101010, the result is 128 + 0 + 32 + 0 + 8 + 0 + 2 + 0 = 170. Examples follow.

Table B-4 *Decimal Values of Bits in a Binary Number*

Power of 2	$2^7 = 128$	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
Binary	1	1	1	1	1	1	1	1

NOTE Just memorize 1, 2, 4, 8, 16, 32, 64, and 128. Use it as you read a binary number from right to left. This technique should be helpful in fast conversions.

Conversion Example B-13 *Convert 10110111 to Decimal*

Sum: 128 + 0 + 32 + 16 + 0 + 4 + 2 + 1
Answer = **183**

Conversion Example B-14 *Convert 00011011 to Decimal*

Sum: 16 + 8 + 0 + 2 + 1
Answer = **27**

Conversion Example B-15 *Convert 11111111 to Decimal*

Sum: 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1
Answer = **255**

Converting Decimal to Binary Numbers

This procedure is similar to converting from hex to decimal (by dividing), but now you divide the decimal number by 2. You use each residual to build the binary number by prepending each residual bit to the previous bit, starting on the right. Repeat the procedure until you cannot divide anymore. The only problem is that for large numbers, you might have to divide many times. You can reduce the number of divisions by first converting the decimal value to a hexadecimal value and then converting the intermediate result to the binary representation. After the following example, you will read about an alternate method suitable for use with decimal values between 0 and 255 that can be represented in a single octet.

Conversion Example B-16 *Convert 26 to Binary*

```
   13
2 | 26
  -26
    0
```

The first bit is 0; now divide 13 by 2. [0]

```
    6
2 | 13
  -12
    1
```

The second bit is 1; now divide 6 by 2. [10]

```
    3
2 | 6
  -6
   0
```

The third bit is 0; now divide 3 by 2. [010]

```
    1
2 | 3
  -2
   1
```

The fourth bit is 1; the leftmost bit is the division result at the top, which is one. [11010]

Answer: **11010**

Alternative Method for Converting from Decimal to Binary

The dividing procedure just described works; it just takes a lot of time. Another way is to remember the bit position values within a byte—128, 64, 32, 16, 8, 4, 2, 1—and play with the bits until the sum adds up to the desired number. This method works when you convert integer values between 0 and 255, inclusive. Table B-5 shows these binary numbers and their decimal values.

Table B-5 *Bit Values*

Binary Number	Decimal Value
10000000	128
01000000	64
00100000	32
00010000	16
00001000	8

Table B-5 *Bit Values (Continued)*

Binary Number	Decimal Value
00000100	4
00000010	2
00000001	1

For example, to convert 26, you know that it is a number smaller than 128, 64, and 32, so those 3 bits are 0 (000?????). Now you need to find a combination of 16, 8, 4, 2, and 1 that adds up to 26. This method involves using subtraction to compute the remaining number. Start with the largest number, and make the bit at 16 a 1 (0001????). The difference between 26 and 16 is 10. What combination of 8, 4, 2, and 1 gives 10? 1010. Therefore, the answer is 00011010. You might think this method involves too much guesswork, but it becomes second nature after some practice.

Conversion Example B-17 *Convert 137 to Binary*

The number is larger than 128; enable that bit. [1???????]

How far is 137 from 128: 9; enable the remaining bits for a value of 9 [1???1001].

The answer is 10001001.

Conversion Example B-18 *Convert 211 to Binary*

The number is larger than 128; enable that bit. [1???????]

Because 211–128 is greater than 64, enable that bit. [11??????] (Remember that 11000000 = 192.)

Because 211–192=19, enable bits 16, 2, and 1. [11?1??11]

The answer is 11010011.

In addition to remembering the bit-position values (128, 64, 32, 16, 8, 4, 2, 1), it helps to remember network subnet mask values. Remembering them makes it easier to figure out whether you need to enable a bit. Table B-6 summarizes the binary subnet mask numbers and their decimal values.

Table B-6 *Binary Masks and Their Decimal Values*

Binary Mask	Decimal
10000000	128
11000000	192
11100000	224
11110000	240

Table B-6 *Binary Masks and Their Decimal Values (Continued)*

Binary Mask	Decimal
11111000	248
11111100	252
11111110	254

References and Recommended Readings

ISO/IEC 7498-1: 1994, "Information Processing Systems - OSI Reference Model - The Basic Model."

Postel, J. RFC 791, *Internet Protocol*. Available from http://www.ietf.org/rfc.

Postel, J. RFC 793, *Transmission Control Protocol*. Available from http://www.ietf.org/rfc.

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K

L

M

N

Q

R

S

T

U

V

W

X-Y-Z