Todd Lammle

CCNA®

Routing and Switching

COMPLETE STUDY GUIDE

Second Edition

EXAM 100-105
EXAM 200-105
EXAM 200-125

Covers 100% of exam objectives, including internetworking, ethernet networking and data encapsulation, IP routing, security, NAT, enhanced switched technologies, wide area networks, and much more...

Includes online interactive learning environment with:

- **3 custom practice exams**
- **200 electronic flashcards**
- **Searchable key term glossary**
- **20% off ITProTV annual membership, includes FREE Premium Switching lab**

SYBEX
A Wiley Brand

CCNA®
Routing and Switching Complete
Study Guide
Second Edition

Todd Lammle

SYBEX
A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: Kim Wimpsett
Technical Editor: Todd Montgomery
Production Editor: Christine O'Connor
Copy Editor: Judy Flynn
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Executive Publisher: Jim Minatel
Book Designers: Judy Fung and Bill Gibson
Proofreader: Josh Chase, Word One New York
Indexer: Johnna vanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-119-28828-2
ISBN: 978-1-119-28830-5 (ebk.)
ISBN: 978-1-119-28829-9 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2016950861

Acknowledgments

There are many people who work to put a book together, and as an author, I dedicated an enormous amount of time to write this book, but it would have never been published without the dedicated, hard work of many other people.

Kenyon Brown, my acquisitions editor, is instrumental to my success in the world of Cisco certification. Ken, I look forward to our continued progress together in both the print and video markets! My technical editor, Todd Montgomery, was absolutely amazing to work with and he was always there to check my work and make suggestions. Thank you! Also, I've worked with Kim Wimpsett, the development editor, for years now and she coordinated all the pages you hold in your hands as they flew from thoughts in my head to the production process.

Christine O'Connor, my production editor, and Judy Flynn, my copyeditor, were my rock and foundation for formatting and intense editing of every page in this book. This amazing team gives me the confidence to help keep me moving during the difficult and very long days, week after week. How Christine stays so organized with all my changes as well as making sure every figure is in the right place in the book is still a mystery to me! You're amazing, Christine! Thank you! Judy understands my writing style so well now, after doing at least a dozen books with me, that she even sometimes finds a technical error that may have slipped through as I was going through the material. Thank you, Judy, for doing such a great job! I truly thank you both.

About the Author

Todd Lammle is the authority on Cisco certification and internetworking and is Cisco certified in most Cisco certification categories. He is a world-renowned author, speaker, trainer, and consultant. Todd has three decades of experience working with LANs, WANs, and large enterprise licensed and unlicensed wireless networks, and lately he's been implementing large Cisco Firepower networks. His years of real-world experience are evident in his writing; he is not just an author but an experienced networking engineer with very practical experience working on the largest networks in the world, at such companies as Xerox, Hughes Aircraft, Texaco, AAA, Cisco, and Toshiba, among many others. Todd has published over 60 books, including the very popular *CCNA: Cisco Certified Network Associate Study Guide, CCNA Wireless Study Guide, CCNA Data Center Study Guide, and SSFIPS (Firepower)*, all from Sybex. He runs an international consulting and training company based in Colorado, Texas, and San Francisco.

You can reach Todd through his forum and blog at www.lammle.com/ccna.

CONTENTS

List of Tables

List of Illustrations

Introduction

Welcome to the exciting world of Cisco certification! If you've picked up this book because you want to improve yourself and your life with a better, more satisfying, and secure job, you've done the right thing. Whether you're striving to enter the thriving, dynamic IT sector or seeking to enhance your skill set and advance your position within it, being Cisco certified can seriously stack the odds in your favor to help you attain your goals!

Cisco certifications are powerful instruments of success that also markedly improve your grasp of all things internetworking. As you progress through this book, you'll gain a complete understanding of networking that reaches far beyond Cisco devices. By the end of this book, you'll comprehensively know how disparate network topologies and technologies work together to form the fully operational networks that are vital to today's very way of life in the developed world. The knowledge and expertise you'll gain here is essential for and relevant to every networking job and is why Cisco certifications are in such high demand—even at companies with few Cisco devices!

Although it's now common knowledge that Cisco rules routing and switching, the fact that it also rocks the security, collaboration, data center, wireless and service provider worlds is also well recognized. And Cisco certifications reach way beyond the popular but less extensive certifications like those offered by CompTIA and Microsoft to equip you with indispensable insight into today's vastly complex networking realm. Essentially, by deciding to become Cisco certified, you're proudly announcing that you want to become an unrivaled networking expert—a goal that this book will get you well on your way to achieving. Congratulations in advance on the beginning of your brilliant future!

For up-to-the-minute updates covering additions or modifications to the Cisco certification exams, as well as additional study tools, review questions, videos, and bonus materials, be sure to visit the Todd Lammle websites and forum at www.lammle.com/ccna.

Cisco's Network Certifications

It used to be that to secure the holy grail of Cisco certifications—the CCIE—you passed only one written test before being faced with a grueling, formidable hands-on lab. This intensely daunting, all-or-nothing approach made it nearly impossible to succeed and predictably didn't work out too well for most people. Cisco responded to this issue by creating a series of new certifications, which not only made it easier to eventually win the highly coveted CCIE prize, it gave employers a way to accurately rate and measure the skill levels of prospective and current employees. This exciting paradigm shift in Cisco's certification path truly opened doors that few were allowed through before!

Beginning in 1998, obtaining the Cisco Certified Network Associate (CCNA) certification was the first milestone in the Cisco certification climb, as well as the official prerequisite to each of the more advanced levels. But that changed in 2007, when Cisco announced the Cisco Certified Entry Network Technician (CCENT) certification. And then in May 2016, Cisco once again proclaimed updates to the CCENT and CCNA Routing and Switching (R/S) tests. Now the Cisco certification process looks like Figure I.1.

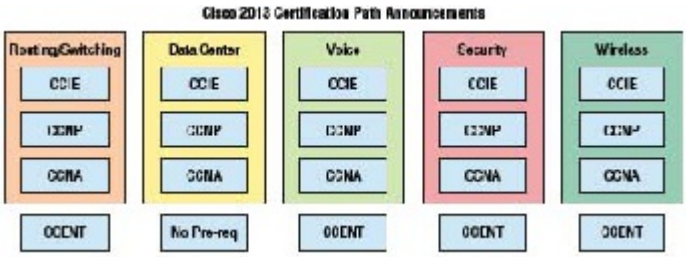


Figure I.1 The Cisco certification path.

I have included only the most popular tracks in Figure I.1. In addition to the ones in this image, there are also tracks for Design, Service Provider, Service Provider Operations, and Video.

The Cisco R/S path is by far the most popular and could very well remain so, but soon you'll see the Data Center path become more and more of a focus as companies migrate to data center technologies. The Security and

Collaboration tracks also actually does provide a good job opportunity, and an even newer one that is becoming more popular is the Industrial CCNA. Still, understanding the foundation of R/S before attempting any other certification track is something I highly recommend.

Even so, and as the figure shows, you only need your CCENT certification to get underway for most of the tracks. Also, note that there are a few other certification tracks you can go down that are not shown in the figure, although they're not as popular as the ones shown.

Cisco Certified Entry Network Technician (CCENT)

Don't be fooled by the oh-so-misleading name of this first certification because it absolutely isn't entry level! Okay—maybe entry level for Cisco's certification path, but definitely not for someone without experience trying to break into the highly lucrative yet challenging IT job market! For the uninitiated, the CompTIA A+ and Network+ certifications aren't official prerequisites, but know that Cisco does expect you to have that type and level of experience before embarking on your Cisco certification journey.

All of this gets us to 2016, when the climb to Cisco supremacy just got much harder again. The innocuous-sounding siren's call of the CCENT can lure you to some serious trouble if you're not prepared, because it's actually much harder than the old CCNA ever was. This will rapidly become apparent once you start studying, but be encouraged! The fact that the certification process is getting harder really works better for you in the long run, because that which is harder to obtain only becomes that much more valuable when you finally do, right? Yes, indeed!

Another important factor to keep in mind is that the Interconnection Cisco Network Devices Part 1 (ICND1) exam, which is the required exam for the CCENT certification, costs $150 per attempt and it's anything but easy to pass! The good news is that Part 1 of this book (Chapters 1-14) will guide you step-by-step in building a strong foundation in routing and switching technologies. You really need to build on a strong technical foundation and stay away from exam cram type books, suspicious online material, and the like. They can help somewhat, but understand that you'll pass the Cisco certification exams only if you have a strong foundation and that you'll get that solid foundation only by reading as much as you can, performing the written labs and review questions in this book, and practicing lots and lots of hands-on labs. Additional practice exam questions, videos, and labs are offered on my website, and what seems like a million other sites offer additional material that can help you study.

However, there is one way to skip the CCENT exam and still meet the prerequisite before moving on to any other certification track, and that path is through the CCNA R/S Composite exam. First, I'll discuss the Interconnecting Cisco Network Devices Part 2 (ICND2) exam, and then I'll tell you about the CCNA Composite exam, which will provide you, when successful, with both the CCENT and the CCNA R/S certification.

Cisco Certified Network Associate Routing and Switching (CCNA R/S)

Once you have achieved your CCENT certification, you can take the ICND2 (200-105) exam in order to achieve your CCNA R/S certification, which is the most popular certification Cisco has by far because it's the most sought-after certification of all employers.

As with the CCENT, the ICND2 exam is also $150 per attempt—although thinking you can just skim a book and pass any of these exams would probably be a really expensive mistake! The CCENT/CCNA exams are extremely hard and cover a lot of material, so you have to really know your stuff. Taking a Cisco class or spending months with hands-on experience is definitely a requirement to succeed when faced with this monster!

And once you have your CCNA, you don't have to stop there—you can choose to continue and achieve an even higher certification, called the Cisco Certified Network Professional (CCNP). There are various ones, as shown in Figure NaN.1. The CCNP R/S is still the most popular, with Voice certifications coming in at a close second. And I've got to tell you that the Data Center certification will be catching up fast. Also good to know is that anyone with a CCNP R/S has all the skills and knowledge needed to attempt the notoriously dreaded but coveted CCIE R/S lab. But just becoming a CCNA R/S can land you that job you've dreamed about and that's what this book is all about: helping you to get and keep a great job!

Still, why take two exams to get your CCNA if you don't have to? Cisco still has the CCNA Composite (200-125) exam that, if passed, will land you with your CCENT and your CCNA R/S via only one test priced at only $250. Some people like the one-test approach, and some people like the two-test approach. Part 2 of this book (Chapters 15-22) covers the ICND2 exam topics.

Why Become a CCENT and CCNA R/S?

Cisco, like Microsoft and other vendors that provide certification, has created the certification process to give administrators a set of skills and to equip prospective employers with a way to measure those skills or match

certain criteria. And as you probably know, becoming a CCNA R/S is certainly the initial, key step on a successful journey toward a new, highly rewarding, and sustainable networking career.

The CCNA program was created to provide a solid introduction not only to the Cisco Internetwork Operating System (IOS) and Cisco hardware but also to internetworking in general, making it helpful to you in areas that are not exclusively Cisco's. And regarding today's certification process, it's not unrealistic that network managers—even those without Cisco equipment—require Cisco certifications for their job applicants.

Rest assured that if you make it through the CCNA and are still interested in Cisco and internetworking, you're headed down a path to certain success!

What Skills Do You Need to Become a CCNA R/S?

This ICND1 exam (100-105) tests a candidate for the knowledge and skills required to successfully install, operate, and troubleshoot a small branch office network. The exam includes questions on the operation of IP data networks, LAN switching technologies, IPv6, IP routing technologies, IP services, network device security, and basic troubleshooting. The ICND2 exam (exam 200-105) tests a candidate for the knowledge and skills required to successfully install, operate, and troubleshoot a small- to medium-size enterprise branch network. The exam includes questions on LAN switching technologies, IP routing technologies, security, troubleshooting, and WAN technologies.

How Do You Become a CCNA R/S

If you want to go straight for our CCNA R/S and take only one exam, all you have to do is pass the CCNA Composite exam (200-125). Oh, but don't you wish it were that easy? True, it's just one test, but it's a whopper, and to pass it you must possess enough knowledge to understand what the test writers are saying, and you need to know everything I mentioned previously, in the sections on the ICND1 and ICND2 exams! Hey, it's hard, but it can be done!

What does the CCNA Composite exam (200-125) cover? Pretty much the same topics covered in the ICND1 and ICND2 exams. Candidates can prepare for this exam by taking the Todd Lammle authorized Cisco boot camps. 200-125 tests a candidate's knowledge and skills required to install, operate, and troubleshoot a small- to medium-size enterprise branch network.

While you can take the Composite exam to get your CCNA, it's good to know that Cisco offers the two-step process I discussed earlier in this Introduction. And this book covers both those exams too! It may be easier than taking that one ginormous exam for you, but don't think the two-test method is easy. It takes work! However, it can be done; you just need to stick with your studies.

The two-test method involves passing the following:

- Exam 100-105: Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Exam 200-105: Interconnecting Cisco Networking Devices Part 2 (ICND2)

I can't stress this point enough: It's critical that you have some hands-on experience with Cisco routers. If you can get a hold of some basic routers and switches, you're set, but if you can't, I've worked hard to provide hundreds of configuration examples throughout this book to help network administrators, or people who want to become network administrators, learn the skills they need to pass the CCENT and CCNA R/S exams.

For Cisco certification hands-on training with CCSI Todd Lammle, please see: www.lammle.com/ccna. Each student will get hands-on experience by configuring at least three routers and two switches.no sharing of equipment!

What Does This Book Cover?

This book covers everything you need to know to pass the ICND1 (100-105) and ICND2 (200-105) exams, as well as the CCNA Composite (200-125) exam. But regardless of which path you choose, as I've said, taking plenty of time to study and practice with routers or a router simulator is the real key to success.

You will learn the following information in this book:

Chapter 1: Internetworking Chapters 1.14 map to the ICND1 exam. In Chapter 1, you will learn the basics of the Open Systems Interconnection (OSI) model the way Cisco wants you to learn it. There are written labs and plenty of review questions to help you. Do not even think of skipping the fundamental written labs in this chapter!

Chapter 2: Ethernet Networking and Data Encapsulation This chapter will provide you with the Ethernet foundation you need in order to pass both the CCENT and CCNA exams. Data encapsulation is discussed in detail in this chapter as well. And as with the other chapters, this chapter includes written labs and review questions to help you.

Chapter 3: Introduction to TCP/IP This chapter provides you with the background necessary for success on the exam, as well as in the real world with a thorough presentation of TCP/IP. This in-depth chapter covers the very beginnings of the Internet Protocol stack and goes all the way to IP addressing and understanding the difference between a network address and a broadcast address before finally ending with network troubleshooting.

Chapter 4: Easy Subnetting You'll actually be able to subnet a network in your head after reading this chapter if you really want to! And you'll find plenty of help in this chapter as long as you don't skip the written labs and review questions at the end.

Chapter 5: VLSMs, Summarization, and Troubleshooting TCP/IP Here, you'll find out all about variable length subnet masks (VLSMs) and how to design a network using VLSMs. This chapter will finish with summarization techniques and configurations. As with Chapter 4, plenty of help is there for you if you don't skip the written lab and review questions.

Chapter 6: Cisco's Internetworking Operating System (IOS) This chapter introduces you to the Cisco Internetworking Operating System (IOS) and command-line interface (CLI). In this chapter you'll learn how to turn on a router and configure the basics of the IOS, including setting passwords, banners, and more. Hands-on labs will help you gain a firm grasp of the concepts taught in the chapter. Before you go through the hands-on labs, be sure to complete the written lab and review questions.

Chapter 7: Managing a Cisco Internetwork This chapter provides you with the management skills needed to run a Cisco IOS network. Backing up and restoring the IOS, as well as router configuration, are covered, as are the troubleshooting tools necessary to keep a network up and running. As always, before tackling the hands-on labs in this chapter, complete the written labs and review questions.

Chapter 8: Managing Cisco Devices This chapter describes the boot process of Cisco routers, the configuration register, and how to manage Cisco IOS files. The chapter finishes with a section on Cisco's new licensing strategy for IOS. Hands-on and written labs, along with review questions, will help you build a strong foundation for the objectives covered in this chapter.

Chapter 9: IP Routing This is a fun chapter because we will begin to build our network, add IP addresses, and route data between routers. You will also learn about static, default, and dynamic routing using RIP and RIPv2. Hands-on labs, a written lab, and the review questions will help you fully nail down IP routing.

Chapter 10: Layer 2 Switching This chapter sets you up with the solid background you need on layer 2 switching, how switches perform address learning and make forwarding and filtering decisions. In addition, switch port security with MAC addresses is covered in detail. As always, go through the hands-on labs, written lab, and review questions to make sure you've really got layer 2 switching down!

Chapter 11: VLANs and Inter-VLAN Routing Here I cover virtual VLANs and how to use them in your internetwork. This chapter covers the nitty-gritty of VLANs and the different concepts and protocols used with VLANs. I'll also guide you through troubleshooting techniques in this all-important chapter. The hands-on labs, written lab, and review questions are there to reinforce the VLAN material.

Chapter 12: Security This chapter covers security and access lists, which are created on routers to filter the network. IP standard, extended, and named access lists are covered in detail. Written and hands-on labs, along with review questions, will help you study for the security and access-list portion of the Cisco exams.

Chapter 13: Network Address Translation (NAT) New information, commands, troubleshooting, and detailed hands-on labs will help you nail the NAT CCENT objectives.

Chapter 14: Internet Protocol Version 6 (IPv6) This is a fun chapter chock-full of some great information. IPv6 is not the big, bad scary creature that most people think it is, and it's a really important objective on the latest exam, so study this chapter carefully—don't just skim it. And make sure you hit those hands-on labs hard!

Chapter 15: Enhanced Switched Technologies Chapter 15 is the first chapter of Part 2 of this book, which maps to the ICND2 exam. This chapter will start off with STP protocols and dive into the fundamentals, covering the modes, as well as the various flavors of STP. VLANs, trunks, and troubleshooting are covered as well. EtherChannel technologies, configuration, and verification are also covered. There are hands-on labs, a written lab, and plenty of review questions to help you. Do not even think of skipping the fundamental written and hands-on labs in this chapter!

Chapter 16: Network Device Management and Security Managing Cisco Devices This chapter describes

the boot process of Cisco routers, the configuration register, and how to manage Cisco IOS files. The chapter finishes with a section on Cisco's new licensing strategy for its IOS. Hands-on and written labs, along with review questions, will help you build a strong foundation for the objectives covered in this chapterhow to mitigate threats at the access layer using various security techniques. AAA with RADIUIS and TACACS+, SNMP and HSRP are also covered in this chapter. Don't skip the hands-on labs that are included, as well as a written lab and review questions at the end of the chapter.

Chapter 17: Enhanced IGRP EIGRP was not covered in the ICND1 (CCENT) chapters, so this is a full chapter on nothing but EIGRP and EIGRPv6. There are lots of examples, including configuration, verification, and troubleshooting labs, with both IP and with IPv6. Great hands-on labs are included, as well as a written lab and review questions.

Chapter 18: Open Shortest Path First (OSPF) Chapter 9 dives into more complex dynamic routing by covering OSPF routing. The written lab, hands-on labs, and review questions will help you master this vital routing protocol.

Chapter 19: Multi-Area OSPF The ICND1 (CCENT) portion of this book had a large chapter on OSPF, so before reading this chapter, be sure you have the CCENT objectives down pat with a strong OSPF foundation. This chapter will take off where that ICND1 chapter left off and add multi-area networks along with advanced configurations and then finish with OSPv3. Hands-on labs, a written lab, and challenging review questions await you at the end of the chapter.

Chapter 20: Troubleshooting IP, IPv6, and VLANs I want to say this is the most important chapter in the book, but that's hard to say. You can decide that yourself when you take the exam! Be sure to go through all the troubleshooting steps for IP, IPv6, and VLANs. The hands-on labs for this chapter will be included in the free bonus material and dynamic labs that I'll write and change as needed. Don't skip the written lab and review questions.

Chapter 21: Wide Area Networks This is the longest, and last, chapter in the book. It covers multiple protocols in depth, especially HDLC, PPP, and Frame Relay, along with a discussion on many other technologies. Good troubleshooting examples are provided in the PPP and Frame Relay configuration sections, and these cannot be skipped! Hands-on labs meant to focus squarely on the objectives are included at the end of the chapter, as well as a written lab and challenging review questions.

Chapter 22: Evolution of Intelligent Networks I saved the hardest chapter for last. What makes this chapter challenging is that there is no configuration section to you really need to dive deep into the cloud, APIC-EM and QoS sections with an open and ready mind. I stuck as close to the objectives as possible in order to help you ace the exam. The written lab and review questions are spot on for the objectives.

Appendix A: Answers to Written Labs This appendix contains the answers to the book's written labs.

Appendix B: Answers to Chapter Review Questions This appendix provides the answers to the end-of-chapter review questions.

Appendix C: Disabling and Configuring Network Services Appendix C takes a look at the basic services you should disable on your routers to make your network less of a target for denial of service (DoS) attacks and break-in attempts.

Be sure to check the announcements section of my forum to find out how to download bonus material I created specifically for this book.

What's Available Online?

I have worked hard to provide some really great tools to help you with your certification process. All of the following tools, most of them available at www.wiley.com/go/sybextestprep, should be loaded on your workstation when you're studying for the test. As a fantastic bonus, I was able to add to the download link a preview section from my CCNA video series! Please understand that these are not the full versions, but they're still a great value for you included free with this book.

Test Preparation Software The test preparation software prepares you to pass the ICND1 and ICND2 exams and the CCNA R/S Composite exam. You'll find all the review and assessment questions from the book plus additional practice exam questions that appear exclusively from the downloadable study tools.

Electronic Flashcards The companion study tools include over 200 flashcards specifically written to hit you hard, so don't get discouraged if you don't ace your way through them at first! They're there to ensure that you're really ready for the exam. And no worries—armed with the review questions, practice exams, and flashcards, you'll be

more than prepared when exam day comes!

Glossary A complete glossary of CCENT, ICND2, CCNA R/S and Cisco routing terms is available at www.wiley.com/go/sybextestprep.

Todd Lammle Bonus Material and Labs Be sure to check the announcement section of my forum at www.lammle.com/ccna for directions on how to download all the latest bonus material created specifically to help you study for your ICND1, ICND2, and CCNA R/S exams.

Todd Lammle Videos I have created a full CCNA series of videos that can be purchased at www.lammle.com/ccna

How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Interconnecting Cisco Network Devices Part 1 and 2 exams, or the CCNA R/S Composite exam, then look no further. I've spent hundreds of hours putting together this book with the sole intention of helping you to pass the Cisco exams, as well as really learn how to correctly configure Cisco routers and switches!

This book is loaded with valuable information, and you will get the most out of your study time if you understand why the book is organized the way it is.

So to maximize your benefit from this book, I recommend the following study method:

1. Take the assessment test that's provided at the end of this introduction. (The answers are at the end of the test.) It's okay if you don't know any of the answers; that's why you bought this book! Carefully read over the explanations for any questions you get wrong and note the chapters in which the material relevant to them is covered. This information should help you plan your study strategy.
2. Study each chapter carefully, making sure you fully understand the information and the test objectives listed at the beginning of each one. Pay extra-close attention to any chapter that includes material covered in questions you missed.
3. Complete the written labs at the end of each chapter. (Answers to these appear in Appendix A.) Do not skip these written exercises because they directly relate to the Cisco exams and what you must glean from the chapters in which they appear. Do not just skim these labs! Make sure you completely understand the reason for each correct answer.
4. Complete all hands-on labs in each chapter, referring to the text of the chapter so that you understand the reason for each step you take. Try to get your hands on some real equipment, but if you don't have Cisco equipment available, try the LammleSim IOS version, which you can use for the hands-on labs found only in this book. These labs will equip you with everything you need for all your Cisco certification goals.
5. Answer all of the review questions related to each chapter. (The answers appear in Appendix B.) Note the questions that confuse you, and study the topics they cover again until the concepts are crystal clear. And again—do not just skim these questions! Make sure you fully comprehend the reason for each correct answer. Remember that these will not be the exact questions you will find on the exam, but they're written to help you understand the chapter material and ultimately pass the exam!
6. Try your hand at the practice questions that are exclusive to this book. The questions can be found only at www.wiley.com/go/sybextestprep. And be sure to check out www.lammle.com/ccna for the most up-to-date Cisco exam prep questions, videos, Todd Lammle boot camps, and more.
7. Test yourself using all the flashcards, which are also found on the download link. These are brand-new and updated flashcards to help you prepare for the CCNA R/S exam and a wonderful study tool!

To learn every bit of the material covered in this book, you'll have to apply yourself regularly, and with discipline. Try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. I'm confident that if you work hard, you'll be surprised at how quickly you learn this material!

If you follow these steps and really study—*doing hands-on labs every single day* in addition to using the review questions, the practice exams, the Todd Lammle video sections, and the electronic flashcards, as well as all the written labs—it would actually be hard to fail the Cisco exams. But understand that studying for the Cisco exams is a lot like getting in shape—if you do not go to the gym every day, it's not going to happen!

Where Do You Take the Exams?

You may take the ICND1, ICND2, or CCNA R/S Composite or any Cisco exam at any of the Pearson VUE authorized testing centers. For information, check www.vue.com or call 877-404-EXAM (3926).

To register for a Cisco exam, follow these steps:

1. Determine the number of the exam you want to take. (The ICND1 exam number is 100-105, ICND2 is

100-205, and CCNA R/S Composite is 200-125.)
2. Register with the nearest Pearson VUE testing center. At this point, you will be asked to pay in advance for the exam. At the time of this writing, the ICND1 and ICND2 exams are $150, and the CCNA R/S Composite exam is $250. The exams must be taken within one year of payment. You can schedule exams up to six weeks in advance or as late as the day you want to take it—but if you fail a Cisco exam, you must wait five days before you will be allowed to retake it. If something comes up and you need to cancel or reschedule your exam appointment, contact Pearson VUE at least 24 hours in advance.
3. When you schedule the exam, you'll get instructions regarding all appointment and cancellation procedures, the ID requirements, and information about the testing-center location.

Tips for Taking Your Cisco Exams

The Cisco exams contain about 40-50 questions and must be completed in about 90 minutes or less. This information can change per exam. You must get a score of about 85 percent to pass this exam, but again, each exam can be different.

Many questions on the exam have answer choices that at first glance look identical—especially the syntax questions! So remember to read through the choices carefully because close just doesn't cut it. If you get commands in the wrong order or forget one measly character, you'll get the question wrong. So, to practice, do the hands-on exercises at the end of this book's chapters over and over again until they feel natural to you.

Also, never forget that the right answer is the Cisco answer. In many cases, more than one appropriate answer is presented, but the *correct* answer is the one that Cisco recommends. On the exam, you will always be told to pick one, two, or three options, never "choose all that apply." The Cisco exam may include the following test formats:

- Multiple-choice single answer
- Multiple-choice multiple answer
- Drag-and-drop
- Router simulations

Cisco proctored exams will not show the steps to follow in completing a router interface configuration, but they do allow partial command responses. For example, `show run`, `sho running`, or `sh running-config` would be acceptable.

Here are some general tips for exam success:

- Arrive early at the exam center so you can relax and review your study materials.
- Read the questions *carefully*. Don't jump to conclusions. Make sure you're clear about exactly what each question asks. "Read twice, answer once," is what I always tell my students.
- When answering multiple-choice questions that you're not sure about, use the process of elimination to get rid of the obviously incorrect answers first. Doing this greatly improves your odds if you need to make an educated guess.
- You can no longer move forward and backward through the Cisco exams, so doublecheck your answer before clicking Next since you can't change your mind.

After you complete an exam, you'll get immediate, online notification of your pass or fail status, a printed examination score report that indicates your pass or fail status, and your exam results by section. (The test administrator will give you the printed score report.) Test scores are automatically forwarded to Cisco within five working days after you take the test, so you don't need to send your score to them. If you pass the exam, you'll receive confirmation from Cisco, typically within two to four weeks, sometimes a bit longer.

Objective Map for CCNA Routing and Switching Certification Exam

We've provided this objective map to help you locate where objectives for the CCNA Routing and Switching certification exams are covered in each chapter. Please refer to it when you want to find an objective quickly.

ICND1 Exam Objectives

Exam objectives are subject to change at any time without prior notice and at Cisco's sole discretion. Please visit Cisco's certification website (www.cisco.com/web/learning) for the latest information on the ICND1 Exam 100-105.

Table I.1 20% 1.0 Network Fundamentals

	3
	3
	1
	1
	1
	1
	2
	1
	1
	1
	1
	2
	3 5
	3 5
	3 5
	3 5
	4 5
	3
	3
	3
	3
	3
	14
	14
	14
	14
	14
	14
	14
	14
	14
	14
	14

Table I.2 26% 2.0 LAN Switching Fundamentals

	10
	10
	10
	10
	10
	2
	6
	11
	11
	11
	11
	11
	11
	11
	7
	7
	7
	10
	10

	10
	10
	10
	10
	10

Table I.3 25% 3.0 Routing Fundamentals

	9
	9
	9
	9
	9
	9
	9
	9
	9
	9
	9
	9
	9
	11
	11
	9
	9
	9 14
	9
	9
	9
	9

Table I.4 15% 4.0 Infrastructure Services

	7
	7
	7
	7
	7
	7
	7
	7
	7
	12
	13
	13
	13
	13

Table I.5 14% 5.0 Infrastructure Maintenance

	7
	7 8
	7
	7
	8
	7
	7
	7
	6
	6
	6
	6
	6
	6
	6
	6
	6 8
	8
	8
	8
	6
	6
	6
	6

ICND2 Exam Objectives

Exam objectives are subject to change at any time without prior notice and at Cisco's sole discretion. Please visit Cisco's certification website (www.cisco.com/web/learning) for the latest information on the ICND2 Exam 200-105.

Table I.6 26% 1.0 LAN Switching Technologies

	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	15
	22
	15 16 20
	16
	16

Table I.7 29% 2.0 Routing Technologies

	15
	15
	15
	17 18 19
	17 18 19
	18 19
	18 19
	17
	17

Table I.8 16% 3.0 WAN Technologies

	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21

Table I.9 14% 4.0 Infrastructure Services

	16
	16
	16
	16
	22
	22
	22
	22
	22
	22
	22
	22
	22
	22

	22
	20
	20
	20
	20
	22

Table I.10 15% 5.0 Infrastructure Maintenance

	16
	16
	16
	20
	20
	16
	22
	22
	22
	22
	22

CCNA Exam Objectives (Composite Exam)

Exam objectives are subject to change at any time without prior notice and at Cisco's sole discretion. Please visit Cisco's certification website (www.cisco.com/web/learning) for the latest information on the CCNA Exam 200-125.

Table I.11 15% 1.0 Network Fundamentals

	3
	3
	1
	1
	1
	1
	22
	22
	22
	22
	2
	1
	1
	1
	1
	2
	3 5
	3 5
	3 5
	3 5
	4 5
	3
	3
	3
	3
	3

	14
	14
	14
	14
	14
	14
	14
	14
	14
	14

Table I.12 21% 2.0 LAN Switching Technologies

	10
	10
	10
	10
	10
	2
	6
	11
	11
	11
	11
	11
	15
	15
	11
	15
	15
	15
	15
	15
	15
	7
	7
	7
	15
	15
	15
	15
	22

Table I.13 23% 3.0 Routing Technologies

	9
	9
	9
	9
	9
	9

	9
	9
	9
	9
	9
	9
	9
	9
	11 15
	11 15
	15
	9
	17 18 19
	18 19
	9
	9 14
	9
	9
	9
	4 5
	4 5
	3
	3
	9
	7

Table I.14 10% 4.0 WAN Technologies

	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	21
	22
	22
	22
	22
	22
	22
	22
	22

	22
	22

Table I.15 10% 5.0 Infrastructure Services

	7
	7
	7
	7
	7
	7
	7
	7
	16
	16
	16
	16
	13
	13
	13
	13
	7

Table I.16 11% 6.0 Infrastructure Security

	10
	10
	10
	10
	10
	10
	10
	15 16 20
	16
	16
	15 20
	20
	20
	20
	20
	22
	6
	6
	6
	6
	6
	6
	6
	16

Table I.17 10% 7.0 Infrastructure Management

****

Assessment Test

1. What is the `sys-id-ext` field in a BPDU used for?
   - It is a 4-bit field inserted into an Ethernet frame to define trunking information between switches.
   - It is a 12-bit field inserted into an Ethernet frame to define VLANs in an STP instance.
   - It is a 4-bit field inserted into an non-Ethernet frame to define EtherChannel options.
   - It is a 12-bit field inserted into an Ethernet frame to define STP root bridges.
2. You have four RSTP PVST+ links between switches and want to aggregate the bandwidth. What solution will you use?
   - EtherChannel
   - PortFast
   - BPDU Channel
   - VLANs
   - EtherBundle
3. What configuration parameters must be configured the same between switches for LACP to form a channel? (Choose three.)
   - Virtual MAC address
   - Port speeds
   - Duplex
   - PortFast enabled
   - Allowed VLAN information
4. You reload a router with a configuration register setting of 0x2101. What will the router do when it reloads?
   - The router enters setup mode.
   - The router enters ROM monitor mode.
   - The router boots the mini-IOS in ROM.
   - The router expands the first IOS in flash memory into RAM.
5. Which of the following commands provides the product ID and serial number of a router?
   - `show license`
   - `show license feature`
   - `show version`
   - `show license udi`
6. Which command allows you to view the technology options and licenses that are supported on your router along with several status variables?

- `show license`
- `show license feature`
- `show license udi`
- `show version`

7. Which of the following services provide the operating system and the network?
   - IaaS
   - PaaS
   - SaaS
   - none of the above
8. You want to send a console message to a syslog server, but you only want to send status messages of 3 and lower. Which of the following commands will you use?
   - `logging trap emergencies`
   - `logging trap errors`
   - `logging trap debugging`
   - `logging trap notifications`
   - `logging trap critical`
   - `logging trap warnings`
   - `logging trap alerts`
9. When stacking switches, which is true? (Choose 2)
   - The stack is managed as multiple objects, and has a single management IP address
   - The stack is managed as a single object, and has a single management IP address
   - The master switch is chosen when you configure the first switches master algorithm to on
   - The master switch is elected form one of the stack member switches
10. You need to connect to a remote IPv6 server in your virtual server farm. You can connect to the IPv4 servers, but not the critical IPv6 server you desperately need. Based on the following output, what could your problem be?

```
C:\>ipconfig
Connection-specific DNS Suffix . : localdomain
IPv6 Address. . . . . . . . . . . : 2001:db8:3c4d:3:ac3b:2ef:1823:8938
Temporary IPv6 Address. . . . . . : 2001:db8:3c4d:3:2f33:44dd:211:1c3d
Link-local IPv6 Address . . . . . : fe80::ac3b:2ef:1823:8938%11
IPv4 Address. . . . . . . . . . . : 10.1.1.10
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.1.1.1
```

   - The global address is in the wrong subnet.
   - The IPv6 default gateway has not been configured or received from the router.
   - The link-local address has not been resolved so the host cannot communicate to the router.
   - There are two IPv6 global addresses configured. One must be removed from the configuration.
11. What command is used to view the IPv6-to-MAC-address resolution table on a Cisco router?
   - `show ip arp`
   - `show ipv6 arp`
   - `show ip neighbors`
   - `show ipv6 neighbors`
   - `show arp`
12. An IPv6 ARP entry is listed as with a status of REACH. What can you conclude about the IPv6-to-MAC-address mapping?
   - The interface has communicated with the neighbor address and the mapping is current.
   - The interface has not communicated within the neighbor reachable time frame.
   - The ARP entry has timed out.
   - IPv6 can reach the neighbor address but the addresses has not yet been resolved.
13. Serial0/1 goes down. How will EIGRP send packets to the 10.1.1.0 network?

```
Corp#show ip eigrp topology
[output cut]
P 10.1.1.0/24, 2 successors, FD is 2681842
via 10.1.2.2 (2681842/2169856), Serial0/0
via 10.1.3.1 (2973467/2579243), Serial0/2
via 10.1.3.3 (2681842/2169856), Serial0/1
```

   - EIGRP will put the 10.1.1.0 network into active mode.
   - EIGRP will drop all packets destined for 10.1.1.0.
   - EIGRP will just keep sending packets out s0/0.
   - EIGRP will use s0/2 as the successor and keep routing to 10.1.1.0.
14. What command produced the following output?

```
via FE80::201:C9FF:FED0:3301 (29110112/33316), Serial0/0/0
via FE80::209:7CFF:FE51:B401 (4470112/42216), Serial0/0/1
via FE80::209:7CFF:FE51:B401 (2170112/2816), Serial0/0/2
```

- show ip protocols
- show ipv6 protocols
- show ip eigrp neighbors
- show ipv6 eigrp neighbors
- show ip eigrp topology
- show ipv6 eigrp topology

15. You need to troubleshoot an adjacency between two EIGRP configured routers? What should you look for? (Choose four.)
    - Verify the AS numbers.
    - Verify that you have the proper interfaces enabled for EIGRP.
    - Make sure there are no mismatched K-values.
    - Check your passive interface settings.
    - Make sure your remote routers are not connected to the Internet.
    - If authentication is configured, make sure all routers use different passwords.
16. You have two OSPF directly configured routers that are not forming an adjacency. What should you check? (Choose three.)
    - Process ID
    - Hello and dead timers
    - Link cost
    - Area
    - IP address/subnet mask
17. When do two adjacent routers-enter the 2WAY state?
    - After both routers have received Hello information
    - After they have exchanged topology databases
    - When they connect only to a DR or BDR
    - When they need to exchange RID information
18. Which type of LSAs are generated by ABRs and referred to summary link advertisements (SLAs)?
    - Type 1
    - Type 2
    - Type 3
    - Type 4
    - Type 5
19. Which of the following is not provided by the AH portion of IPsec?
    - Integrity
    - Confidentiality
    - Authenticity
    - Anti-reply
20. Which statement about GRE is not true?
    - GRE is stateless and has no flow control.
    - GRE has security.
    - GRE has additional overhead for tunneled packets, at least 24 bytes.
    - GRE uses a protocol-type field in the GRE header so any layer 3 protocol can be used through the tunnel.
21. Which QoS mechanism will drop traffic if a session uses more than the allotted bandwidth?
    - Congestion management
    - Shaping
    - Policing
    - Marking
22. IPv6 unicast routing is running on the Corp router. Which of the following addresses would show up with the show ipv6 int brief command?

```
Corp#sh int f0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000d.bd3b.0d80 (bia 000d.bd3b.0d80)
[output cut]
```

- FF02::3c3d:0d:bdff:fe3b:0d80
- FE80::3c3d:2d:bdff:fe3b:0d80
- FE80::3c3d:0d:bdff:fe3b:0d80
- FE80::3c3d:2d:ffbd:3bfe:0d80

23. A host sends a type of NDP message providing the MAC address that was requested. Which type of NDP

was sent?

- NA
- RS
- RA
- NS

24. Each field in an IPv6 address is how many bits long?
    - 4
    - 16
    - 32
    - 128
25. To enable OSPFv3, which of the following would you use?
    - Router(config-if)#**ipv6 ospf 10 area 0.0.0.0**
    - Router(config-if)#**ipv6 router rip 1**
    - Router(config)#**ipv6 router eigrp 10**
    - Router(config-rtr)#**no shutdown**
    - Router(config-if)#**ospf ipv6 10 area 0**
26. What does the command `routerA(config)#line cons 0` allow you to perform next?
    - Set the Telnet password.
    - Shut down the router.
    - Set your console password.
    - Disable console connections.
27. Which two statements describe the IP address 10.16.3.65/23? (Choose two.)
    - The subnet address is 10.16.3.0 255.255.254.0.
    - The lowest host address in the subnet is 10.16.2.1 255.255.254.0.
    - The last valid host address in the subnet is 10.16.2.254 255.255.254.0.
    - The broadcast address of the subnet is 10.16.3.255 255.255.254.0.
    - The network is not subnetted.
28. On which interface do you configure an IP address for a switch?
    - `int fa0/0`
    - `int vty 0 15`
    - `int vlan 1`
    - `int s/0/0`
29. Which of the following is the valid host range for the subnet on which the IP address 192.168.168.188 255.255.255.192 resides?
    - 192.168.168.129–190
    - 192.168.168.129–191
    - 192.168.168.128–190
    - 192.168.168.128–192
30. Which of the following is considered to be the inside host's address after translation?
    - Inside local
    - Outside local
    - Inside global
    - Outside global
31. Your inside locals are not being translated to the inside global addresses. Which of the following commands will show you if your inside globals are allowed to use the NAT pool?

```
ip nat pool Corp 198.18.41.129 198.18.41.134 netmask 255.255.255.248
ip nat inside source list 100 int pool Corp overload
```

    - `debug ip nat`
    - `show access-list`
    - `show ip nat translation`
    - `show ip nat statistics`
32. How many collision domains are created when you segment a network with a 12-port switch?
    - 1
    - 2
    - 5
    - 12
33. Which of the following commands will allow you to set your Telnet password on a Cisco router?
    - `line telnet 0 4`
    - `line aux 0 4`
    - `line vty 0 4`
    - `line con 0`
34. Which router command allows you to view the entire contents of all access lists?
    - `show all access-lists`
    - `show access-lists`
    - `show ip interface`

- `show interface`

35. What does a VLAN do?
    - Acts as the fastest port to all servers
    - Provides multiple collision domains on one switch port
    - Breaks up broadcast domains in a layer 2 switch internetwork
    - Provides multiple broadcast domains within a single collision domain
36. If you wanted to delete the configuration stored in NVRAM, choose the best answer for the Cisco objectives.
    - `erase startup`
    - `delete running`
    - `erase flash`
    - `erase running`
37. Which protocol is used to send a destination network unknown message back to originating hosts?
    - TCP
    - ARP
    - ICMP
    - BootP
38. Which class of IP address provides 15 bits for subnetting?
    - A
    - B
    - C
    - D
39. There are three possible routes for a router to reach a destination network. The first route is from OSPF with a metric of 782. The second route is from RIPv2 with a metric of 4. The third is from EIGRP with a composite metric of 20514560. Which route will be installed by the router in its routing table?
    - RIPv2
    - EIGRP
    - OSPF
    - All three
40. Which one of the following is true regarding VLANs?
    - Two VLANs are configured by default on all Cisco switches.
    - VLANs only work if you have a complete Cisco switched internetwork. No off-brand switches are allowed.
    - You should not have more than 10 switches in the same VTP domain.
    - You need to have a trunk link configured between switches in order to send information about more than one VLAN down the link.
41. Which two of the following commands will place network 10.2.3.0/24 into area 0? (Choose two.)
    - `router eigrp 10`
    - `router ospf 10`
    - `router rip`
    - `network 10.0.0.0`
    - `network 10.2.3.0 255.255.255.0 area 0`
    - `network 10.2.3.0 0.0.0.255 area0`
    - `network 10.2.3.0 0.0.0.255 area 0`
42. How many broadcast domains are created when you segment a network with a 12-port switch?
    - 1
    - 2
    - 5
    - 12
43. If routers in a single area are configured with the same priority value, what value does a router use for the OSPF router ID in the absence of a loopback interface?
    - The lowest IP address of any physical interface
    - The highest IP address of any physical interface
    - The lowest IP address of any logical interface
    - The highest IP address of any logical interface
44. What protocols are used to configure trunking on a switch? (Choose two.)
    - VLAN Trunking Protocol
    - VLAN
    - 802.1q
    - ISL
45. What is a stub network?
    - A network with more than one exit point
    - A network with more than one exit and entry point
    - A network with only one entry and no exit point
    - A network that has only one entry and exit point
46. Where is a hub specified in the OSI model?
    - Session layer
    - Physical layer

- Data Link layer
- Application layer

47. What are the two main types of access control lists (ACLs)? (Choose two.)
    - Standard
    - IEEE
    - Extended
    - Specialized
48. Which of the following is the best summarization of the following networks: 192.168.128.0 through 192.168.159.0?
    - 192.168.0.0/24
    - 192.168.128.0/16
    - 192.168.128.0/19
    - 192.168.128.0/20
49. What command is used to create a backup configuration?
    - `copy running backup`
    - `copy running-config startup-config`
    - `config mem`
    - `wr net`
50. 1000Base-T is which IEEE standard?
    - 802.3f
    - 802.3z
    - 802.3ab
    - 802.3ae
51. Which protocol does DHCP use at the Transport layer?
    - IP
    - TCP
    - UDP
    - ARP
52. If your router is facilitating a CSU/DSU, which of the following commands do you need to use to provide the router with a 64000 bps serial link?
    - `RouterA(config)#bandwidth 64`
    - `RouterA(config-if)#bandwidth 64000`
    - `RouterA(config)#clockrate 64000`
    - `RouterA(config-if)#clock rate 64`
    - `RouterA(config-if)#clock rate 64000`
53. Which command is used to determine if an access list is enabled on a particular interface?
    - `show access-lists`
    - `show interface`
    - `show ip interface`
    - `show interface access-lists`
54. Which of the following statements is true with regard to ISL and 802.1q?
    - 802.1q encapsulates the frame with control information; ISL inserts an ISL field along with tag control information.
    - 802.1q is Cisco proprietary.
    - ISL encapsulates the frame with control information; 802.1q inserts an 802.1q field along with tag control information.
    - ISL is a standard.
55. The protocol data unit (PDU) encapsulation is completed in which order?
    - Bits, frames, packets, segments, data
    - Data, bits, segments, frames, packets
    - Data, segments, packets, frames, bits
    - Packets, frames, bits, segments, data
56. Based on the configuration shown below, what statement is true?

```
S1(config)#ip routing
S1(config)#int vlan 10
S1(config-if)#ip address 192.168.10.1 255.255.255.0
S1(config-if)#int vlan 20
S1(config-if)#ip address 192.168.20.1 255.255.255.0
```

    - This is a multilayer switch.
    - The two VLANs are in the same subnet.
    - Encapsulation must be configured.
    - VLAN 10 is the management VLAN.

****

Answers to Assessment Test

1. B. To allow for the PVST+ to operate, there's a field inserted into the BPDU to accommodate the extended system ID so that PVST+ can have a root bridge configured on a per-STP instance. The extended system ID (VLAN ID) is a 12-bit field, and we can even see what this field is carrying via show spanning-tree command output. See Chapter 15 for more information.
2. A. Cisco's EtherChannel can bundle up to eight ports between switches to provide resiliency and more bandwidth between switches. See Chapter 15 for more information.
3. B, C, E. All the ports on both sides of every link must be configured exactly the same between switches or it will not work. Speed, duplex, and allowed VLANs must match. See Chapter 15 for more information.
4. C. 2100 boots the router into ROM monitor mode, 2101 loads the mini-IOS from ROM, and 2102 is the default and loads the IOS from flash. See Chapter 8 for more information.
5. D. The `show license udi` command displays the unique device identifier (UDI) of the router, which comprises the product ID (PID) and serial number of the router. See Chapter 8 for more information.
6. B. The `show license` feature command allows you to view the technology package licenses and feature licenses that are supported on your router along with several status variables related to software activation and licensing, both licensed and unlicensed features. See Chapter 8 for more information.
7. C, D, F. The SDN architecture slightly differs from the architecture of traditional networks. It comprises three stacked layers: Data, Control and Application. See Chapter 8 for more information.
8. B. There are eight different trap levels. If you choose, for example level 3, level 0 through level 3 messages will be displayed. See Chapter 8 for more information.
9. B, D. Each stack of switches has a single IP address and is managed as a single object. This single IP management applies to activities such as fault detection, VLAN creation and modification, security, and QoS controls. Each stack has only one configuration file, which is distributed to each member in the stack. When you add a new switch to the stack, the master switch automatically configures the unit with the currently running IOS image and the configuration of the stack. You do not have to do anything to bring up the switch before it is ready to operate. See chapter 22 for more information.
10. B. There is no IPv6 default gateway listed in the output, which will be the link-local address of the router interface, sent to the host as a router advertisement. Until this host receives the router address, the host will communicate with IPv6 only on the local subnet. See Chapter 20 for more information.
11. D. The command `show ipv6 neighbors` provides the ARP cache for on a router. See Chapter 20 for more information.
12. A. If the state is STALE when the interface has not communicated within the neighbor reachable time frame. The next time the neighbor communicates, the state will be REACH. See Chapter 20 for more information.
13. C. There are two successor routes, so by default, EIGRP was load-balancing out s0/0 and s0/1. When s0/1 goes down, EIGRP will just keep forwarding traffic out the second link s0/0. s0/1 will be removed from the routing table. See Chapter 17 for more information.
14. F. There isn't a lot to go on from with the output, but the only commands that provide the FD and AD are `show ip eigrp` topology and `show ipv6 eigrp topology`. The addresses in the output are link-local IPv6 addresses, so our answer is the latter. See Chapter 17 for more information.
15. A, B, C, D. Cisco has documented steps, according to the objectives, that you must go through when troubleshooting an adjacency. See Chapter 18 for more information.
16. B, D, E. In order for two OSPF routers to create an adjacency, the Hello and dead timers must match, and they must both be configured into the same area, as well as being in the same subnet. See Chapter 18 for more information.
17. A. The process starts by sending out Hello packets. Every listening router will then add the originating router to the neighbor database. The responding routers will reply with all of their Hello information so that the originating router can add them to its own neighbor table. At this point, we will have reached the 2WAY state—only certain routers will advance beyond to this. See Chapter 19 for more information.
18. C. Referred to as summary link advertisements (SLAs), Type 3 LSAs are generated by area border routers. These ABRs send Type 3 LSAs toward the area external to the one where they were generated. See Chapter 19 for more information.
19. B. Authentication Header (AH) provides authentication of either all or part of the IP packet through the addition of a header that is calculated based on the values in the packet, but it doesn't offer any encryption services. See Chapter 21 for more information.
20. B. Generic Routing Encapsulation (GRE) has no built-in security mechanisms. See Chapter 21 for more information.
21. C. When traffic exceeds the allocated rate, the policer can take one of two actions. It can either drop traffic or re-mark it to another class of service. The new class usually has a higher drop probability. See Chapter 21 for more information.
22. B. This can be a hard question if you don't remember to invert the 7th bit of the first octet in the MAC address! Always look for the 7th bit when studying for the Cisco R/S, and when using eui-64, invert it. The eui-64 autoconfiguration then inserts an FF:FE in the middle of the 48-bit MAC address to create a unique IPv6 address. See Chapter 14 for more information.
23. A. The NDP neighbor advertisement (NA) contains the MAC address. A neighbor solicitation (NS) was

initially sent asking for the MAC address. See Chapter 14 for more information.

24. B. Each field in an IPv6 address is 16 bits long. An IPv6 address is a total of 128 bits. See Chapter 14 for more information.
25. A. To enable OSPFv3, you enable the protocol at the interface level, as with RIPng. The command string is area-id. It's important to understand that area `0` and area `0.0.0.0` both describe area `0`. See Chapter 19 for more information.
26. C. The command line console `0` places you at a prompt where you can then set your console user-mode password. See Chapter 6 for more information.
27. B, D. The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256–254). So this makes the subnets in the interesting octet 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 2.0 subnet. The next subnet is 4.0, so the broadcast address for the 2.0 subnet is 3.255. The valid host addresses are 2.1 through 3.254. See Chapter 4 for more information.
28. C. The IP address is configured under a logical interface, called a management domain or VLAN 1, by default. See Chapter 10 for more information.
29. A. 256 – 192 = 64, so 64 is our block size. Just count in increments of 64 to find our subnet: 64 + 64 = 128. 128 + 64 = 192. The subnet is 128, the broadcast address is 191, and the valid host range is the numbers in between, or 129–190. See Chapter 4 for more information.
30. C. An inside global address is considered to be the IP address of the host on the private network after translation. See Chapter 13 for more information.
31. B. Once you create your pool, the command ip nat inside source must be used to say which inside locals are allowed to use the pool. In this question, we need to see if access list 100 is configured correctly, if at all, so `show access-list` is the best answer. See Chapter 13 for more information.
32. D. Layer 2 switching creates individual collision domains per port. See Chapter 1 for more information.
33. C. The command line vty 0 4 places you in a prompt that will allow you to set or change your Telnet password. See Chapter 6 for more information.
34. B. To see the contents of all access lists, use the `show access-lists` command. See Chapter 12 for more information.
35. C. VLANs break up broadcast domains at layer 2. See Chapter 11 for more information.
36. A. The command `erase startup-config` deletes the configuration stored in NVRAM. See Chapter 6 for more information.
37. C. ICMP is the protocol at the Network layer that is used to send messages back to an originating router. See Chapter 3 for more information.
38. A. Class A addressing provides 22 bits for host subnetting. Class B provides 16 bits, but only 14 are available for subnetting. Class C provides only 6 bits for subnetting. See Chapter 3 for more information.
39. B. Only the EIGRP route will be placed in the routing table because EIGRP has the lowest administrative distance (AD), and that is always used before metrics. See Chapter 8 for more information.
40. D. Switches send information about only one VLAN down a link unless it is configured as a trunk link. See Chapter 11 for more information.
41. B, G. To enable OSPF, you must first start OSPF using a process ID. The number is irrelevant; just choose a number from 1 to 65,535 and you're good to go. After you start the OSPF process, you must configure interfaces on which to activate OSPF using the network command with wildcards and specification of an area. Option F is wrong because there must be a space after the parameter area and before you list the area number. See Chapter 9 for more information.
42. A. By default, switches break up collision domains on a per-port basis but are one large broadcast domain. See Chapter 1 for more information.
43. B. At the moment of OSPF process startup, the highest IP address on any active interface will be the router ID (RID) of the router. If you have a loopback interface configured (logical interface), then that will override the interface IP address and become the RID of the router automatically. See Chapter 18 for more information.
44. C, D. VLAN Trunking Protocol (VTP) is not right because it has nothing to do with trunking except that it sends VLAN information across a trunk link. 802.1q and ISL encapsulations are used to configure trunking on a port. See Chapter 11 for more information.
45. D. Stub networks have only one connection to an internetwork. Default routes should be set on a stub network or network loops may occur; however, there are exceptions to this rule. See Chapter 9 for more information.
46. B. Hubs regenerate electrical signals, which are specified at the Physical layer. See Chapter 1 for more information.
47. A, C. Standard and extended access control lists (ACLs) are used to configure security on a router. See Chapter 12 for more information.
48. C. If you start at 192.168.128.0 and go through 192.168.159.0, you can see that this is a block of 32 in the third octet. Since the network address is always the first one in the range, the summary address is 192.168.128.0. What mask provides a block of 32 in the third octet? The answer is 255.255.224.0, or /19. See Chapter 5 for more information.
49. B. The command to back up the configuration on a router is `copy running-config startup-config`. See Chapter 7 for more information.

50. C. IEEE 802.3ab is the standard for 1 Gbps on twisted-pair. See Chapter 2 for more information.
51. C. User Datagram Protocol is a connection network service at the Transport layer, and DHCP uses this connectionless service. See Chapter 3 for more information
52. E. The clock rate command is two words, and the speed of the line is in bits per second (bps). See Chapter 6 for more information.
53. C. The `show ip interface` command will `show` you if any interfaces have an outbound or inbound access list set. See Chapter 12 for more information.
54. C. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information. See Chapter 11 for more information.
55. C. The PDU encapsulation method defines how data is encoded as it goes through each layer of the TCP/IP model. Data is segmented at the Transport later, packets created at the Network layer, frames at the Data Link layer, and finally, the Physical layer encodes the 1s and 0s into a digital signal. See Chapter 2 for more information.
56. A. With a multilayer switch, enable IP routing and create one logical interface for each VLAN using the interface vlan number command and you're now doing inter-VLAN routing on the backplane of the switch! See Chapter 11 for more information.

Assess ment Test

1. What is the `sys-id-ext` field in a BPDU used for?
   - It is a 4-bit field inserted into an Ethernet frame to define trunking information between switches.
   - It is a 12-bit field inserted into an Ethernet frame to define VLANs in an STP instance.
   - It is a 4-bit field inserted into an non-Ethernet frame to define EtherChannel options.
   - It is a 12-bit field inserted into an Ethernet frame to define STP root bridges.
2. You have four RSTP PVST+ links between switches and want to aggregate the bandwidth. What solution will you use?
   - EtherChannel
   - PortFast
   - BPDU Channel
   - VLANs
   - EtherBundle
3. What configuration parameters must be configured the same between switches for LACP to form a channel? (Choose three.)
   - Virtual MAC address
   - Port speeds
   - Duplex
   - PortFast enabled
   - Allowed VLAN information
4. You reload a router with a configuration register setting of 0x2101. What will the router do when it reloads?
   - The router enters setup mode.
   - The router enters ROM monitor mode.
   - The router boots the mini-IOS in ROM.
   - The router expands the first IOS in flash memory into RAM.
5. Which of the following commands provides the product ID and serial number of a router?
   - `show license`
   - `show license feature`
   - `show version`
   - `show license udi`
6. Which command allows you to view the technology options and licenses that are supported on your router along with several status variables?
   - `show license`
   - `show license feature`
   - `show license udi`
   - `show version`
7. Which of the following services provide the operating system and the network?
   - IaaS
   - PaaS
   - SaaS
   - none of the above
8. You want to send a console message to a syslog server, but you only want to send status messages of 3 and lower. Which of the following commands will you use?
   - `logging trap emergencies`
   - `logging trap errors`
   - `logging trap debugging`
   - `logging trap notifications`
   - `logging trap critical`
   - `logging trap warnings`
   - `logging trap alerts`
9. When stacking switches, which is true? (Choose 2)
   - The stack is managed as multiple objects, and has a single management IP address
   - The stack is managed as a single object, and has a single management IP address
   - The master switch is chosen when you configure the first switches master algorithm to on
   - The master switch is elected form one of the stack member switches
10. You need to connect to a remote IPv6 server in your virtual server farm. You can connect to the IPv4 servers, but not the critical IPv6 server you desperately need. Based on the following output, what could your problem be?

```
C:\>ipconfig
Connection-specific DNS Suffix . : localdomain
IPv6 Address. . . . . . . . . . . : 2001:db8:3c4d:3:ac3b:2ef:1823:8938
Temporary IPv6 Address. . . . . . : 2001:db8:3c4d:3:2f33:44dd:211:1c3d
Link-local IPv6 Address . . . . . : fe80::ac3b:2ef:1823:8938%11
IPv4 Address. . . . . . . . . . . : 10.1.1.10
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.1.1.1
```

- The global address is in the wrong subnet.
- The IPv6 default gateway has not been configured or received from the router.
- The link-local address has not been resolved so the host cannot communicate to the router.
- There are two IPv6 global addresses configured. One must be removed from the configuration.

11. What command is used to view the IPv6-to-MAC-address resolution table on a Cisco router?
    - `show ip arp`
    - `show ipv6 arp`
    - `show ip neighbors`
    - `show ipv6 neighbors`
    - `show arp`
12. An IPv6 ARP entry is listed as with a status of REACH. What can you conclude about the IPv6-to-MAC-address mapping?
    - The interface has communicated with the neighbor address and the mapping is current.
    - The interface has not communicated within the neighbor reachable time frame.
    - The ARP entry has timed out.
    - IPv6 can reach the neighbor address but the addresses has not yet been resolved.
13. Serial0/1 goes down. How will EIGRP send packets to the 10.1.1.0 network?

```
Corp#show ip eigrp topology
[output cut]
P 10.1.1.0/24, 2 successors, FD is 2681842
via 10.1.2.2 (2681842/2169856), Serial0/0
via 10.1.3.1 (2973467/2579243), Serial0/2
via 10.1.3.3 (2681842/2169856), Serial0/1
```

    - EIGRP will put the 10.1.1.0 network into active mode.
    - EIGRP will drop all packets destined for 10.1.1.0.
    - EIGRP will just keep sending packets out s0/0.
    - EIGRP will use s0/2 as the successor and keep routing to 10.1.1.0.
14. What command produced the following output?

```
via FE80::201:C9FF:FED0:3301 (29110112/33316), Serial0/0/0
via FE80::209:7CFF:FE51:B401 (4470112/42216), Serial0/0/1
via FE80::209:7CFF:FE51:B401 (2170112/2816), Serial0/0/2
```

    - `show ip protocols`
    - `show ipv6 protocols`
    - `show ip eigrp neighbors`
    - `show ipv6 eigrp neighbors`
    - `show ip eigrp topology`
    - `show ipv6 eigrp topology`
15. You need to troubleshoot an adjacency between two EIGRP configured routers? What should you look for? (Choose four.)
    - Verify the AS numbers.
    - Verify that you have the proper interfaces enabled for EIGRP.
    - Make sure there are no mismatched K-values.
    - Check your passive interface settings.
    - Make sure your remote routers are not connected to the Internet.
    - If authentication is configured, make sure all routers use different passwords.
16. You have two OSPF directly configured routers that are not forming an adjacency. What should you check? (Choose three.)
    - Process ID
    - Hello and dead timers
    - Link cost
    - Area
    - IP address/subnet mask
17. When do two adjacent routers-enter the 2WAY state?
    - After both routers have received Hello information
    - After they have exchanged topology databases
    - When they connect only to a DR or BDR
    - When they need to exchange RID information
18. Which type of LSAs are generated by ABRs and referred to summary link advertisements (SLAs)?
    - Type 1

- Type 2
- Type 3
- Type 4
- Type 5

19. Which of the following is not provided by the AH portion of IPsec?
    - Integrity
    - Confidentiality
    - Authenticity
    - Anti-reply
20. Which statement about GRE is not true?
    - GRE is stateless and has no flow control.
    - GRE has security.
    - GRE has additional overhead for tunneled packets, at least 24 bytes.
    - GRE uses a protocol-type field in the GRE header so any layer 3 protocol can be used through the tunnel.
21. Which QoS mechanism will drop traffic if a session uses more than the allotted bandwidth?
    - Congestion management
    - Shaping
    - Policing
    - Marking
22. IPv6 unicast routing is running on the Corp router. Which of the following addresses would show up with the show ipv6 int brief command?

```
Corp#sh int f0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000d.bd3b.0d80 (bia 000d.bd3b.0d80)
[output cut]
```

    - FF02::3c3d:0d:bdff:fe3b:0d80
    - FE80::3c3d:2d:bdff:fe3b:0d80
    - FE80::3c3d:0d:bdff:fe3b:0d80
    - FE80::3c3d:2d:ffbd:3bfe:0d80
23. A host sends a type of NDP message providing the MAC address that was requested. Which type of NDP was sent?
    - NA
    - RS
    - RA
    - NS
24. Each field in an IPv6 address is how many bits long?
    - 4
    - 16
    - 32
    - 128
25. To enable OSPFv3, which of the following would you use?
    - Router(config-if)#**ipv6 ospf 10 area 0.0.0.0**
    - Router(config-if)#**ipv6 router rip 1**
    - Router(config)#**ipv6 router eigrp 10**
    - Router(config-rtr)#**no shutdown**
    - Router(config-if)#**ospf ipv6 10 area 0**
26. What does the command `routerA(config)#line cons 0` allow you to perform next?
    - Set the Telnet password.
    - Shut down the router.
    - Set your console password.
    - Disable console connections.
27. Which two statements describe the IP address 10.16.3.65/23? (Choose two.)
    - The subnet address is 10.16.3.0 255.255.254.0.
    - The lowest host address in the subnet is 10.16.2.1 255.255.254.0.
    - The last valid host address in the subnet is 10.16.2.254 255.255.254.0.
    - The broadcast address of the subnet is 10.16.3.255 255.255.254.0.
    - The network is not subnetted.
28. On which interface do you configure an IP address for a switch?
    - int fa0/0
    - int vty 0 15
    - int vlan 1
    - int s/0/0
29. Which of the following is the valid host range for the subnet on which the IP address 192.168.168.188

255.255.255.192 resides?

- 192.168.168.129–190
- 192.168.168.129–191
- 192.168.168.128–190
- 192.168.168.128–192

30. Which of the following is considered to be the inside host's address after translation?
    - Inside local
    - Outside local
    - Inside global
    - Outside global
31. Your inside locals are not being translated to the inside global addresses. Which of the following commands will show you if your inside globals are allowed to use the NAT pool?

```
ip nat pool Corp 198.18.41.129 198.18.41.134 netmask 255.255.255.248
ip nat inside source list 100 int pool Corp overload
```

    - `debug ip nat`
    - `show access-list`
    - `show ip nat translation`
    - `show ip nat statistics`
32. How many collision domains are created when you segment a network with a 12-port switch?
    - 1
    - 2
    - 5
    - 12
33. Which of the following commands will allow you to set your Telnet password on a Cisco router?
    - `line telnet 0 4`
    - `line aux 0 4`
    - `line vty 0 4`
    - `line con 0`
34. Which router command allows you to view the entire contents of all access lists?
    - `show all access-lists`
    - `show access-lists`
    - `show ip interface`
    - `show interface`
35. What does a VLAN do?
    - Acts as the fastest port to all servers
    - Provides multiple collision domains on one switch port
    - Breaks up broadcast domains in a layer 2 switch internetwork
    - Provides multiple broadcast domains within a single collision domain
36. If you wanted to delete the configuration stored in NVRAM, choose the best answer for the Cisco objectives.
    - `erase startup`
    - `delete running`
    - `erase flash`
    - `erase running`
37. Which protocol is used to send a destination network unknown message back to originating hosts?
    - TCP
    - ARP
    - ICMP
    - BootP
38. Which class of IP address provides 15 bits for subnetting?
    - A
    - B
    - C
    - D
39. There are three possible routes for a router to reach a destination network. The first route is from OSPF with a metric of 782. The second route is from RIPv2 with a metric of 4. The third is from EIGRP with a composite metric of 20514560. Which route will be installed by the router in its routing table?
    - RIPv2
    - EIGRP
    - OSPF
    - All three
40. Which one of the following is true regarding VLANs?
    - Two VLANs are configured by default on all Cisco switches.
    - VLANs only work if you have a complete Cisco switched internetwork. No off-brand switches are allowed.

- You should not have more than 10 switches in the same VTP domain.
- You need to have a trunk link configured between switches in order to send information about more than one VLAN down the link.

41. Which two of the following commands will place network 10.2.3.0/24 into area 0? (Choose two.)
    - `router eigrp 10`
    - `router ospf 10`
    - `router rip`
    - `network 10.0.0.0`
    - `network 10.2.3.0 255.255.255.0 area 0`
    - `network 10.2.3.0 0.0.0.255 area0`
    - `network 10.2.3.0 0.0.0.255 area 0`
42. How many broadcast domains are created when you segment a network with a 12-port switch?
    - 1
    - 2
    - 5
    - 12
43. If routers in a single area are configured with the same priority value, what value does a router use for the OSPF router ID in the absence of a loopback interface?
    - The lowest IP address of any physical interface
    - The highest IP address of any physical interface
    - The lowest IP address of any logical interface
    - The highest IP address of any logical interface
44. What protocols are used to configure trunking on a switch? (Choose two.)
    - VLAN Trunking Protocol
    - VLAN
    - 802.1q
    - ISL
45. What is a stub network?
    - A network with more than one exit point
    - A network with more than one exit and entry point
    - A network with only one entry and no exit point
    - A network that has only one entry and exit point
46. Where is a hub specified in the OSI model?
    - Session layer
    - Physical layer
    - Data Link layer
    - Application layer
47. What are the two main types of access control lists (ACLs)? (Choose two.)
    - Standard
    - IEEE
    - Extended
    - Specialized
48. Which of the following is the best summarization of the following networks: 192.168.128.0 through 192.168.159.0?
    - 192.168.0.0/24
    - 192.168.128.0/16
    - 192.168.128.0/19
    - 192.168.128.0/20
49. What command is used to create a backup configuration?
    - `copy running backup`
    - `copy running-config startup-config`
    - `config mem`
    - `wr net`
50. 1000Base-T is which IEEE standard?
    - 802.3f
    - 802.3z
    - 802.3ab
    - 802.3ae
51. Which protocol does DHCP use at the Transport layer?
    - IP
    - TCP
    - UDP
    - ARP
52. If your router is facilitating a CSU/DSU, which of the following commands do you need to use to provide the router with a 64000 bps serial link?
    - `RouterA(config)#bandwidth 64`
    - `RouterA(config-if)#bandwidth 64000`
    - `RouterA(config)#clockrate 64000`

- `RouterA(config-if)#clock rate 64`
- `RouterA(config-if)#clock rate 64000`

53. Which command is used to determine if an access list is enabled on a particular interface?
    - `show access-lists`
    - `show interface`
    - `show ip interface`
    - `show interface access-lists`
54. Which of the following statements is true with regard to ISL and 802.1q?
    - 802.1q encapsulates the frame with control information; ISL inserts an ISL field along with tag control information.
    - 802.1q is Cisco proprietary.
    - ISL encapsulates the frame with control information; 802.1q inserts an 802.1q field along with tag control information.
    - ISL is a standard.
55. The protocol data unit (PDU) encapsulation is completed in which order?
    - Bits, frames, packets, segments, data
    - Data, bits, segments, frames, packets
    - Data, segments, packets, frames, bits
    - Packets, frames, bits, segments, data
56. Based on the configuration shown below, what statement is true?

```
S1(config)#ip routing
S1(config)#int vlan 10
S1(config-if)#ip address 192.168.10.1 255.255.255.0
S1(config-if)#int vlan 20
S1(config-if)#ip address 192.168.20.1 255.255.255.0
```

    - This is a multilayer switch.
    - The two VLANs are in the same subnet.
    - Encapsulation must be configured.
    - VLAN 10 is the management VLAN.

Answers to Ass essment Test

1. B. To allow for the PVST+ to operate, there's a field inserted into the BPDU to accommodate the extended system ID so that PVST+ can have a root bridge configured on a per-STP instance. The extended system ID (VLAN ID) is a 12-bit field, and we can even see what this field is carrying via show spanning-tree command output. See Chapter 15 for more information.
2. A. Cisco's EtherChannel can bundle up to eight ports between switches to provide resiliency and more bandwidth between switches. See Chapter 15 for more information.
3. B, C, E. All the ports on both sides of every link must be configured exactly the same between switches or it will not work. Speed, duplex, and allowed VLANs must match. See Chapter 15 for more information.
4. C. 2100 boots the router into ROM monitor mode, 2101 loads the mini-IOS from ROM, and 2102 is the default and loads the IOS from flash. See Chapter 8 for more information.
5. D. The `show license udi` command displays the unique device identifier (UDI) of the router, which comprises the product ID (PID) and serial number of the router. See Chapter 8 for more information.
6. B. The `show license` feature command allows you to view the technology package licenses and feature licenses that are supported on your router along with several status variables related to software activation and licensing, both licensed and unlicensed features. See Chapter 8 for more information.
7. C, D, F. The SDN architecture slightly differs from the architecture of traditional networks. It comprises three stacked layers: Data, Control and Application. See Chapter 8 for more information.
8. B. There are eight different trap levels. If you choose, for example level 3, level 0 through level 3 messages will be displayed. See Chapter 8 for more information.
9. B, D. Each stack of switches has a single IP address and is managed as a single object. This single IP management applies to activities such as fault detection, VLAN creation and modification, security, and QoS controls. Each stack has only one configuration file, which is distributed to each member in the stack. When you add a new switch to the stack, the master switch automatically configures the unit with the currently running IOS image and the configuration of the stack. You do not have to do anything to bring up the switch before it is ready to operate. See chapter 22 for more information.
10. B. There is no IPv6 default gateway listed in the output, which will be the link-local address of the router interface, sent to the host as a router advertisement. Until this host receives the router address, the host will communicate with IPv6 only on the local subnet. See Chapter 20 for more information.
11. D. The command `show ipv6 neighbors` provides the ARP cache for on a router. See Chapter 20 for more information.
12. A. If the state is STALE when the interface has not communicated within the neighbor reachable time frame. The next time the neighbor communicates, the state will be REACH. See Chapter 20 for more information.
13. C. There are two successor routes, so by default, EIGRP was load-balancing out s0/0 and s0/1. When s0/1 goes down, EIGRP will just keep forwarding traffic out the second link s0/0. s0/1 will be removed from the routing table. See Chapter 17 for more information.
14. F. There isn't a lot to go on from with the output, but the only commands that provide the FD and AD are `show ip eigrp` topology and `show ipv6 eigrp topology`. The addresses in the output are link-local IPv6 addresses, so our answer is the latter. See Chapter 17 for more information.
15. A, B, C, D. Cisco has documented steps, according to the objectives, that you must go through when troubleshooting an adjacency. See Chapter 18 for more information.
16. B, D, E. In order for two OSPF routers to create an adjacency, the Hello and dead timers must match, and they must both be configured into the same area, as well as being in the same subnet. See Chapter 18 for more information.
17. A. The process starts by sending out Hello packets. Every listening router will then add the originating router to the neighbor database. The responding routers will reply with all of their Hello information so that the originating router can add them to its own neighbor table. At this point, we will have reached the 2WAY state—only certain routers will advance beyond to this. See Chapter 19 for more information.
18. C. Referred to as summary link advertisements (SLAs), Type 3 LSAs are generated by area border routers. These ABRs send Type 3 LSAs toward the area external to the one where they were generated. See Chapter 19 for more information.
19. B. Authentication Header (AH) provides authentication of either all or part of the IP packet through the addition of a header that is calculated based on the values in the packet, but it doesn't offer any encryption services. See Chapter 21 for more information.
20. B. Generic Routing Encapsulation (GRE) has no built-in security mechanisms. See Chapter 21 for more information.
21. C. When traffic exceeds the allocated rate, the policer can take one of two actions. It can either drop traffic or re-mark it to another class of service. The new class usually has a higher drop probability. See Chapter 21 for more information.
22. B. This can be a hard question if you don't remember to invert the 7th bit of the first octet in the MAC address! Always look for the 7th bit when studying for the Cisco R/S, and when using eui-64, invert it. The eui-64 autoconfiguration then inserts an FF:FE in the middle of the 48-bit MAC address to create a unique IPv6 address. See Chapter 14 for more information.

23. A. The NDP neighbor advertisement (NA) contains the MAC address. A neighbor solicitation (NS) was initially sent asking for the MAC address. See Chapter 14 for more information.
24. B. Each field in an IPv6 address is 16 bits long. An IPv6 address is a total of 128 bits. See Chapter 14 for more information.
25. A. To enable OSPFv3, you enable the protocol at the interface level, as with RIPng. The command string is area-id. It's important to understand that area `0` and area `0.0.0.0` both describe area `0`. See Chapter 19 for more information.
26. C. The command line console `0` places you at a prompt where you can then set your console user-mode password. See Chapter 6 for more information.
27. B, D. The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256–254). So this makes the subnets in the interesting octet 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 2.0 subnet. The next subnet is 4.0, so the broadcast address for the 2.0 subnet is 3.255. The valid host addresses are 2.1 through 3.254. See Chapter 4 for more information.
28. C. The IP address is configured under a logical interface, called a management domain or VLAN 1, by default. See Chapter 10 for more information.
29. A. 256 – 192 = 64, so 64 is our block size. Just count in increments of 64 to find our subnet: 64 + 64 = 128. 128 + 64 = 192. The subnet is 128, the broadcast address is 191, and the valid host range is the numbers in between, or 129–190. See Chapter 4 for more information.
30. C. An inside global address is considered to be the IP address of the host on the private network after translation. See Chapter 13 for more information.
31. B. Once you create your pool, the command ip nat inside source must be used to say which inside locals are allowed to use the pool. In this question, we need to see if access list 100 is configured correctly, if at all, so `show access-list` is the best answer. See Chapter 13 for more information.
32. D. Layer 2 switching creates individual collision domains per port. See Chapter 1 for more information.
33. C. The command line vty 0 4 places you in a prompt that will allow you to set or change your Telnet password. See Chapter 6 for more information.
34. B. To see the contents of all access lists, use the `show access-lists` command. See Chapter 12 for more information.
35. C. VLANs break up broadcast domains at layer 2. See Chapter 11 for more information.
36. A. The command `erase startup-config` deletes the configuration stored in NVRAM. See Chapter 6 for more information.
37. C. ICMP is the protocol at the Network layer that is used to send messages back to an originating router. See Chapter 3 for more information.
38. A. Class A addressing provides 22 bits for host subnetting. Class B provides 16 bits, but only 14 are available for subnetting. Class C provides only 6 bits for subnetting. See Chapter 3 for more information.
39. B. Only the EIGRP route will be placed in the routing table because EIGRP has the lowest administrative distance (AD), and that is always used before metrics. See Chapter 8 for more information.
40. D. Switches send information about only one VLAN down a link unless it is configured as a trunk link. See Chapter 11 for more information.
41. B, G. To enable OSPF, you must first start OSPF using a process ID. The number is irrelevant; just choose a number from 1 to 65,535 and you're good to go. After you start the OSPF process, you must configure interfaces on which to activate OSPF using the network command with wildcards and specification of an area. Option F is wrong because there must be a space after the parameter area and before you list the area number. See Chapter 9 for more information.
42. A. By default, switches break up collision domains on a per-port basis but are one large broadcast domain. See Chapter 1 for more information.
43. B. At the moment of OSPF process startup, the highest IP address on any active interface will be the router ID (RID) of the router. If you have a loopback interface configured (logical interface), then that will override the interface IP address and become the RID of the router automatically. See Chapter 18 for more information.
44. C, D. VLAN Trunking Protocol (VTP) is not right because it has nothing to do with trunking except that it sends VLAN information across a trunk link. 802.1q and ISL encapsulations are used to configure trunking on a port. See Chapter 11 for more information.
45. D. Stub networks have only one connection to an internetwork. Default routes should be set on a stub network or network loops may occur; however, there are exceptions to this rule. See Chapter 9 for more information.
46. B. Hubs regenerate electrical signals, which are specified at the Physical layer. See Chapter 1 for more information.
47. A, C. Standard and extended access control lists (ACLs) are used to configure security on a router. See Chapter 12 for more information.
48. C. If you start at 192.168.128.0 and go through 192.168.159.0, you can see that this is a block of 32 in the third octet. Since the network address is always the first one in the range, the summary address is 192.168.128.0. What mask provides a block of 32 in the third octet? The answer is 255.255.224.0, or /19. See Chapter 5 for more information.
49. B. The command to back up the configuration on a router is `copy running-config startup-config`.

See Chapter 7 for more information.

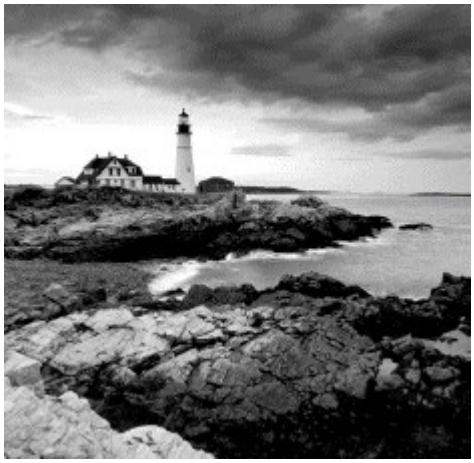
50. C. IEEE 802.3ab is the standard for 1 Gbps on twisted-pair. See Chapter 2 for more information.
51. C. User Datagram Protocol is a connection network service at the Transport layer, and DHCP uses this connectionless service. See Chapter 3 for more information
52. E. The clock rate command is two words, and the speed of the line is in bits per second (bps). See Chapter 6 for more information.
53. C. The `show ip interface` command will `show` you if any interfaces have an outbound or inbound access list set. See Chapter 12 for more information.
54. C. Unlike ISL, which encapsulates the frame with control information, 802.1q inserts an 802.1q field along with tag control information. See Chapter 11 for more information.
55. C. The PDU encapsulation method defines how data is encoded as it goes through each layer of the TCP/IP model. Data is segmented at the Transport later, packets created at the Network layer, frames at the Data Link layer, and finally, the Physical layer encodes the 1s and 0s into a digital signal. See Chapter 2 for more information.
56. A. With a multilayer switch, enable IP routing and create one logical interface for each VLAN using the interface vlan number command and you're now doing inter-VLAN routing on the backplane of the switch! See Chapter 11 for more information.

Part 1
ICND1

Chapter 1
Internetworking

THE FOLLOWING ICND1 EXAM TOPICS ARE COVERED IN THIS CHAPTER:

1. ✓ **Network Fundamentals**
    1. ▪ 1.3 Describe the impact of infrastructure components in an enterprise network
        1. ▪ 1.3.a Firewalls
        2. ▪ 1.3.b Access points
        3. ▪ 1.3.c Wireless controllers
    2. ▪ 1.5 Compare and contrast network topologies
        1. ▪ 1.5.a Star
        2. ▪ 1.5.b Mesh
        3. ▪ 1.5.c Hybrid



Welcome to the exciting world of internetworking. This first chapter will serve as an internetworking review by focusing on how to connect networks together using Cisco routers and switches, and I've written it with the assumption that you have some simple basic networking knowledge. The emphasis of this review will be on the Cisco CCENT and/or CCNA Routing and Switching (CCNA R/S) objectives, on which you'll need a solid grasp in order to succeed in getting your certifications.

Let's start by defining exactly what an internetwork is: You create an internetwork when you connect two or more networks via a router and configure a logical network addressing scheme with a protocol such as IP or IPv6.

We'll also dissect the Open Systems Interconnection (OSI) model, and I'll describe each part of it to you in detail because you really need complete, reliable knowledge of it. Understanding the OSI model is key for the solid foundation you'll need to build upon with the more advanced Cisco networking knowledge gained as you become increasingly more skilled.

The OSI model has seven hierarchical layers that were developed to enable different networks to communicate reliably between disparate systems. Since this book is centering upon all things CCNA, it's crucial for you to understand the OSI model as Cisco sees it, so that's how I'll be presenting the seven layers to you.

After you finish reading this chapter, you'll encounter review questions and written labs. These are given to you to really lock the information from this chapter into your memory. So don't skip them!

To find up-to-the-minute updates for this chapter, please see www.lammle.com/ccna or the book's web page via www.sybex.com/go/ccna.

Internetworking Basics

Before exploring inter networking models and the OSI model's specifications, you need to grasp the big picture and the answer to this burning question: Why is it so important to learn Cisco internetworking anyway?

Networks and networking have grown exponentially over the past 20 years, and understandably so. They've had to evolve at light speed just to keep up with huge increases in basic, mission-critical user needs (e.g., the simple sharing of data and printers) as well as greater burdens like multimedia remote presentations and conferencing. Unless everyone who needs to share network resources is located in the same office space—an increasingly uncommon situation—the challenge is to connect relevant networks so all users can share the wealth of whatever services and resources are required.

Figure 1.1 shows a basic *local area network (LAN)* that's connected using a *hub*, which is basically just an antiquated device that connects wires together. Keep in mind that a simple network like this would be considered one collision domain and one broadcast domain. No worries if you have no idea what I mean by that because coming up soon, I'm going to talk about collision and broadcast domains enough to make you dream about them!

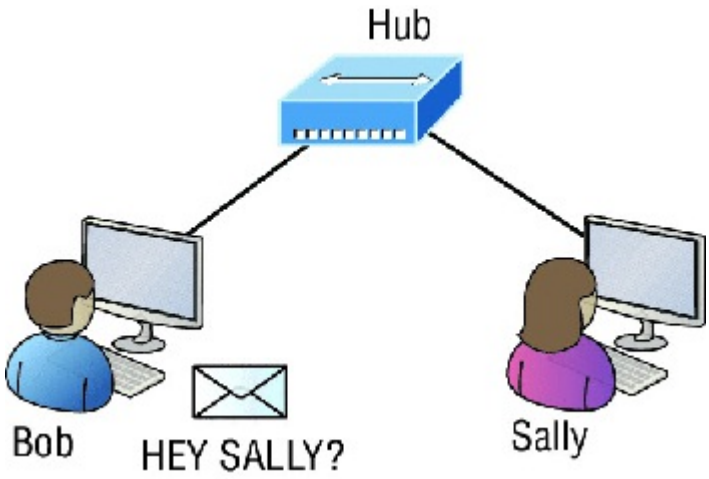


FIGURE 1.1 A very basic network

Things really can't get much simpler than this. And yes, though you can still find this configuration in some home networks, even many of those as well as the smallest business networks are more complicated today. As we move through this book, I'll just keep building upon this tiny network a bit at a time until we arrive at some really nice, robust, and current network designs—the types that will help you get your certification and a job!

But as I said, we'll get there one step at a time, so let's get back to the network shown in Figure 1.1 with this scenario: Bob wants to send Sally a file, and to complete that goal in this kind of network, he'll simply broadcast that he's looking for her, which is basically just shouting out over the network. Think of it like this: Bob walks out of his house and yells down a street called Chaos Court in order to contact Sally. This might work if Bob and Sally were the only ones living there, but not so much if it's crammed with homes and all the others living there are always hollering up and down the street to their neighbors just like Bob. Nope, Chaos Court would absolutely live up to its name, with all those residents going off whenever they felt like it—and believe it or not, our networks actually still work this way to a degree! So, given a choice, would you stay in Chaos Court, or would you pull up stakes and move on over to a nice new modern community called Broadway Lanes, which offers plenty of amenities and room for your home plus future additions all on nice, wide streets that can easily handle all present and future traffic? If you chose the latter, good choice… so did Sally, and she now lives a much quieter life, getting letters (packets) from Bob instead of a headache!

The scenario I just described brings me to the basic point of what this book and the Cisco certification objectives are really all about. My goal of showing you how to create efficient networks and segment them correctly in order to minimize all the chaotic yelling and screaming going on in them is a universal theme throughout my CCENT and CCNA series books. It's just inevitable that you'll have to break up a large network into a bunch of smaller ones at some point to match a network's equally inevitable growth, and as that expansion occurs, user response time simultaneously dwindles to a frustrating crawl. But if you master the vital technology and skills I have in store for you in this series, you'll be well equipped to rescue your network and its users by creating an efficient new network neighborhood to give them key amenities like the bandwidth they need to meet their evolving demands.

And this is no joke; most of us think of growth as good—and it can be—but as many of us experience daily when commuting to work, school, etc., it can also mean your LAN's traffic congestion can reach critical mass and grind to a complete halt! Again, the solution to this problem begins with breaking up a massive network into a number of smaller ones—something called *network segmentation*. This concept is a lot like planning a new community or modernizing an existing one. More streets are added, complete with new intersections and traffic signals, plus post offices are built with official maps documenting all those street names and directions on how to get to each. You'll need to effect new laws to keep order to it all and provide a police station to protect this nice new neighborhood as well. In a networking neighborhood environment, all of this is carried out using devices like *routers, switches*, and

bridges.

So let's take a look at our new neighborhood now, because the word has gotten out; many more hosts have moved into it, so it's time to upgrade that new high-capacity infrastructure that we promised to handle the increase in population. Figure 1.2 shows a network that's been segmented with a switch, making each network segment that connects to the switch its own separate c ollision domain. Doing this results in a lot less yelling!

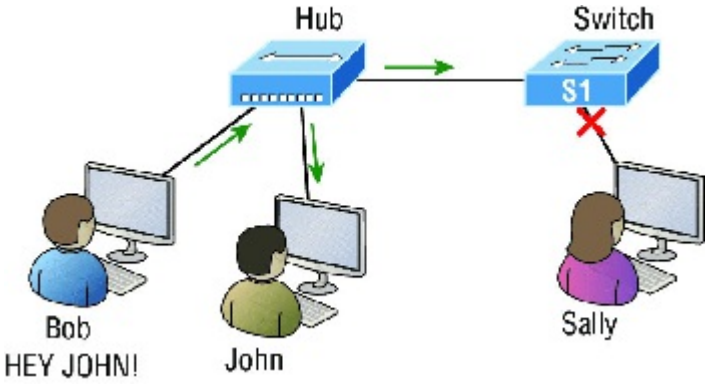


FIGURE 1.2 A switch can break up collision domains.

This is a great start, but I really want you to make note of the fact that this network is still one, single broadcast domain, meaning that we've really only decreased our screaming and yelling, not eliminated it. For example, if there's some sort of vital announcement that everyone in our neighborhood needs to hear about, it will definitely still get loud! You can see that the hub used in Figure 1.2 just extended the one collision domain from the switch port. The result is that John received the data from Bob but, happily, Sally did not. This is good because Bob intended to talk with John directly, and if he had needed to send a broadcast instead, everyone, including Sally, would have received it, possibly causing unnecessary congestion.

Here's a list of some of the things that commonly cause LAN traffic congestion:

1. Too many hosts in a collision or broadcast domain
2. Broadcast storms
3. Too much multicast traffic
4. Low bandwidth
5. Adding hubs for connectivity to the network
6. A bunch of ARP broadcasts

Take another look at Figure 1.2 and make sure you see that I extended the main hub from Figure 1.1 to a switch in Figure 1.2. I did that because hubs don't segment a network; they just connect network segments. Basically, it's an inexpensive way to connect a couple of PCs, and again, that's great for home use and troubleshooting, but that's about it!

As our planned community starts to grow, we'll need to add more streets with traffic control, and even some basic security. We'll achieve this by adding routers because these convenient devices are used to connect networks and route packets of data from one network to another. Cisco became the de facto standard for routers because of its unparalleled selection of high-quality router products and fantastic service. So never forget that by default, routers are basically employed to efficiently break up a *broadcast domain*—the set of all devices on a network segment, which are allowed to "hear" all broadcasts sent out on that specific segment.

Figure 1.3 depicts a router in our growing network, creating an internetwork and breaking up broadcast domains.

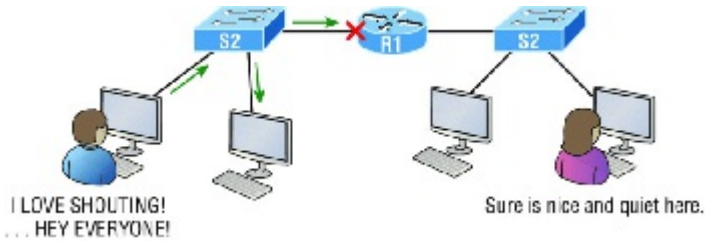


FIGURE 1.3 Routers create an internetwork.

The network in Figure 1.3 is actually a pretty cool little network. Each host is connected to its own collision domain

because of the switch, and the router has created two broadcast domains. So now our Sally is happily living in peace in a completely different neighborhood, no longer subjected to Bob's incessant shouting! If Bob wants to talk with Sally, he has to send a packet with a destination address using her IP address—he cannot broadcast for her!

But there's more… routers provide connections to *wide area network (WAN)* services as well via a serial interface for WAN connections—specifically, a V.35 physical interface on a Cisco router.

Let me make sure you understand why breaking up a broadcast domain is so important. When a host or server sends a network broadcast, every device on the network must read and process that broadcast—unless you have a router. When the router's interface receives this broadcast, it can respond by basically saying, "Thanks, but no thanks," and discard the broadcast without forwarding it on to other networks. Even though routers are known for breaking up broadcast domains by default, it's important to remember that they break up collision domains as well.

There are two advantages to using routers in your network:

1. They don't forward broadcasts by default.
2. They can filter the network based on layer 3 (Network layer) information such as an IP address.

Here are four ways a router functions in your network:

1. Packet switching
2. Packet filtering
3. Internetwork communication
4. Path selection

I'll tell you all about the various layers later in this chapter, but for now, it's helpful to think of routers as layer 3 switches. Unlike plain-vanilla layer 2 switches, which forward or filter frames, routers (layer 3 switches) use logical addressing and provide an important capacity called *packet switching*. Routers can also provide packet filtering via access lists, and when routers connect two or more networks together and use logical addressing (IP or IPv6), you then have an *internetwork*. Finally, routers use a routing table, which is essentially a map of the internetwork, to make best path selections for getting data to its proper destination and properly forward packets to remote networks.

Conversely, we don't use layer 2 switches to create internetworks because they don't break up broadcast domains by default. Instead, they're employed to add functionality to a network LAN. The main purpose of these switches is to make a LAN work better—to optimize its performance—providing more bandwidth for the LAN's users. Also, these switches don't forward packets to other networks like routers do. Instead, they only "switch" frames from one port to another within the switched network. And don't worry, even though you're probably thinking, "Wait—what are frames and packets?" I promise to completely fill you in later in this chapter. For now, think of a packet as a package containing data.

Okay, so by default, switches break up collision domains, but what are these things? *Collision domain* is an Ethernet term used to describe a network scenario in which one device sends a packet out on a network segment and every other device on that same segment is forced to pay attention no matter what. This isn't very efficient because if a different device tries to transmit at the same time, a collision will occur, requiring both devices to retransmit, one at a time—not good! This happens a lot in a hub environment, where each host segment connects to a hub that represents only one collision domain and a single broadcast domain. By contrast, each and every port on a switch represents its own collision domain, allowing network traffic to flow much more smoothly.

Switches create separate collision domains within a single broadcast domain. Routers provide a separate broadcast domain for each interface. Don't let this ever confuse you!

The term *bridging* was introduced before routers and switches were implemented, so it's pretty common to hear people referring to switches as bridges. That's because bridges and switches basically do the same thing—break up collision domains on a LAN. Note to self that you cannot buy a physical bridge these days, only LAN switches, which use bridging technologies. This does not mean that you won't still hear Cisco and others refer to LAN switches as multiport bridges now and then.

But does it mean that a switch is just a multiple-port bridge with more brainpower? Well, pretty much, only there are still some key differences. Switches do provide a bridging function, but they do that with greatly enhanced management ability and features. Plus, most bridges had only 2 or 4 ports, which is severely limiting. Of course, it was possible to get your hands on a bridge with up to 16 ports, but that's nothing compared to the hundreds of ports available on some switches!

You would use a bridge in a network to reduce collisions within broadcast domains and to increase the number of collision domains in your network. Doing this provides more bandwidth for users. And never forget that using hubs in your Ethernet network can contribute to congestion. As always, plan your network design carefully!

Figure 1.4 shows how a network would look with all these internetwork devices in place. Remember, a router doesn't just break up broadcast domains for every LAN interface, it breaks up collision domains too.

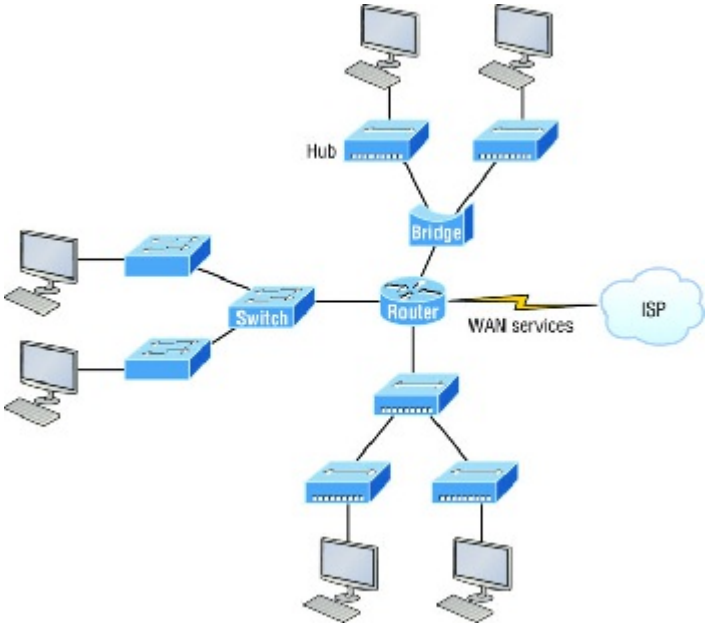


FIGURE 1.4 Internetworking devices

Looking at Figure 1.4, did you notice that the router has the center stage position and connects each physical network together? I'm stuck with using this layout because of the ancient bridges and hubs involved. I really hope you don't run across a network like this, but it's still really important to understand the strategic ideas that this figure represents!

See that bridge up at the top of our internetwork shown in Figure 1.4? It's there to connect the hubs to a router. The bridge breaks up collision domains, but all the hosts connected to both hubs are still crammed into the same broadcast domain. That bridge also created only three collision domains, one for each port, which means that each device connected to a hub is in the same collision domain as every other device connected to that same hub. This is really lame and to be avoided if possible, but it's still better than having one collision domain for all hosts! So don't do this at home; it's a great museum piece and a wonderful example of what not to do, but this inefficient design would be terrible for use in today's networks! It does show us how far we've come though, and again, the foundational concepts it illustrates are really important for you to get.

And I want you to notice something else: The three interconnected hubs at the bottom of the figure also connect to the router. This setup creates one collision domain and one broadcast domain and makes that bridged network, with its two collision domains, look majorly better by contrast!

Don't misunderstand… bridges/switches are used to segment networks, but they will not isolate broadcast or multicast packets.

The best network connected to the router is the LAN switched network on the left. Why? Because each port on that switch breaks up collision domains. But it's not all good—all devices are still in the same broadcast domain. Do you remember why this can be really bad? Because all devices must listen to all broadcasts transmitted, that's why! And if your broadcast domains are too large, the users have less bandwidth and are required to process more broadcasts. Network response time eventually will slow to a level that could cause riots and strikes, so it's important to keep your broadcast domains small in the vast majority of networks today.

Once there are only switches in our example network, things really change a lot! Figure 1.5 demonstrates a

network you'll typically stumble upon today.

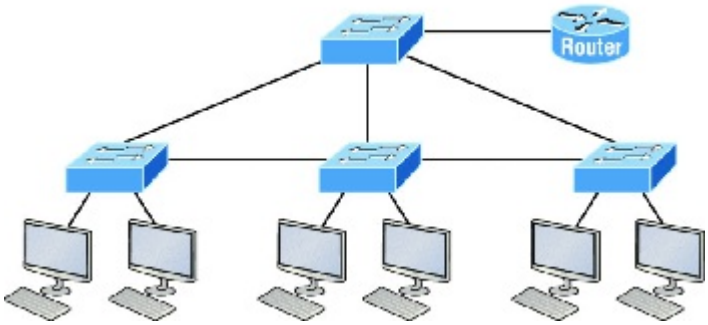


FIGURE 1.5 Switched networks creating an internetwork

Here I've placed the LAN switches at the center of this network world, with the router connecting the logical networks. If I went ahead and im plemented this design, I'll have created something called virtual LANs, or VLANs, which are used when you logically break up broadcast domains in a layer 2, switched network. It's really important to understand that even in a switched network environment, you still need a router to provide communication between VLANs. Don't forget that!

Still, clearly the best network design is the one that's perfectly configured to meet the business requirements of the specific company or client it serves, and it's usually one in which LAN switches exist in harmony with routers strategically placed in the network. It's my hope that this book will help you understand the basics of routers and switches so you can make solid, informed decisions on a case-by-case basis and be able to achieve that goal! But I digress…

So let's go back to Figure 1.4 now for a minute and really scrutinize it because I want to ask you this question: How many collision domains and broadcast domains are really there in this internetwork? I hope you answered nine collision domains and three broadcast domains! The broadcast domains are definitely the easiest to spot because only routers break up broadcast domains by default, and since there are three interface connections, that gives you three broadcast domains. But do you see the nine collision domains? Just in case that's a no, I'll explain. The all-hub network at the bottom is one collision domain; the bridge network on top equals three collision domains. Add in the switch network of five collision domains—one for each switch port—and you get a total of nine!

While we're at this, in Figure 1.5, each port on the switch is a separate collision domain, and each VLAN would be a separate broadcast domain. So how many collision domains do you see here? I'm counting 12—remember that connections between the switches are considered a collision domain! Since the figure doesn't show any VLAN information, we can assume the default of one broadcast domain is in place.

Before we move on to Internetworking Models, let's take a look at a few more network devices that we'll find in pretty much every network today as shown in Figure 1.6.

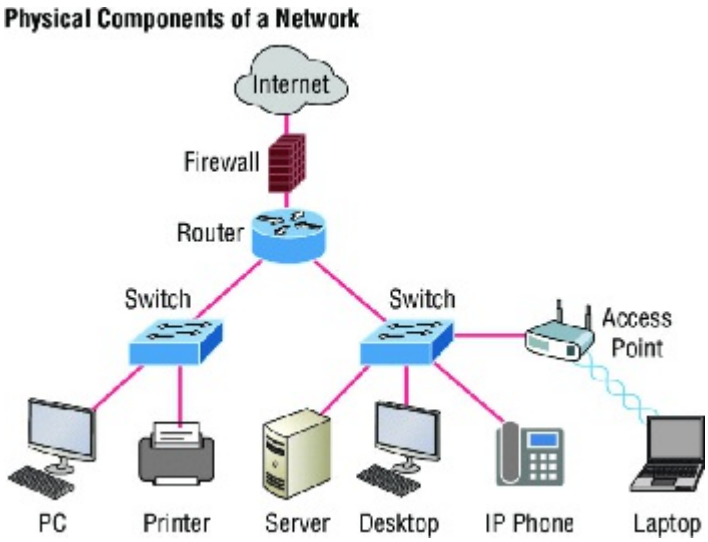


FIGURE 1.6 Other devices typically found in our internetworks to day.

Taking off from the switched network in Figure 1.5, you'll find WLAN devices, i ncluding AP's and wireless controllers, and firewalls. You'd be hard pressed not to find these devices in your networks today.

Let's look closer at these devices:

1. WLAN devices: These devices connect wireless devices such as computers, printers, and tablets to the network. Since pretty much every device manufactured today has a wireless NIC, you just need to configure a basic access point (AP) to connect to a traditional wired network.
2. Access Points or APs: These devices allow wireless devices to connect to a wired network and extend a collision domain from a switch, and are typically in their own broadcast domain or what we'll refer to as a Virtual LAN (VLAN). An AP can be a simple standalone device, but today they are usually managed by wireless controllers either in house or through the internet.
3. WLAN Controllers: These are the devices that network administrators or network operations centers use to manage access points in medium to large to extremely large quantities. The WLAN controller automatically handles the configuration of wireless access points and was typically used only in larger enterprise systems. However, with Cisco's acquisition of Meraki systems, you can easily manage a small to medium sized wireless network via the cloud using their simple to configure web controller system.
4. Firewalls: These devices are network security systems that monitor and control the incoming and outgoing network traffic based on predetermined security rules, and is usually an Intrusion Protection System (IPS). Cisco Adaptive Security Appliance (ASA) firewall typically establishes a barrier between a trusted, secure internal network and the Internet, which is not secure or trusted. Cisco's new acquisition of Sourcefire put them in the top of the market with Next Generation Firewalls (NGFW) and Next Generation IPS (NGIPS), which Cisco now just calls Firepower. Cisco new Firepower runs on dedicated appliances, Cisco's ASA's, ISR routers and even on Meraki products.

Should I Replace My Existing 10/100 Mbps Switches?

Let's say you're a network administrator at a large company. The boss comes to you and says that he got your requisition to buy a bunch of new switches but he's really freaking out about the price tag! Should you push it—do you really need to go this far?

Absolutely! Make your case and go for it because the newest switches add really huge capacity to a network that older 10/100 Mbps switches just can't touch. And yes, five-year-old switches are considered pretty Pleistocene these days. But in reality, most of us just don't have an unlimited budget to buy all new gigabit switches; however, 10/100 switches are just not good enough in today's networks.

Another good question: Do you really need low-latency 1 Gbps or better switch ports for all your users, servers, and other devices? Yes, you *absolutely* need new higher-end switches! This is because servers and hosts are no longer the bottlenecks of our internetworks, our routers and switches are—especially legacy ones. We now need gigabit on the desktop and on every router interface; 10 Gbps is now the minimum between switch uplinks, so go to 40 or even 100 Gbps as uplinks if you can afford it.

Go ahead. Put in that requisition for all new switches. You'll be a hero before long!

Okay, so now that you've gotten a pretty thorough introduction to internetworking and the various devices that populate an internetwork, it's time to head into exploring the internetworking models.

Internetworking Models

First a little history: When networks first came into being, computers could typically communicate only with computers from the same manufacturer. For example, companies ran either a complete DECnet solution or an IBM solution, never both together. In the late 1970s, the *Op en Systems Interconnection (OSI) reference model* was created by the International Organization for Standardization (ISO) to break through this barrier.

The OSI model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work in peaceable accord with each other. Like world peace, it'll probably never happen completely, but it's still a great goal!

Anyway the OSI model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.

Coming up, I'll explain the layered approach to you plus how we can use it to help us troubleshoot our internetworks.


Goodness! ISO, OSI, and soon you'll hear about IOS! Just remember that the ISO created the OSI and that Cisco created the Internetworking Operating System (IOS), which is what this book is all-so-about.

The Layered Approach

Understand that a *reference model* is a conceptual blueprint of how communications should take place. It addresses all the processes required for effective communication and divides them into logical groupings called *layers*. When a communication system is designed in this manner, it's known as a hierarchical or *layered architecture*.

Think of it like this: You and some friends want to start a company. One of the first things you'll do is sort out every task that must be done and decide who will do what. You would move on to determine the order in which you would like everything to be done with careful consideration of how all your specific operations relate to each other. You would then organize everything into departments (e.g., sales, inventory, and shipping), with each department dealing with its specific responsibilities and keeping its own staff busy enough to focus on their own particular area of the enterprise.

In this scenario, departments are a metaphor for the layers in a communication system. For things to run smoothly, the staff of each department has to trust in and rely heavily upon those in the others to do their jobs well. During planning sessions, you would take notes, recording the entire process to guide later discussions and clarify standards of operation, thereby creating your business blueprint—your own reference model.

And once your business is launched, your department heads, each armed with the part of the blueprint relevant to their own department, will develop practical ways to implement their distinct tasks. These practical methods, or protocols, will then be compiled into a standard operating procedures manual and followed closely because each procedure will have been included for different reasons, delimiting their various degrees of importance and implementation. All of this will become vital if you form a partnership or acquire another company because then it will be really important that the new company's business model is compatible with yours!

Models happen to be really important to software developers too. They often use a reference model to understand computer communication processes so they can determine which functions should be accomplished on a given layer. This means that if someone is creating a protocol for a certain layer, they only need to be concerned with their target layer's function. Software that maps to another layer's protocols and is specifically designed to be deployed there will handle additional functions. The technical term for this idea is *binding*. The communication processes that are related to each other are bound, or grouped together, at a particular layer.

Advantages of Reference Models

The OSI model is hierarchical, and there are many advantages that can be applied to any layered model, but as I said, the OSI model's primary purpose is to allow different vendors' networks to interoperate.

Here's a list of some of the more important benefits of using the OSI layered model:

1. It divides the network communication process into smaller and simpler components, facilitating component development, design, and troubleshooting.
2. It allows multiple-vendor development through the standardization of network components.
3. It encourages industry standardization by clearly defining what functions occur at each layer of the model.
4. It allows various types of network hardware and software to communicate.
5. It prevents changes in one layer from affecting other layers to expedite development.

The OSI Reference Model

One of best gifts the OSI specifications gives us is paving the way for the data transfer between disparate hosts running different operating systems, like Unix hosts, Windows machines, Macs, smartphones, and so on.

And remember, the OSI is a logi cal model, not a physical one. It's essentially a set of guidelines that developers can use to create and implement applications to run on a network. It also provides a framework for creating and implementing networking standards, devices, and internetworking schemes.

The OSI has seven different layers, divided into two groups. The top three layers define how the applications within the end stations will communicate with each other as well as with users. The bottom four layers define how data is transmitted end to end.

Figure 1.7 shows the three upper layers and their functions.

Application	• Provides a user interface
Presentation	• Presents data • Handles processing such as encryption
Session	• Keeps different applications' data separate

FIGURE 1.7 The upper layers

When looking at Figure 1.6, understand that users interact with the computer at the Application layer and also that the upper layers are responsible for applications communicating between hosts. None of the upper layers knows anything about networking or network addresses because that's the responsibility of the four bottom layers.

In Figure 1.8, which shows the four lower layers and their functions, you can see that it's these four bottom layers that define how data is transferred through physical media like wire, cable, fiber optics, switches, and routers. These bottom layers also determine how to rebuild a data stream from a transmitting host to a destination host's pplication.

Transport	• Provides reliable or unreliable delivery • Performs error correction before retransmit
Network	• Provides logical addressing, which routers use for path determination
Data Link	• Combines packets into bytes and bytes into frames • Provides access to media using MAC address • Performs error detection not correction
Physical	• Moves bits between devices • Specifies voltage, wire speed, and pinout of cables

FIGURE 1.8 The lower layers

The following network devices operate at all seven layers of the OSI model:

1. *Network management stations (NMSs)*
2. Web and application servers
3. Gateways (not default gateways)
4. Servers
5. Network hosts

Basically, the ISO is pretty much the Emily Post of the network protocol world. Just as Ms. Post wrote the book setting the standards—or protocols—for human social interaction, the ISO developed the OSI reference model as the precedent and guide for an open network protocol set. Defining the etiquette of communication models, it remains the most popular means of comparison for protocol suites today.

The OSI reference model has the following seven layers:

1. Application layer (layer 7)
2. Presentation layer (layer 6)
3. Session layer (layer 5)
4. Transport layer (layer 4)
5. Network layer (layer 3)
6. Data Link layer (layer 2)
7. Physical layer (layer 1)

Some people like to use a mnemonic to remember the seven layers, such as All People Seem To Need Data Processing. Figure 1.9 shows a summary of the functions defined at each layer of the OSI model.

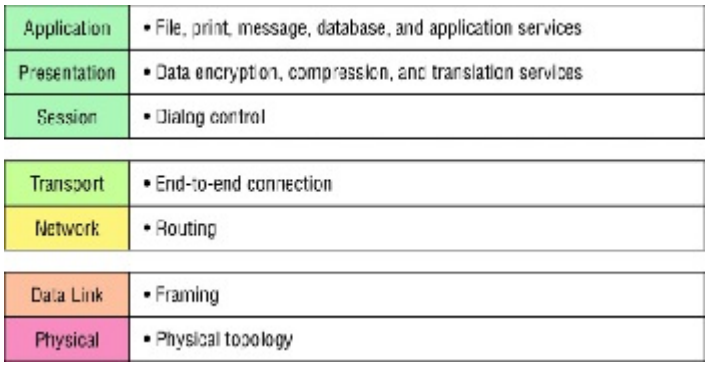


FIGURE 1.9 OSI layer functions

I've separated the seven-layer model into three different functions: the upper layers, the middle layers, and the bottom layers. The upper layers communicate with the user interface and application, the middle layers do reliable communication and routing to a remote network, and t he bottom layers communicate to the local network.

With this in hand, you're now ready to explore each layer's function in detail!

The Application Layer

The *Application layer* of the OSI model marks the spot where users actually communicate to the computer and comes into play only when it's clear that access to the network will be needed soon. Take the case of Internet Explorer (IE). You could actually uninstall every trace of networking components like TCP/IP, the NIC card, and so on and still use IE to view a local HTML document. But things would get ugly if you tried to do things like view a remote HTML document that must be retrieved because IE and other browsers act on these types of requests by attempting to access the Application layer. So basically, the Application layer is working as the interface between the actual application program and the next layer down by providing ways for the application to send information down through the protocol stack. This isn't actually part of the layered structure, because browsers don't live in the Application layer, but they interface with it as well as the relevant protocols when asked to access remote resources.

Identifying and confirming the communication partner's availability and verifying the required resources to permit the specified type of communication to take place also occurs at the Application layer. This is important because, like the lion's share of browser functions, computer applications sometimes need more than desktop resources. It's more typical than you would think for the communicating components of several network applications to come together to carry out a requested function. Here are a few good examples of these kinds of events:

1. File transfers
2. Email
3. Enabling remote access
4. Network management activities
5. Client/server processes
6. Information location

Many network applications provide services for communication over enterprise networks, but for present and future internetworking, the need is fast developing to reach beyond the limits of current physical networking.

The Application layer works as the interface between actual application programs. This means end-user programs like Microsoft Word don't reside at the Application layer, they interface with the Application layer protocols. Later, in Chapter 3, "Introduction to TCP/IP," I'll talk in detail about a few important programs that actually reside at the Application layer, like Telnet, FTP, and TFTP.

The Presentation Layer

The *Presentation layer* gets its name from its purpose: It presents data to the Application layer and is responsible for data translation and code formatting. Think of it as the OSI model's translator, providing coding and conversion services. One very effective way of ensuring a successful data transfer is to convert the data into a standard format before transmission. Computers are configured to receive this generically formatted data and then reformat it back into its native state to read it. An example of this type of translation service occurs when translating old Extended Binary Coded Decimal Interchange Code (EBCDIC) data to ASCII, the American Standard Code for Information Interchange (often pronounced "askee"). So just remember that by providing translation services, the Presentation

layer ensures that data transferred from the Application layer of one system can be read by the Application layer of another one.

With this in mind, it follows that the OSI would include protocols that define how standard data should be formatted, so key functions like data compression, decompression, encryption, and decryption are also associated with this layer. Some Presentation layer standards are involved in multimedia operations as well.

The Session Layer

The *Session layer* is responsible for setting up, managing, and dismantling sessions between Presentation layer entities and keeping user data separate. Dialog control between devices also occurs at this layer.

Communication between hosts' various applications at the Session layer, as from a client to a server, is coordinated and organized via three different modes: *simplex*, *half-duplex*, and *full-duplex*. Simplex is simple one-way communication, kind of like saying something and not getting a reply. Half-duplex is actual two-way communication, but it can take place in only one direction at a time, preventing the interruption of the transmitting device. It's like when pilots and ship captains communicate over their radios, or even a walkie-talkie. But full-duplex is exactly like a real conversation where devices can transmit and receive at the same time, much like two people arguing or interrupting each other during a telephone conversation.

The Transport Layer

The *Transport layer* segments and reassembles data into a single data stream. Services located at this layer take all the various data received from upper-layer applications, then combine it into the same, concise data stream. These protocols provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an internetwork.

A pair of well-known protocols called TCP and UDP are integral to this layer, but no worries if you're not already familiar with them because I'll bring you up to speed later, in Chapter 3. For now, understand that although both work at the Transport layer, TCP is known as a reliable service but UDP is not. This distinction gives application developers more options because they have a choice between the two protocols when they are designing products for this layer.

The Transport layer is responsible for providing mechanisms for multiplexing upper-layer applications, establishing sessions, and tearing down virtual circuits. It can also hide the details of network-dependent information from the higher layers as well as provide transparent data transfer.

The term *reliable networking* can be used at the Transport layer. Reliable networking requires that acknowledgments, sequencing, and flow control will all be used.

The Transport layer can be either connectionless or connection-oriented, but because Cisco really wants you to understand the connection-oriented function of the Transport layer, I'm going to go into that in more detail here.

Connection-Oriented Communication

For reliable transport to occur, a device that wants to transmit must first establish a connection-oriented communication session with a remote device—its peer system—known as a *call setup* or a *three-way handshake*. Once this process is complete, the data transfer occurs, and when it's finished, a call termination takes place to tear down the virtual circuit.

Figure 1.10 depicts a typical reliable session taking place between sending and receiving systems. In it, you can see that both hosts' application programs begin by notifying their individual operating systems that a connection is about to be initiated. The two operating systems communicate by sending messages over the network confirming that the transfer is approved and that both sides are ready for it to t ake place. After all of this required synchronization takes place, a connection is fully established and the data transfer begins. And by the way, it's really helpful to understand that this virtual circuit setup is often referred to as overhead!

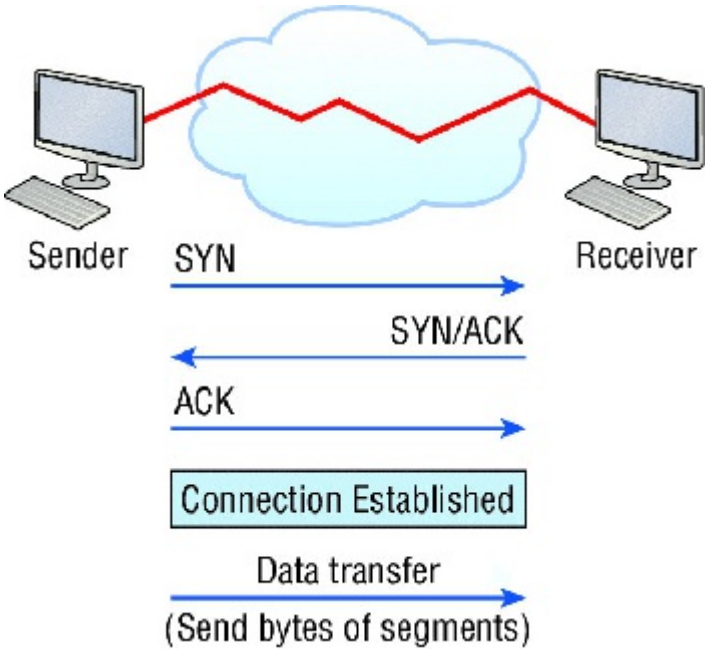


FIGURE 1.10 Establishing a connection-oriented session

Okay, now while the information is being transferred between hosts, the two machines periodically check in with each other, communicating through their protocol software to ensure that all is going well and that the data is being received properly.

Here's a summary of the steps in the connection-oriented session—that three-way handshake—pictured in Figure 1.9:

1. The first "connection agreement" segment is a request for *synchronization (SYN)*.
2. The next segments *acknowledge (ACK)* the request and establish connection parameters—the rules—between hosts. These segments request that the receiver's sequencing is synchronized here as well so that a bidirectional connection can be formed.
3. The final segment is also an acknowledgment, which notifies the destination host that the connection agreement has been accepted and that the actual connection has been established. Data transfer can now begin.

Sounds pretty simple, but things don't always flow so smoothly. Sometimes during a transfer, congestion can occur because a high-speed computer is generating data traffic a lot faster than the network itself can process it! And a whole bunch of computers simultaneously sending datagrams through a single gateway or destination can also jam things up pretty badly. In the latter case, a gateway or destination can become congested even though no single source caused the problem. Either way, the problem is basically akin to a freeway bottleneck—too much traffic for too small a capacity. It's not usually one car that's the problem; it's just that there are way too many cars on that freeway at once!

But what actually happens when a machine receives a flood of datagrams too quickly for it to process? It stores them in a memory section called a *buffer*. Sounds great; it's just that this buffering action can solve the problem only if the datagrams are part of a small burst. If the datagram deluge continues, eventually exhausting the device's memory, its flood capacity will be exceeded and it will dump any and all additional datagrams it receives just like an inundated overflowing bucket!

Flow Control

Since floods and losing data can both be tragic, we have a fail-safe solution in place known as *flow control*. Its job is to ensure data integrity at the Transport layer by allowing applications to request reliable data transport between systems. Flow control prevents a sending host on one side of the connection from overflowing the buffers in the receiving host. Reliable data transport employs a connection-oriented communications session between systems, and the protocols involved ensure that the following will be achieved:

1. The segments delivered are acknowledged back to the sender upon their reception.
2. Any segments not acknowledged are retransmitted.
3. Segments are sequenced back into their proper order upon arrival at their destination.
4. A manageable data flow is maintained in order to avoid congestion, overloading, or worse, data loss.


The purpose of flow control is to provide a way for the receiving device to control the amount of data sent by the sender.

Because of the transport function, network flood control systems really work well. Instead of dumping and losing data, the Transport layer can issue a "not ready" indicator to the sender, or potential source of the flood. This mechanism works kind of like a stoplight, signaling the sending device to stop transmitting segment traffic to its overwhelmed peer. After the peer receiver processes the segments already in its memory reservoir—its buffer—it sends out a "ready" transport indicator. When the machine waiting to transmit the rest of its datagrams receives this "go" indicator, it resumes its transmission. The process is pictured in Figure 1.11.

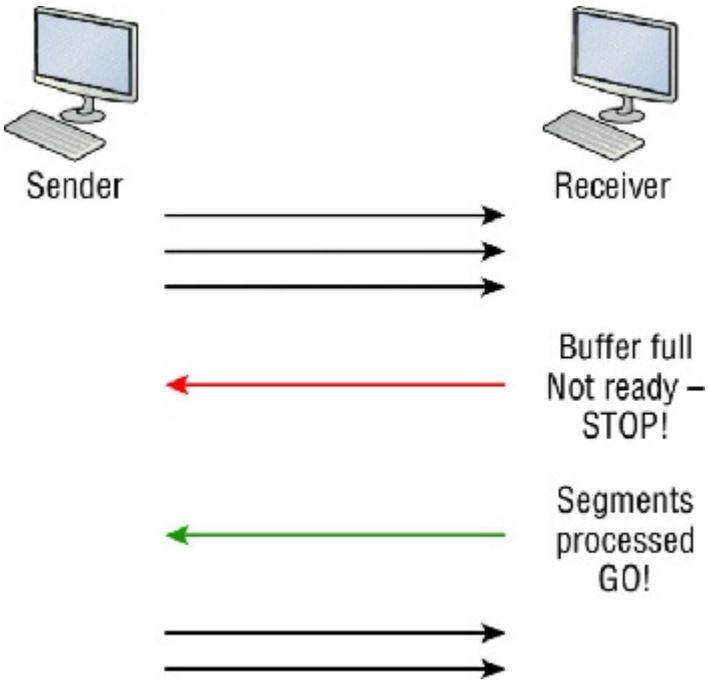


FIGURE 1.11 Transmitting segments with flow control

In a reliable, connection-oriented data transfer, datagrams are delivered to the receiving host hopefully in the same sequence they' re transmitted. A failure will occur if any data segments are lost, duplicated, or damaged along the way—a problem solved by having the receiving host acknowledge that it has received each and every data egment.

A service is considered connection-oriented if it has the following characteristics:

1. A virtual circuit, or "three-way handshake," is set up.
2. It uses sequencing.
3. It uses acknowledgments.
4. It uses flow control.


The types of flow control are buffering, windowing, and congestion avoidance.

Windowing

Ideally, data throughput happens quickly and efficiently. And as you can imagine, it would be painfully slow if the transmitting machine had to actually wait for an acknowledgment after sending each and every segment! The quantity of data segments, measured in bytes, that the transmitting machine is allowed to send without receiving an acknowledgment is called a *window*.


Windows are used to control the amount of outstanding, unacknowledged data segments.

The size of the window controls how much information is transferred from one end to the other before an acknowledgement is required. While some protocols quantify information depending on the number of packets, TCP/IP measures it by counting the number of bytes.

As you can see in Figure 1.12, there are two window sizes—one set to 1 and one set to 3.

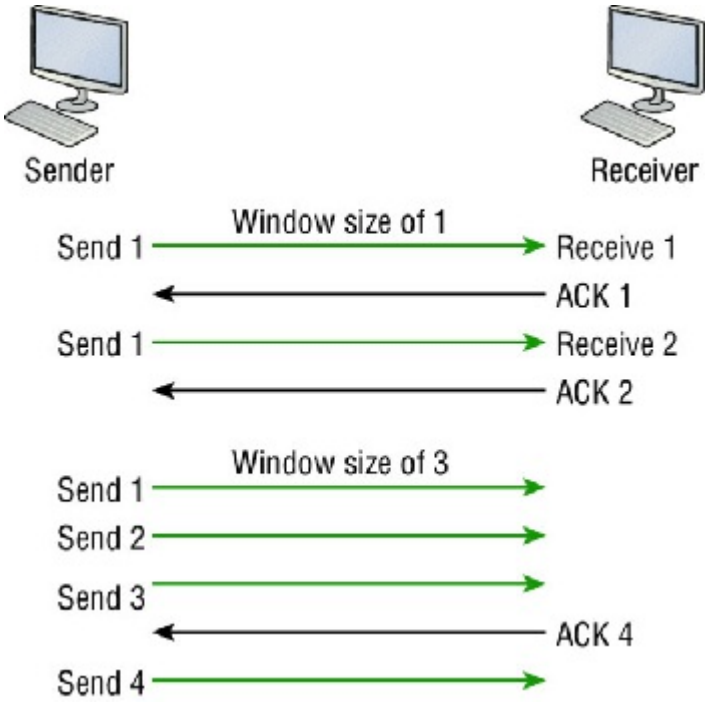


FIGURE 1.12 Windowing

If you've configured a window size of 1, the sending machine will wait for an acknowledgment for each data egme nt it transmits before transmitting another one but will allow three to be transmitted before receiving an acknowledgement if the window size is set to 3.

In this simplified example, both the sending and receiving machines a re workstations. Remember that in reality, the transmission isn't based on simple numbers but in the amount of bytes that can be sent!

If a receiving host fails to receive all the bytes that it should acknowledge, the host can improve the communication session by decreasing the window size.

Acknowledgments

Reliable data delivery ensures the integrity of a stream of data sent from one machine to the other through a fully functional data link. It guarantees that the data won't be duplicated or lost. This is achieved through something called *positive acknowledgment with retransmission*—a technique that requires a receiving machine to communicate with the transmitting source by sending an acknowledgment message back to the sender when it receives data. The sender documents each segment measured in bytes, then sends and waits for this acknowledgment before sending the next segment. Also important is that when it sends a segment, the transmitting machine starts a timer and will retransmit if it expires before it gets an acknowledgment back from the receiving end. Figure 1.13 shows the process I just described.

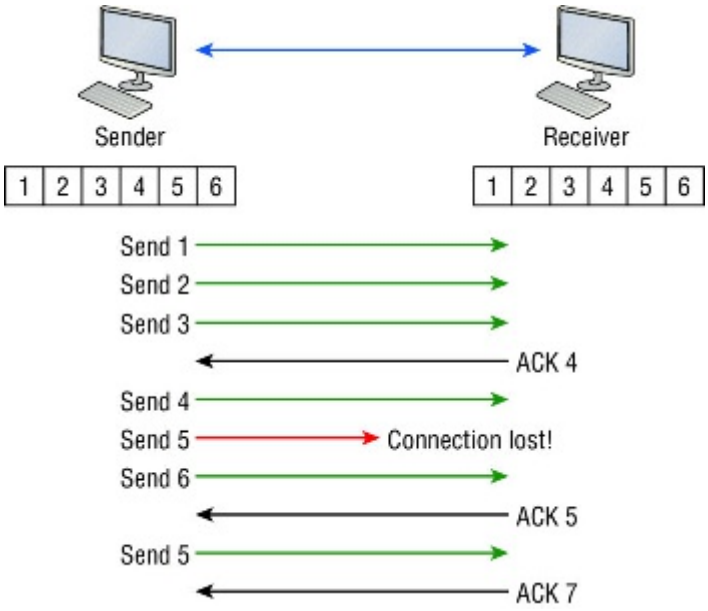


FIGURE 1.13 Transport layer reliable delivery

In the figure, the sending machine transmits segments 1, 2, and 3. The receiving node acknowledges that it has received t hem by requesting segment 4 (what it is expecting next). When it receives the acknowledgment, the sender then transmits segments 4, 5, and 6. If segment 5 doesn't make it to the destination, the receiving node acknowledges that event with a request for the segm ent to be re-sent. The sending machine will then resend the lost segment and wait for an acknowledgment, which it must receive in order to move on to the transmission of segment 7.

The Transport layer, working in tandem with the Session layer, also separates the data from different applications, an activity known as *session multiplexing*, and it happens when a client connects to a server with multiple browser sessions open. This is exactly what's taking place when you go someplace online like Amazon and click multiple links, opening them simultaneously to get information when comparison shopping. The client data from each browser session must be separate when the server application receives it, which is pretty slick technologically speaking, and it's the Transport layer to the rescue for that juggling act!

The Network Layer

The *Network layer*, or layer 3, manages device addressing, tracks the location of devices on the network, and determines the best way to move data. This means that it's up to the Network layer to transport traffic between devices that aren't locally attached. Routers, which are layer 3 devices, are specified at this layer and provide the routing services within an internetwork.

Here's how that works: first, when a packet is received on a router interface, the destination IP address is checked. If the packet isn't destined for that particular router, it will look up the destination network address in the routing table. Once the router chooses an exit interface, the packet will be sent to that interface to be framed and sent out on the local network. If the router can't find an entry for the packet's destination network in the routing table, the router drops the packet.

Data and route update packets are the two types of packets used at the Network layer:

Data Packets These are used to transport user data through the internetwork. Protocols used to support data traffic are called routed protocols, and IP and IPv6 are key examples. I'll cover IP addressing in Chapter 3, "Introduction to TCP/IP," and Chapter 4, "Easy Subnetting," and I'll cover IPv6 in Chapter 14, "Internet Protocol Version 6 (IPv6)."

Route Update Packets These packets are used to update neighboring routers about the networks connected to all routers within the internetwork. Protocols that send route update packets are called routing protocols; the most critical ones for CCNA are RIPv2, EIGRP, and OSPF. Route update packets are used to help build and maintain routing tables.

Figure 1.14 shows an example of a routing table. The routing table each router keeps and refers to includes the following information:

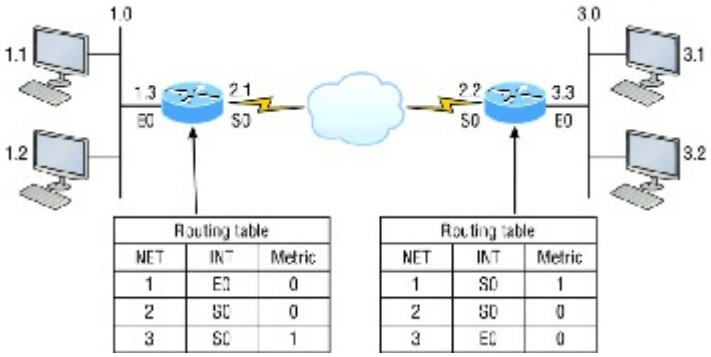


FIGURE 1.14 Routing table used in a router

Network Addresses Protocol-specific network addresses. A router must maintain a routing table for individual routing protocols because each routed protocol keeps track of a network with a different addressing scheme. For example, the routing tables for IP and IPv6 are completely different, so the router keeps a table for each one. Think of it as a street sign in each of the different languages spoken by the A merican, Spanish, and French people living on a street; the street sign would read Cat/Gato/Chat.

Interface The exit interface a packet will take when destined for a specific network.

Metric The distance to the remote network. Different routing protocols use different ways of computing this distance. I'm going to cover routing protocols thoroughly in Chapter 9, "IP Routing." For now, know that some routing protocols like the Routing Information Protocol, or RIP, use hop count, which refers to the number of routers a packet passes through en route to a remote network. Others use bandwidth, delay of the line, or even tick count (1/18 of a second) to determine the best path for data to get to a given destination.

And as I mentioned earlier, routers break up broadcast domains, which means that by default, broadcasts aren't forwarded through a router. Do you remember why this is a good thing? Routers also break up collision domains, but you can also do that using layer 2 (Data Link layer) switches. Because each interface in a router represents a separate network, it must be assigned unique network identification numbers, and each host on the network connected to that router must use the same network number. Figure 1.15 shows how a router works in an internetwork.

FIGURE 1.15 A router in an internetwork. Each router LAN interface is a broadcast domain. Routers break up broadcast domains by default and provide WAN services.

Here are some router characteristics t hat you should never forget:

1. Routers, by default, will not forward any broadcast or multicast packets.
2. Routers use the logical address in a Network layer header to determine the next-hop router to forward the packet to.
3. Routers can use access lists, created by an administrator, to control security based on the types of packets allowed to enter or exit an interface.
4. Routers can provide layer 2 bridging functions if needed and can simultaneously route through the same interface.
5. Layer 3 devices—in this case, routers—provide connections between *virtual LANs (VLANs)*.
6. Routers can provide *quality of service (QoS)* for specific types of network traffic.

The Data Link Layer

The *Data Link layer* provides for the physical transmission of data and handles error notification, network topology, and flow control. This means that the Data Link layer will ensure that messages are delivered to the proper device on a LAN using hardware addresses and will translate messages from the Network layer into bits for the Physical layer to transmit.

The Data Link layer formats the messages, each called a *data frame*, and adds a customized header containing the hardware destination and source address. This added information forms a sort of capsule that surrounds the

original message in much the same way that engines, navigational devices, and other tools were attached to the lunar modules of the Apollo project. These various pieces of equipment were useful only during certain stages of space flight and were stripped off the module and discarded when their designated stage was completed. The process of data traveling through networks is similar.

Figure 1.16 shows the Data Link layer with the Ethernet and IEEE specifications. When you check it out, notice that the IEEE 802.2 standard is used in conjunction with and adds functionality to the other IEEE standards. (You'll read more about the important IEEE 802 standards used with the Cisco objectives in Chapter 2, "Ethernet Networking and Data Encapsulation.")

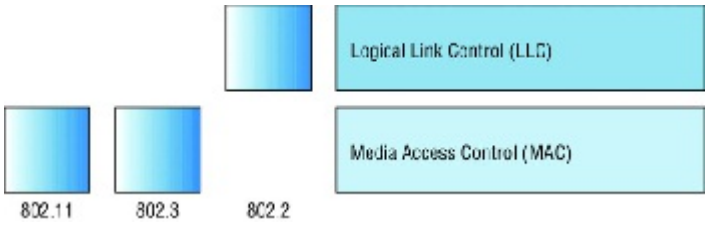


FIGURE 1.16 Data Link layer

It's important for you to understand that routers, which work at the Network layer, don't care at all about where a particular host is located. They're only concerned about where networks are located and the best way to reach them—including remote ones. Routers are totally obsessive when it comes to networks, which in this case is a good thing! It's the Data Link layer that's responsible for the actual unique identification of each device that resi des on a local network.

For a host to send packets to individual hosts on a local network as well as transmit packets between routers, the Data Link layer uses hardware addressing. Each time a packet is sent between routers, it's framed with control information at the Data Link layer, but that information is stripped off at the receiving router and only the original packet is left completely intact. This framing of the packet continues for each hop until the packet is finally delivered to the correct receiving host. It's really important to understand that the packet itself is never altered along the route; it's only encapsulated with the type of control information required for it to be properly passed on to the different media types.

The IEEE Ethernet Data Link layer has two sublayers:

Media Access Control (MAC) Defines how packets are placed on the media. Contention for media access is "first come/first served" access where everyone shares the same bandwidth—hence the name. Physical addressing is defined here as well as logical topologies. What's a logical topology? It's the signal path through a physical topology. Line discipline, error notification (but not correction), the ordered delivery of frames, and optional flow control can also be used at this sublayer.

Logical Link Control (LLC) Responsible for identifying Network layer protocols and then encapsulating them. An LLC header tells the Data Link layer what to do with a packet once a frame is received. It works like this: a host receives a frame and looks in the LLC header to find out where the packet is destined—for instance, the IP protocol at the Network layer. The LLC can also provide flow control and sequencing of control bits.

The switches and bridges I talked about near the beginning of the chapter both work at the Data Link layer and filter the network using hardware (MAC) addresses. I'll talk about these next.

As data is encoded with control information at each layer of the OSI model, the data is named with something called a protocol data unit (PDU). At the Transport layer, the PDU is called a segment, at the Network layer it's a packet, at the Data Link a frame, and at the Physical layer it's called bits. This method of naming the data at each layer is covered thoroughly in Chapter 2.

Switches and Bridges at the Data Link Layer

Layer 2 switching is considered hardware-based bridging because it uses specialized hardware called an *application-specific integrated circuit (ASIC)*. ASICs can run up to high gigabit speeds with very low latency rates.

Latency is the time measured from when a frame enters a port to when it exits a port.

Bridges and switches read each frame as it passes through the network. The layer 2 device then puts the source hardware address in a filter table and keeps track of which port the frame was received on. This information (logged in the bridge's or switch's filter table) is what helps the machine determine the location of the specific sending device. Figure 1.17 shows a switch in an internetwork and how John is sending packets to the Internet and Sally doesn't hear his frames because she is in a different collision domain. The destination frame goes directly to the default gateway router, and Sally doesn't see John's traffic, much to her relief.

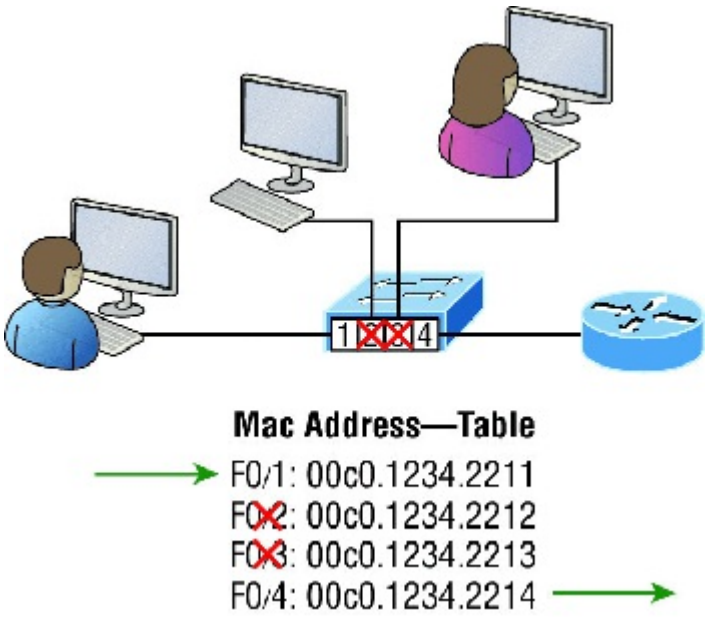


FIGURE 1.17 A switch in an in ternetwork

The real estate business is all about location, location, location, and it's the same way for both layer 2 and layer 3 devices. Though both need to be able to negotiate the network, it's crucial to remember that they're concerned with very different parts of it. Primarily, layer 3 machines (such as routers) need to locate specific networks, whereas layer 2 machines (switches and bridges) need to eventually locate specific devices. So, networks are to routers as individual devices a re to switches and bridges. And routing tables that "map" the internetwork are for routers as filter tables that "map" individual devices are for switches and bridges.

After a filter table is built on the layer 2 device, it will forward frames only to the segment where the destination hardware address is located. If the destination device is on the same segment as the frame, the layer 2 device will block the frame from going to any other segments. If the destination is on a different segment, the frame can be transmitted only to that segment. This is called *transparent bridging*.

When a switch interface receives a frame with a destination hardware address that isn't found in the device's filter table, it will forward the frame to all connected segments. If the unknown device that was sent the "mystery frame" replies to this forwarding action, the switch updates its filter table regarding that device's location. But in the event the destination address of the transmitting frame is a broadcast address, the switch will forward all broadcasts to every connected segment by default.

All devices that the broadcast is forwarded to are considered to be in the same broadcast domain. This can be a problem because layer 2 devices propagate layer 2 broadcast storms that can seriously choke performance, and the only way to stop a broadcast storm from propagating through an internetwork is with a layer 3 device—a router!

The biggest benefit of using switches instead of hubs in your internetwork is that each switch port is actually its own collision domain. Remember that a hub creates one large collision domain, which is not a good thing! But even armed with a switch, you still don't get to just break up broadcast domains by default because neither switches nor bridges will do that. They'll simply forward all broadcasts instead.

Another benefit of LAN switching over hub-centered implementations is that each device on every segment plugged into a switch can transmit simultaneously. Well, at least they can as long as there's only one host on each port and there isn't a hub plugged into a switch port! As you might have guessed, this is because hubs allow only one device per network segment to communicate at a time.

The Physical Layer

Finally arriving at the bottom, we find that the *Physical layer* does two things: it sends bits and receives bits. Bits

come only in values of 1 or 0—a Morse code with numerical values. The Physical layer communicates directly with the various types of actual communication media. Different kinds of media represent these bit values in different ways. Some use audio tones, while others employ *state transitions*—changes in voltage from high to low and low to high. Specific protocols are needed for each type of media to describe the proper bit patterns to be used, how data is encoded into media signals, and the various qualities of the physical media's attachment interface.

The Physical layer specifies the electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating a physical link between end systems. This layer is also where you identify the interface between the *data terminal equipment (DTE)* and the *data communication equipment (DCE)*. (Some old phone-company employees still call DCE "data circuit-terminating equipment.") The DCE is usually located at the service provider, while the DTE is the attached device. The services available to the DTE are most often accessed via a modem or *channel service unit/data service unit (CSU/DSU)*.

The Physical layer's connectors and different physical topologies are defined by the OSI as standards, allowing disparate systems to communicate. The Cisco exam objectives are interested only in the IEEE Ethernet standards.

Hubs at the Physical Layer

A hub is really a multiple-port repeater. A repeater receives a digital signal, reamplifies or regenerates that signal, then forwards the signal out the other port without looking at any data. A hub does the same thing across all active ports: any digital signal received from a segment on a hub port is regenerated or reamplified and transmitted out all other ports on the hub. This means all devices plugged into a hub are in the same collision domain as well as in the same broadcast domain. Figure 1.18 shows a hub in a network and how when one host transmits, all other hosts must stop and listen.

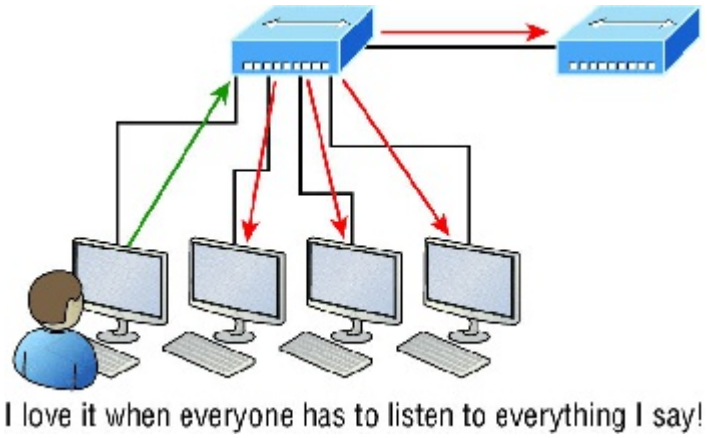


FIGURE 1.18 A hub in a network

Hubs, like repeaters, don't examine any of the traffic as it enters or before it's transmitted out to the other parts of the physical media. And every device connected to the hub, or hubs, must listen if a device transmi ts. A physical star network, where the hub is a central device and cables extend in all directions out from it, is the type of topology a hub creates. Visually, the design really does resemble a star, whereas Ethernet networks run a logical bus topology, meaning that the signal has to run through the network from end to end.

Hubs and repeaters can be used to enlarge the area covered by a single LAN segment, but I really do not recommend going with this configuration! LAN switches are affordable for almost every situation and will make you much happier.

Topologies at the Physical layer

One last thing I want to discuss at the Physical layer is topologies, both physical and logical. Understand that every type of network has both a physical and a logical topology.

1. The physical topology of a network refers to the physical layout of the devices, but mostly the cabling and cabling layout.
2. The logical topology defines the logical path on which the signal will travel on the physical topology.

Figure 1.19 shows the four types of topologies.

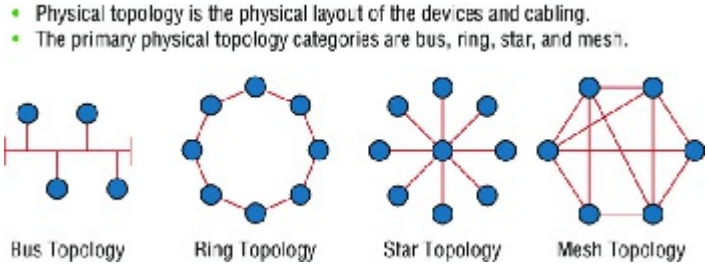


FIGURE 1.19 Physical vs. Logical Topolgies

Here are the topology types, although the most common, and pretty much the only network we use today is a physical star, logical bus technology, which is considered a hybrid topology (think Ethernet):

1. Bus: In a bus topology, every workstation is connected to a single cable, meaning every host is directly connected to every other workstation in the network.
2. Rin g: In a ring topology, computers and other network devices are cabled together in a way that the last device is connected to the first to form a circle or ring.
3. Star: The most common physical topology is a star topology, which is your Ethernet switching physical layout. A central cabling device (switch) connects the computers and other network devices together. This category includes star and extended star topologies. Physical connection is commonly made using twisted-pair wiring.
4. Mesh: In a mesh topology, every network device is cabled together with connection to each other. Redundant links increase reliability and self-healing. The physical connection is commonly made using fiber or twisted-pair wiring.
5. Hybrid: Ethernet uses a physical star layout (cables come from all directions), and the signal travels end-to-end, like a bus route.

Summary

Whew! I know this seemed like the chapter that wouldn't end, but it did—and you made it through! You're now armed with a ton of fundamental information; you're ready to build upon it and are well on your way to certification.

I started by discussing simple, basic networking and the differences between collision and broadcast domains.

I then discussed the OSI model—the seven-layer model used to help application developers design applications that can run on any type of syst em or network. Each layer has its special jobs and select responsibilities within the model to ensure that solid, effective communications do, in fact, occur. I provided you with complete details of each layer and discussed how Cisco views the specifications of the OSI model.

In addition, each layer in the OSI model specifies different types of devices, and I described the different devices used at each layer.

Remember that hubs are Physical layer devices and repeat the digital signal to all segments except the one from which it was received. Switches segment the network using hardware addresses and break up collision domains. Routers break up broadcast domains as well as collision domains and use logical addressing to send packets through an internetwork.

Exam Essentials

Identify the possible causes of LAN traffic congestion. Too many hosts in a broadcast domain, broadcast storms, multicasting, and low bandwidth are all possible causes of LAN traffic congestion.

Describe the difference between a collision domain and a broadcast domain. *Collision domain* is an Ethernet term used to describe a network collection of devices in which one particular device sends a packet on a network segment, forcing every other device on that same segment to pay attention to it. With a broadcast domain, a set of all devices on a network hears all broadcasts sent on all segments.

Differentiate a MAC address and an IP address and describe how and when each address type is used in a network. A MAC address is a hexadecimal number identifying the physical connection of a host. MAC addresses are said to operate on layer 2 of the OSI model. IP addresses, which can be expressed in binary or decimal format, are logical identifiers that are said to be on layer 3 of the OSI model. Hosts on the same physical

segment locate one another with MAC addresses, while IP addresses are used when they reside on different LAN segments or subnets.

Understand the difference between a hub, a bridge, a switch, and a router. A hub creates one collision domain and one broadcast domain. A bridge breaks up collision domains but creates one large broadcast domain. They use hardware addresses to filter the network. Switches are really just multiple-port bridges with more intelligence; they break up collision domains but create one large broadcast domain by default. Bridges and switches use hardware addresses to filter the network. Routers break up broadcast domains (and collision domains) and use logical addressing to filter the network.

Identify the functions and advantages of routers. Routers perform packet switching, filtering, and path selection, and they facilitate internetwork communication. One advantage of routers is that they reduce broadcast traffic.

Differentiate connection-oriented and connectionless network services and describe how each is handled during network communications. Connection-oriented services use acknowledgments and flow control to create a reliable session. More overhead is used than in a connectionless network service. Connectionless services are used to send data with no acknowledgments or flow control. This is considered unreliable.

Define the OSI layers, understand the function of each, and describe how devices and networking protocols can be mapped to each layer. You must remember the seven layers of the OSI model and what function each layer provides. The Application, Presentation, and Session layers are upper layers and are responsible for communicating from a user interface to an application. The Transport layer provides segmentation, sequencing, and virtual circuits. The Network layer provides logical network addressing and routing through an internetwork. The Data Link layer provides framing and placing of data on the network medium. The Physical layer is responsible for taking 1s and 0s and encoding them into a digital signal for transmission on the network segment.

Written Labs

In this section, you'll complete the following labs to make sure you've got the information and concepts contained within them fully dialed in:

1. Lab 1.1: OSI Questions
2. Lab 1.2: Defining the OSI Layers and Devices
3. Lab 1.3: Identifying Collision and Broadcast Domains

You can find the answers to these labs in Appendix A, "Answers to Written Labs."

Written Lab 1.1: OSI Questions

Answer the following questions about the OSI model:

1. Which layer chooses and determines the availability of communicating partners along with the resources necessary to make the connection, coordinates partnering applications, and forms a consensus on procedures for controlling data integrity and error recovery?
2. Which layer is responsible for converting data packets from the Data Link layer into electrical signals?
3. At which layer is routing implemented, enabling connections and path selection between two end systems?
4. Which layer defines how data is formatted, presented, encoded, and converted for use on the network?
5. Which layer is responsible for creating, managing, and terminating sessions between applications?
6. Which layer ensures the trustworthy transmission of data across a physical link and is primarily concerned with physical addressing, line discipline, network topology, error notification, ordered delivery of frames, and flow control?
7. Which layer is used for reliable communication between end nodes over the network and provides mechanisms for establishing, maintaining, and terminating virtual circuits; transport-fault detection and recovery; and controlling the flow of information?
8. Which layer provides logical addressing that routers will use for path determination?
9. Which layer specifies voltage, wire speed, and cable pinouts and moves bits between devices?
10. Which layer combines bits into bytes and bytes into frames, uses MAC addressing, and provides error detection?
11. Which layer is responsible for keeping the data from different applications separate on the network?
12. Which layer is represented by frames?
13. Which layer is represented by segments?
14. Which layer is represented by packets?
15. Which layer is represented by bits?
16. Rearrange the following in order of encapsulation:
    1. Packets
    2. Frames

3. Bits
4. Segments

17. Which layer segments and reassembles data into a data stream?
18. Which layer provides the physical transmission of the data and handles error notification, network topology, and flow control?
19. Which layer manages logical device addressing, tracks the location of devices on the internetwork, and determines the best way to move data?
20. What is the bit length and expression form of a MAC address?

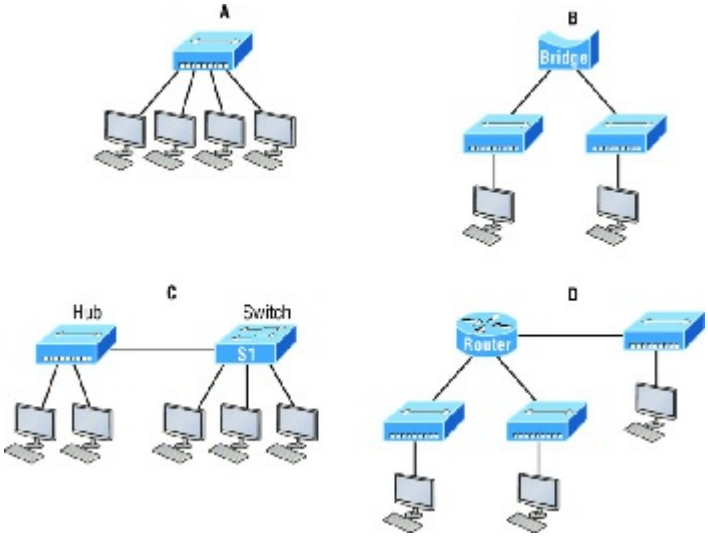
Written Lab 1.2: Defining the OSI Layers and Devices

Fill in the blanks with the appropriate layer of the OSI or hub, switch, or router device.

Written Lab 1.3: Identifying Collision and Broadcast Domains

1. In the following exhibit, identify the number of collision domains and broadcast domains in each specified device. Each device is represented by a letter:

    1. Hub
    2. Bridge
    3. Switch
    4. Router

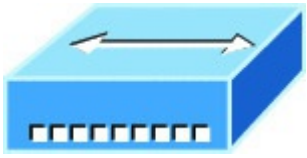


Review Questions

The following questions are designed to test your understanding of this chapter's material. For more information on how to get additional questions, please see www.lammle.com/ccna.

You can find the answers to these questions in Appendix B, "Answers to Review Questions."

1. Which of the following statements is/are true with regard to the device shown here? (Choose all that apply.)

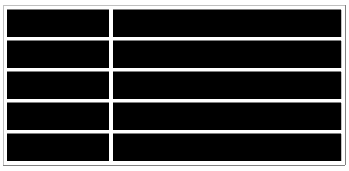


    1. It includes one collision domain and one broadcast domain.
    2. It includes 10 collision domains and 10 broadcast domains.
    3. It includes 10 collision domains and one broadcast domain.
    4. It includes one collision domain and 10 broadcast domains.
2. With respect to the OSI model, which one of the following is the correct statement about PDUs?
    1. A segment contains IP addresses.
    2. A packet contains IP addresses.
    3. A segment contains MAC addresses.
    4. A packet contains MAC addresses.
3. You are the Cisco administrator for your company. A new branch office is opening and you are selecting the necessary hardware to support the network. There will be two groups of computers, each organized by department. The Sales group computers will be assigned IP addresses ranging from 192.168.1.2 to 192.168.1.50. The Accounting group will be assigned IP addresses ranging from 10.0.0.2 to 10.0.0.50. What type of device should you select to connect the two groups of computers so that data communication can occur?
    1. Hub
    2. Switch
    3. Router
    4. Bridge
4. The most effective way to mitigate congestion on a LAN would be to _____.
    1. Upgrade the network cards
    2. Change the cabling to CAT 6
    3. Replace the hubs with switches
    4. Upgrade the CPUs in the routers
5. In the following work area, draw a line from the OSI model layer to its PDU.

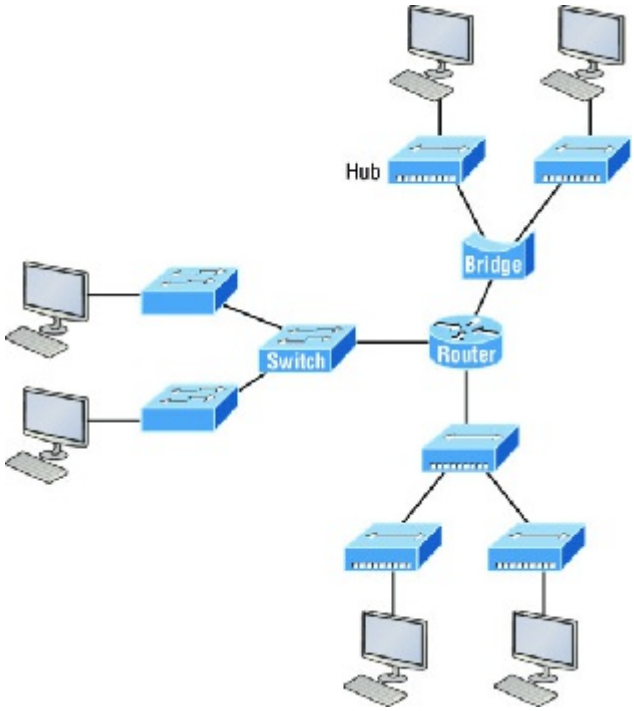
Layer	Description
Transport	Bits
Data Link	Segment
Physical	Packet
Network	Frame

6. What is a function of the WLAN Controller?
    1. To monitor and control the incoming and outgoing network traffic
    2. To automatically handle the configuration of wireless access points
    3. To allow wireless devices to connect to a wired network
    4. To connect networks and intelligently choose the best paths between networks
7. You need to provide network connectivity to 150 client computers that will reside in the same subnetwork, and each client computer must be allocated dedicated bandwidth. Which device should you use to accomplish the task?
    1. Hub
    2. Switch
    3. Router
    4. Bridge
8. In the following work area, draw a line from the OSI model layer definition on the left to its description on

the right.



9. What is the function of a firewall?
    1. To automatically handle the configuration of wireless access points
    2. To allow wireless devices to connect to a wired network
    3. To monitor and control the incoming and outgoing network traffic
    4. To connect networks and intelligently choose the best paths between networks
10. Which layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see whether enough resources exist for that communication?
    1. Transport
    2. Network
    3. Presentation
    4. Application
11. Which of the following correctly describe steps in the OSI data encapsulation process? (Choose two.)
    1. The Transport layer divides a data stream into segments and may add reliability and flow control information.
    2. The Data Link layer adds physical source and destination addresses and an FCS to the segment.
    3. Packets are created when the Network layer encapsulates a frame with source and destination host addresses and protocol-related control information.
    4. Packets are created when the Network layer adds layer 3 addresses and control information to a segment.
    5. The Presentation layer translates bits into voltages for transmission across the physical link.
12. Which of the following layers of the OSI model was later subdivided into two layers?
    1. Presentation
    2. Transport
    3. Data Link
    4. Physical
13. What is a function of an access point (AP)?
    1. To monitor and control the incoming and outgoing network traffic
    2. To automatically handle the configuration of wireless access point
    3. To allow wireless devices to connect to a wired network
    4. To connect networks and intelligently choose the best paths between networks
14. A_____is an example of a device that operates only at the physical layer.
    1. Hub
    2. Switch
    3. Router
    4. Bridge
15. Which of the following is *not* a benefit of using a reference model?
    1. It divides the network communication process into smaller and simpler components.
    2. It encourages industry standardization.
    3. It enforces consistency across vendors.
    4. It allows various types of network hardware and software to communicate.
16. Which of the following statements is not true with regard to routers?
    1. They forward broadcasts by default.
    2. They can filter the network based on Network layer information.
    3. They perform path selection.
    4. They perform packet switching.
17. Switches break up_____domains, and routers break up_____domains.
    1. broadcast, broadcast
    2. collision, collision
    3. collision, broadcast
    4. broadcast, collision
18. How many collision domains are present in the following diagram?



1. 8
2. 9
3. 10
4. 11

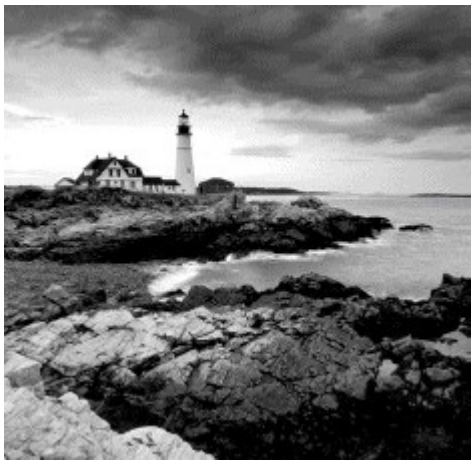
19. Which of the following layers of the OSI model is not involved in defining how the applications within the end stations will communicate with each other as well as with users?
    1. Transport
    2. Application
    3. Presentation
    4. Session
20. Which of the following is the *only* device that operates at all layers of the OSI model?

    1. Network host
    2. Switch
    3. Router
    4. Bridge

Chapter 2
Ethernet Networking and Data Encapsulation

THE FOLLOWING ICND1 EXAM TOPICS ARE COVERED IN THIS CHAPTER:

1. ✓ **Network Fundamentals**
   1.
      - 1.6 Select the appropriate cabling type based on implementation requirements
   2. - 1.4 Compare and contrast collapsed core and three-tier architectures
2. ✓ **LAN Switching Technologies**
   1. - 2.2 Interpret Ethernet frame format



Before we begin exploring a set of key foundational topics like the TCP/IP DoD model, IP addressing, subnetting, and routing in the upcoming chapters, I really want you to grasp the big picture of LANs conceptually. The role Ethernet plays in today's networks as well as what Media Access Control (MAC) addresses are and how they are used are two more critical networking basics you'll want a solid understanding of as well.

We'll cover these important subjects and more in this chapter, beginning with Ethernet basics and the way MAC addresses are used on an Ethernet LAN, and then we'll focus in on the actual protocols used with Ethernet at the Data Link layer. To round out this discussion, you'll also learn about some very important Ethernet specifications.

You know by now that there are a whole bunch of different devices specified at the various layers of the OSI model and that it's essential to be really familiar with the many types of cables and connectors employed to hook them up to the network correctly. I'll review the types of cabling used with Cisco devices in this chapter, demonstrate how to connect to a router or switch, plus show you how to connect a router or switch via a console connection.

I'll also introduce you to a vital process of encoding data as it makes its way down the OSI stack, known as encapsulation.

I'm not nagging at all here—okay, maybe just a little, but promise that you'll actually work through the four written labs and 20 review questions I added to the end of this chapter just for you. You'll be so happy you did because they're written strategically to make sure all the important material covered in this chapter gets locked in, vault-tight into your memory. So don't skip them!

To find up-to-the-minute updates for this chapter, please see www.lammle.com/ccna or the book's web page via www.sybex.com/go/ccna.

Ethernet Networks in Review

Ethernet is a contention-based media access method that allows all hosts on a network to share the same link's bandwidth. Some reasons it's so popular are that Ethernet is really pretty simple to implement and it makes troubleshooting fairly straightforward as well. Ethernet is also readily scalable, meaning that it eases the process of

integrating new technologies into an existing network infrastructure, like upgrading from Fast Ethernet to Gigabit Ethernet.

Ethernet uses both Data Link and Physical layer specifications, so you'll be presented with info rmation relative to both layers, which you'll need to effectively implement, troubleshoot, and maintain an Ethernet network.

Collision Domain

In Chapter 1, "Internetworking," you learned that the Ethernet term *collision domain* refers to a network scenario wherein one device sends a frame out on a physical network segment forcing every other device on the same segment to pay attention to it. This is bad because if two devices on a single physical segment just happen to transmit simultaneously, it will cause a collision and require these devices to retransmit. Think of a collision event as a situation where each device's digital signals totally interfere with one another on the wire. Figure 2.1 shows an old, legacy network that's a single collision domain where only one host can transmit at a time.

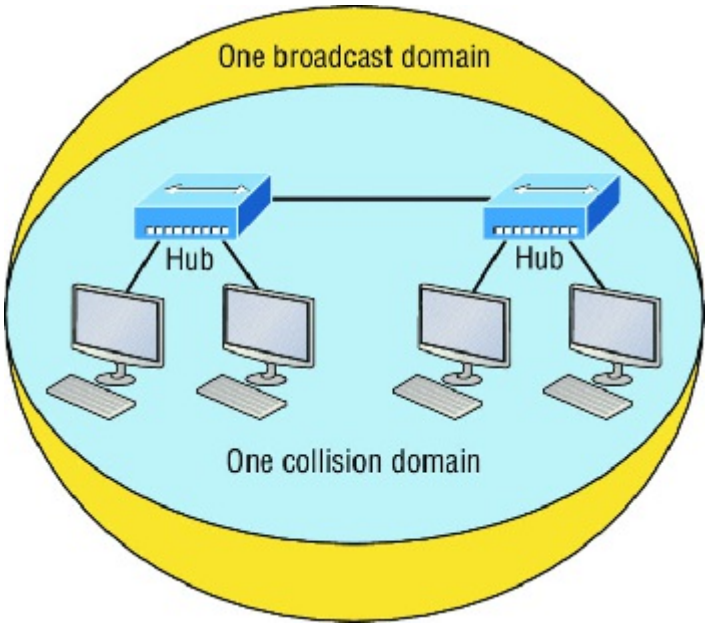


FIGURE 2.1 Legacy collision domain design

The hosts connected to each hub are in the same collision domain, so if one of them transmits, all the others must take the time to listen for and read the digital signal. It is easy to see how collisions can be a serious drag on network performance, so I'll show you how t o strategically avoid them soon!

Okay—take another look at the network pictured in Figure 2.1. True, it has only one collision domain, but worse, it's also a single broadcast domain—wh at a mess! Let's check out an example, in Figure 2.2, of a typical network design still used today and see if it's any better.

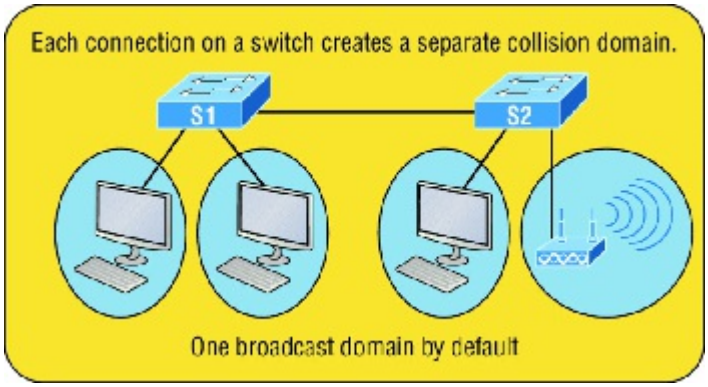


FIGURE 2.2 A typical network you'd see today

Because each port off a switch is a single collision domain, we gain more bandwidth for users, which is a great

start. But switches don't break up broadcast domains by default, so this is still only one broadcast domain, which is not so good. This can work in a really small network , but to expand it at all, we would need to break up the network into smaller broadcast domains or our users won't get enough bandwidth! And you're probably wondering about that device in the lower-right corner, right? Well, that's a *wireless access point*, which is sometimes referred as an AP (which stands for access point). It's a wireless device that allows hosts to connect wirelessly using the IEEE 802.11 specification and I added it to the figure to demonstrate how these devices can be used to extend a collision domain. But still, understand that APs don't actually segment the network, they only extend them, meaning our LAN just got a lot bigger, with an unknown amount of hosts that are all still part of one measly broadcast domain! This clearly demonstrates why it's so important to understand exactly what a broadcast domain is, and now is a great time to talk about them in detail.

Broadcast Domain

Let me start by giving you the formal definition: *broadcast domain* refers to a group of devices on a specific network segment that hear all the broadcasts sent out on that specific network segment.

But even though a broadcast domain is usually a boundary delimited by physical media like switches and routers, the term can also refer to a logical division of a network segment, where all hosts can communicate via a Data Link layer, hardware address broadcast.

Figure 2.3 shows how a router would create a broadcast domain boundary.

Here you can see there are two router interfaces giving us two broadcast domains, and I count 10 switch segments, meaning we've got 10 collision domains.

The design depicted in Figure 2.3 is still in use today, and routers will be around for a long time, but in the latest, modern switched networks, it's important to create small broadcast domains. We achieve this by building virtual LANs (VLANs) within our switched networks, which I'll demo nstrate shortly. Without employing VLANs in today's switched environments, there wouldn't be much bandwidth available to individual users. Switches break up collision domains with each port, which is awesome, but they're still only one broadcast domain by default! It's also one more reason why it's extremely important to design our networks very carefully.

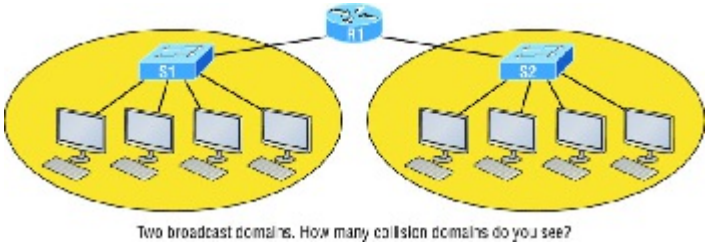


FIGURE 2.3 A router creates broadcast domain boundaries.

And key to carefully planning your network design is never to allow broadcast domains to grow too large and get out of control. Both collision and broadcast domains can easily be controlled with routers and VLANs, so there's just no excuse to allow user bandwidth to slow to a painful crawl when there are plenty of tools in your arsenal to prevent the suffering!

An important reason for this book's existence is to ensure that you really get the foundational basics of Cisco networks nailed down so you can effectively design, implement, configure, troubleshoot, and even dazzle colleagues and superiors with elegant designs that lavish your users with all the bandwidth their hearts could possibly desire.

To make it to the top of that mountain, you need more than just the basic story, so let's move on to explore the collision detection mechanism used in half-duplex Ethernet.

CSMA/CD

Ethernet networking uses a protocol called *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*, which helps devices share the bandwidth evenly while preventing two devices from transmitting simultaneously on the same network medium. CSMA/CD was actually created to overcome the problem of the collisions that occur when packets are transmitted from different nodes at the same time. And trust me—good collision management is crucial, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only switches and routers can effectively prevent a transmission from propagating throughout the entire network!

So, how does the CSMA/CD protocol work? Let's start by taking a look at Figure 2.4.

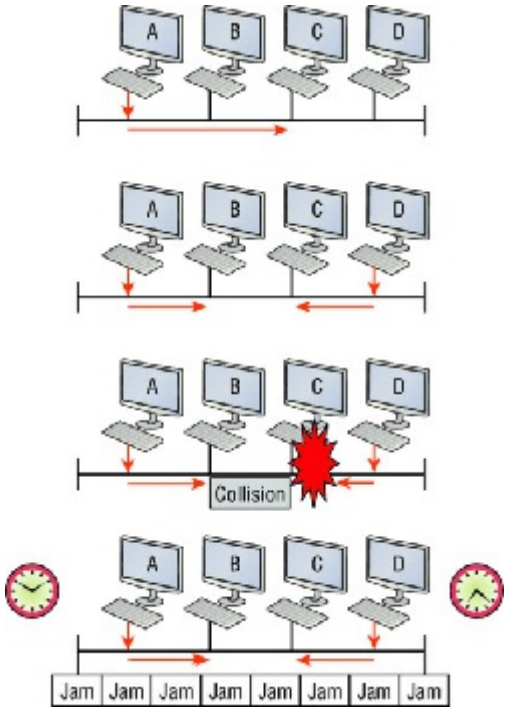


FIGURE 2.4 CSMA/CD

When a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear and no other host is transmitting, the host will then proceed with its transmission.

But it doesn't stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects an other signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data—think busy signal.

The nodes respond to that jam signal by waiting a bit be fore attempting to transmit again. Backoff algorithms determine when the colliding stations can retransmit. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out. Half-duplex can be pretty messy!

When a collision occurs on an Ethernet LAN, the following happens:

1. A jam signal informs all devices that a collision occurred.
2. The collision invokes a random backoff algorithm.
3. Each device on the Ethernet segment stops transmitting for a short time until its backoff timer expires.
4. All hosts have equal priority to transmit after the timers have expired.

The ugly effects of having a CSMA/CD network sustain heavy collisions are delay, low throughput, and congestion.

Backoff on an Ethernet network is the retransmission delay that's enforced when a collision occurs. When that happens, a host will resume transmission only after the forced time delay has expired. Keep in mind that after the backoff has elapsed, all stations have equal priority to transmit data.

At this point, let's take a minute to talk about Ethernet in detail at both the Data Link layer (layer 2) and the Physical layer (layer 1).

Half- and Full-Duplex Ethernet

Half-duplex Ethernet is defined in the original IEEE 802.3 Ethernet specification, which differs a bit from how Cisco describes things. Cisco says Ethernet uses only one wire pair with a digital signal running in both directions on the wire. Even though the IEEE specifications discuss the half-duplex process somewhat differently, it's not actually a full-blown technical disagreement. Cisco is really just talking about a general sense of what's happening with Ethernet.

Half-duplex also uses the CSMA/CD protocol I just discussed to help prevent collisions and to permit retransmitting

if one occurs. If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions. Figure 2.5 shows a network with four hosts connected to a hub.

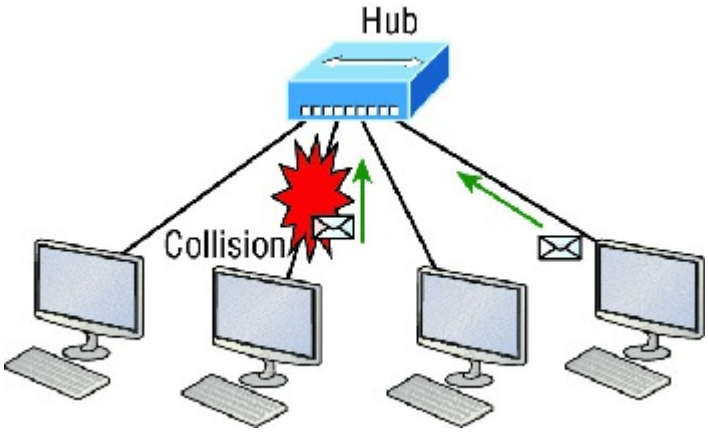


FIGURE 2.5 Half-duplex example

The problem here is that we can only run half-duplex, and if two hosts communicate at the same time there will be a collision. Also, half-duplex Ethernet is only about 30 to 40 percent efficient because a large 100Base-T network will usually only give you 30 to 40 Mbps, at most, due to overhead.

But full-duplex Ethernet uses two pairs of wire s at the same time instead of a single wire pair like half-duplex. And full-duplex uses a point-to-point connection between the transmitter of the transmitting device and the receiver of the receiving device. This means that full-duplex data transfers happen a lot faster when compared to half-duplex transfers. Also, because the transmitted data is sent on a different set of wires than the received data, collisions won't happen. Figure 2.6 shows four hosts connected to a switch, plus a hub. Definitely try not to use hubs if you can help it!

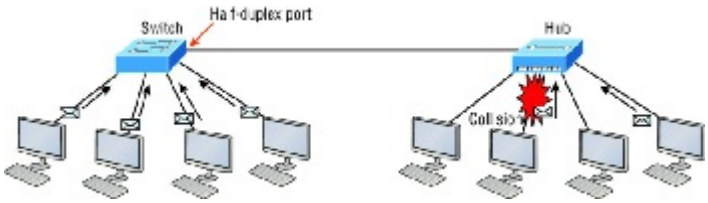


FIGURE 2.6 Full-duplex example

Theoretically all hosts connected to the switch in Figure 2.6 can communicate at the same time because they can run full-duplex. Just keep in mind that the switch port connecting to the hub as well as the hosts connecting to that hub must run at half-duplex.

The reason you don't need to worry about collisions is because now it's like a freeway with multiple lanes instead of the single-lane road provided by half-duplex. Full-duplex Ethernet is supposed to offer 100 percent efficiency in both directions—for example, you can get 20 M bps with a 10 Mbps Ethernet running full-duplex, or 200 Mbps for Fast Ethernet. But this rate is known as an aggregate rate, which translates as "you're supposed to get" 100 percent efficiency. No guarantees, in networking as in life!

You can use full-duplex Ethernet in at least the following six situations:

1. With a connection from a switch to a host
2. With a connection from a switch to a switch
3. With a connection from a host to a host
4. With a connection from a switch to a router
5. With a connection from a router to a router
6. With a connection from a router to a host

Full-duplex Ethernet requires a point-to-point connection when only two nodes are present. You can run full-duplex with just about any device except a hub.

Now this may be a little confusing because this begs the question that if it's capable of all that speed, why wouldn't it actually deliver? Well, when a full-duplex Ethernet port is powered on, it first connects to the remote end and then negotiates with the other end of the Fast Ethernet link. This is called an *auto-detect mechanism*. This mechanism first decides on the exchange capability, which means it checks to see if it can run at 10, 100, or even 1000 Mbps. It then checks to see if it can run full-duplex, and if it can't, it will run half-duplex.

Remember that half-duplex Ethernet shares a collision domain and provides a lower effective throughput than full-duplex Ethernet, which typically has a private per-port collision domain plus a higher effective throughput.

Last, remember these important points:

1. There are no collisions in full-duplex mode.
2. A dedicated switch port is required for each full-duplex node.
3. The host network card and the switch port must be capable of operating in full-duplex mode.
4. The default behavior of 10Base-T and 100Base-T hosts is 10 Mbps half-duplex if the autodetect mechanism fails, so it is always good practice to set the speed and duplex of each port on a switch if you can.

Now let's take a look at how Ethernet works at the Data Link layer.

Ethernet at the Data Link Layer

Ethernet at the Data Link layer is responsible for Ethernet addressing, commonly referred to as MAC or hardware addressing. Ethernet is also responsible for framing packets received from the Network layer and preparing them for transmission on the local network through the Ethernet contention-based media access method.

Ethernet Addressing

Here's where we get into how Ethernet addressing works. It uses the *Media Access Control (MAC)* address burned into each and every Ethernet network interface card (NIC). The MAC, or hardware, address is a 48-bit (6-byte) address written in a hexadecimal format.

Figure 2.7 shows the 48-bit MAC addresses and how the bits are divided.

FIGURE 2.7 Ethernet addressing using MAC addresses

The *organizationally unique identifier (OUI)* is assigned by the IEEE to an organization. It's composed of 24 bits, or 3 bytes, and it in turn assigns a globally administered address also made up of 24 bits, or 3 bytes, that's supposedly unique to each and every adapter an organization manufactures. Surprisingly, there's no guarantee when it comes to that unique claim! Okay, now look closely at the figure. The high-order bit is the Individual/Group (I/G) bit. When it has a value of 0, we can assume that the address is the MAC address of a device and that it may well appear in the source portion of the MAC header. When it's a 1, we can assume that the address represents either a broadcast or multicast address in Ethernet.

The next bit is the Global/Local bit, sometimes called the G/L bit or U/L bit, where *U* means *universal*. When set to 0, this bit represents a globally administered address, as assigned by the IEEE, but when it's a 1, it represents a locally governed and administered address. The low-order 24 bits of an Ethernet address represent a locally administered or manufacturer-assigned code. This portion commonly starts with 24 0s for the first card made and continues in order until there are 24 1s for the last (16,777,216th) card made. You'll find that many manufacturers use these same six hex digits as the last six characters of their serial number on the same card.

Let's stop for a minute and go over some addressing schemes important in the Ethernet world.

Binary to Decimal and Hexadecimal Conversion

Before we get into working with the TCP/IP protocol and IP addressing, which we'll do in Chapter 3, "Introduction to TCP/IP," it's really important for you to truly grasp the differences between binary, decimal, and hexadecimal numbers and how to convert one format into the other.

We'll start with binary numbering, which is really pretty simple. The digits used are limited to either a 1 or a 0, and each digit is called a *bit*, which is short for *binary digit*. Typically, you group either 4 or 8 bits together, with these being referred to as a nibble and a byte, respectively.

The interesting thing about binary numbering is how the value is represented in a decimal format—the typical decimal format being the base-10 number scheme that we've all used since kindergarten. The binary numbers are placed in a value spot, starting at the right and moving left, with each spot having double the value of the previous spot.

Table 2.1 shows the decimal values of each bit location in a nibble and a byte. Remember, a nibble is 4 bits and a byte is 8 bits.

TABLE 2.1 Binary values

What all this means is that if a one digit (1) is placed in a value spot, then the nibble or byte takes on that decimal value and adds it to any other value spots that have a 1. If a zero (0) is placed in a bit spot, you don't count that value.

Let me clarify this a little. If we have a 1 placed in each spot of our nibble, we would then add up 8 + 4 + 2 + 1 to give us a maximum value of 15. Another example for our nibble values would be 1001, meaning that the 8 bit and the 1 bit are turned on, which equals a decimal value of 9. If we have a nibble binary value of 0110, then our decimal value would be 6, because the 4 and 2 bits are turned on.

But the *byte* decimal values can add up to a number that's significantly higher than 15. This is how: If we counted every bit as a one (1), then the byte binary value would look like the following example because, remember, 8 bits equal a byte:

11111111

We would then count up every bit spot because each is turned on. It would look like this, which demonstrates the maximum value of a byte:

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

There are plenty of other decimal values that a binary number can equal. Let's work through a few examples:

10010110

Which bits are on? The 128, 16, 4, and 2 bits are on, so we'll just add them up: 128 + 16 + 4 + 2 = 150.

01101100

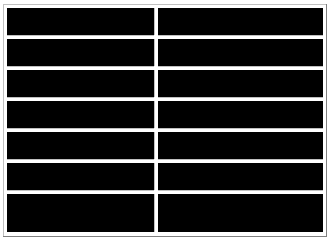
Which bits are on? The 64, 32, 8, and 4 bits are on, so we just need to add them up: 64 + 32 + 8 + 4 = 108.

11101000

Which bits are on? The 128, 64, 32, and 8 bits are on, so just add the values up: 128 + 64 + 32 + 8 = 232.

I highly recommend that you memorize Table 2.2 before braving the IP sections in Chapter 3, "Introduction to TCP/IP," and Chapter 4, "Easy Subnetting"!

TABLE 2.2 Binary to decimal memorization chart

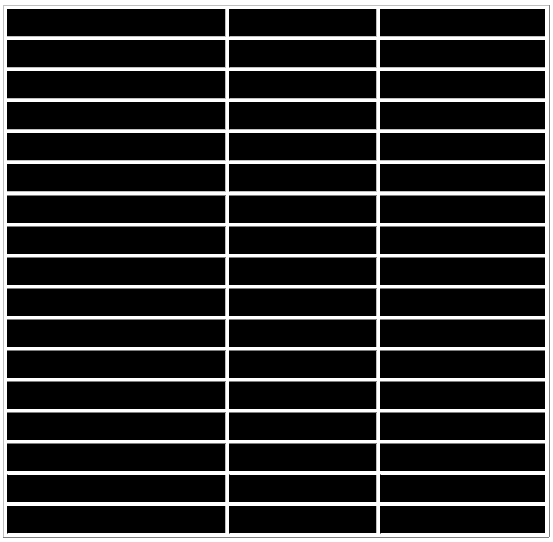


Hexadecimal addressing is completely different than binary or decimal—it's converted by reading nibbles, not bytes. By using a nibble, we can convert these bits to hex pretty simply. First, understand that the hexadecimal addressing scheme uses only the characters 0 through 9. Because the numbers 10, 11, 12, and so on can't be used (because they are two-digit numbers), the letters *A*, *B*, *C*, *D*, *E*, and *F* are used instead to represent 10, 11, 12, 13, 14, and 15, respectively.

Hex is short for *hexadecimal*, which is a numbering system that uses the first six letters of the alphabet, *A* through *F*, to extend beyond the available 10 characters in the decimal system. These values are not case sensitive.

Table 2.3 shows both the binary value and the decimal value for each hexadecimal digit.

TABLE 2.3 Hex to binary to decimal chart



Did you notice that the first 10 hexadecimal digits (0–9) are the same value as the decimal values? If not, look again because this handy fact makes those values super easy to convert!

Now suppose you have something like this: 0x6A. This is important because sometimes Cisco likes to put *0x* in front of characters so you know that they are a hex value. It doesn't have any other special meaning. So what are the binary and decimal values? All you have to remember is that each hex character is one nibble and that two hex characters joined together make a byte. To figure out the binary value, put the hex characters into two nibbles and then join them together into a byte. Six equals 0110, and A, which is 10 in hex, equals 1010, so the complete byte would be 01101010.

To convert from binary to hex, just take the byte and break it into nibbles. Let me clarify this.

Say you have the binary number 01010101. First, break it into nibbles—0101 and 0101—with the value of each nibble being 5 since the 1 and 4 bits are on. This makes the hex answer 0x55. And in decimal format, the binary number is 01010101, which converts to 64 + 16 + 4 + 1 = 85.

Here's another binary number:

11001100

Your answer would be 1100 = 12 and 1100 = 12, so therefore, it's converted to CC in hex. The decimal conversion answer would be 128 + 64 + 8 + 4 = 204.

One more example, then we need to get working on the Physical layer. Suppose you had the following binary number:

10110101

The hex answer would be 0xB5, since 1011 converts to B and 0101 converts to 5 in hex value. The decimal equivalent is 128 + 32 + 16 + 4 + 1 = 181.

Make sure you check out Written Lab 2.1 for more practice with binary/decimal/hex conversion!

Ethernet Frames

The Data Link layer is responsible for combining bits into bytes and bytes into frames. Frames are used at the Data Link layer to encapsulate packets handed down from the Network layer for transmission on a type of media access.

The function of Ethernet stations is to pass data frames between each other using a group of bits known as a MAC frame format. This provides error detection from a *cyclic redundancy check (CRC)*. But remember—this is error detection, not error correction. An example of a typical Ethernet frame used today is shown in Figure 2.8.

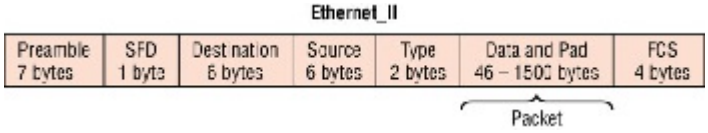


FIGURE 2.8 Typical Ethernet frame format

Encapsulating a frame within a different type of frame is called *tunneling*.

Following are the details of the various fields in the typical Ethernet frame type:

Preamble An alternating 1,0 pattern provides a 5 MHz clock at the start of each packet, which allows the rec eiving devices to lock the incoming bit stream.

Start Frame Delimiter (SFD)/Synch The preamble is seven octets and the SFD is one octet (synch). The SFD is 10101011, where the last pair of 1s allows the receiver to come into the alternating 1,0 pattern somewhere in the middle and still sync up to detect the beginning of the data.

Destination Address (DA) This transmits a 48-bit value using the least significant bit (LSB) first. The DA is used by receiving stations to determine whether an incoming packet is addressed to a particular node. The destination address can be an individual address or a broadcast or multicast MAC address. Remember that a broadcast is all 1s —all *F*s in hex—and is sent to all devices. A multicast is sent only to a similar subset of nodes on a network.

Source Address (SA) The SA is a 48-bit MAC address used to identify the transmitting device, and it uses the least significant bit first. Broadcast and multicast address formats are illegal within the SA field.

Length or Type 802.3 uses a Length field, but the Ethernet_II frame uses a Type field to identify the Network layer protocol. The old, original 802.3 cannot identify the upper-layer protocol and must be used with a proprietary LAN—IPX, for example.

Data This is a packet sent down to the Data Link layer from the Network layer. The size can vary from 46 to 1,500 bytes.

Frame Check Sequence (FCS) FCS is a field at the end of the frame that's used to store the cyclic redundancy check (CRC) answer. The CRC is a mathematical algorithm that's run when each frame is built based on the data in the frame. When a receiving host receives the frame and runs the CRC, the answer should be the same. If not, the frame is discarded, assuming errors have occurred.

Let's pause here for a minute and take a look at some frames caught on my trusty network analyzer. You can see that the frame below has only three fields: Destination, Source, and Type, which is shown as Protocol Type on this particular analyzer:

```
Destination:   00:60:f5:00:1f:27
Source:        00:60:f5:00:1f:2c
Protocol Type: 08-00 IP
```

This is an Ethernet_II frame. Notice that the Type field is IP, or 08-00, mostly just referred to as 0x800 in hexadecimal.

The next frame has the same fields, so it must be an Ethernet_II frame as well:

```
Destination:   ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:        02:07:01:22:de:a4
Protocol Type: 08-00 IP
```

Did you notice that this frame was a broadcast? You can tell because the destination hardware address is all 1s in binary, or all *F*s in hexadecimal.

Let's take a look at one more Ethernet_II frame. I'll talk about this next example again when we use IPv6 in Chapter 14, "Internet Protocol Version 6 (IPv6)," but you can see that the Ethernet frame is the same Ethernet_II frame used with the IPv4 routed protocol. The Type field has 0x86dd when the frame is carrying IPv6 data, and when we have IPv4 data, the frame uses 0x0800 in the protocol field:

```
Destination: IPv6-Neighbor-Discovery_00:01:00:03 (33:33:00:01:00:03)
Source: Aopen_3e:7f:dd (00:01:80:3e:7f:dd)
Type: IPv6 (0x86dd)
```

This is the beauty of the Ethernet_II frame. Because of the Type field, we can run any Network layer routed protocol and the frame will carry the data because it can identify the Network layer protocol!

Ethernet at the Physical Layer

Ethernet was first implemented by a group called DIX, which stands for Digital, Intel, and Xerox. They created and implemented the first Ethernet LAN specification, which the IEEE used to create the IEEE 802.3 committee. This was a 10 Mbps network that ran on coax and then eventually twisted-pair and fiber physical media.

The IEEE extended the 802.3 committee to three new committees known as 802.3u (Fast Ethernet), 802.3ab (Gigabit Ethernet on category 5), and then finally one more, 802.3ae (10 Gbps over fiber and coax). There are more standards evolving almost daily, such as the new 100 Gbps Ethernet (802.3ba)!

When designing your LAN, it's really important to understand the different types of Ethernet media available to you. Sure, it would be great to run Gigabit Ethernet to each desktop and 10 Gbps between switches, but you would need to figure out how to justify the cost of that network today! However, if you mix and match the different types of Ethernet media methods currently available, you can come up with a cost-effective network solution that works really great.

The *EIA/TIA* (Electronic Industries Alliance and the newer Telecommunications Industry Association) is the standards body that creates the Physical layer specifications for Ethernet. The EIA/TIA specifies that Ethernet use a *registered jack (RJ) connector* on *unshielded twisted-pair (UTP)* cabling (RJ45). But the industry is moving toward simply calling this an 8-pin modular connector.

Every Ethernet cable type that's specified by the EIA/TIA has inherent attenuation, which is defined as the loss of signal strength as it travels the length of a cable and is measured in decibels (dB). The cabling used in corporate and home markets is measured in categories. A higher-quality cable will have a higher-rated category and lower attenuation. For example, category 5 is better than category 3 because category 5 cables have more wire twists per foot and therefore less crosstalk. Crosstalk is the unwanted signal interference from adjacent pairs in the cable.

Here is a list of some of the most common IEEE Ethernet standards, starting with 10 Mbps Ethernet:

10Base-T (IEEE 802.3) 10 Mbps using category 3 unshielded twisted pair (UTP) wiring for runs up to 100 meters. Unlike with the 10Base-2 and 10Base-5 networks, each device must connect into a hub or switch, and you can have only one host per segment or wire. It uses an RJ45 connector (8-pin modular connector) with a physical star topology and a logical bus.

100Base-TX (IEEE 802.3u) 100Base-TX, most commonly known as Fast Ethernet, uses EIA/TIA category 5, 5E, or 6 UTP two-pair wiring. One user per segment; up to 100 meters long. It uses an RJ45 connector with a physical star topology and a logical bus.

100Base-FX (IEEE 802.3u) Uses fiber cabling 62.5/125-micron multimode fiber. Point-to-point topology; up to 412 meters long. It uses ST and SC connectors, which are media-interface connectors.

1000Base-CX (IEEE 802.3z) Copper twisted-pair, called twinax, is a balanced coaxial pair that can run only up to 25 meters and uses a special 9-pin connector known as the High Speed Serial Data Connector (HSSDC). This is used in Cisco's new Data Center technologies.

1000Base-T (IEEE 802.3ab) Category 5, four-pair UTP wiring up to 100 meters long and up to 1 Gbps.

1000Base-SX (IEEE 802.3z) The implementation of 1 Gigabit Ethernet running over multimode fiber-optic cable instead of copper twisted-pair cable, using short wavelength laser. Multimode fiber (MMF) using 62.5- and 50-micron core; uses an 850 nanometer (nm) laser and can go up to 220 meters with 62.5-micron, 550 meters with 50-micron.

1000Base-LX (IEEE 802.3z) Single-mode fiber that uses a 9-micron core and 1300 nm laser and can go from 3 kilometers up to 10 kilometers.

1000Base-ZX (Cisco standard) 1000BaseZX, or 1000Base-ZX, is a Cisco specified standard for Gigabit Ethernet communication. 1000BaseZX operates on ordinary single-mode fiber-optic links with spans up to 43.5 miles (70 km).

10GBase-T (802.3.an) 10GBase-T is a standard proposed by the IEEE 802.3an committee to provide 10 Gbps connections over conventional UTP cables, (category 5e, 6, or 7 cables). 10GBase-T allows the conventional RJ45 used for Ethernet LANs and can support signal transmission at the full 100-meter distance specified for LAN wiring.

If you want to implement a network medium that is not susceptible to electromagnetic interference (EMI), fiber-optic cable provides a more secure, long-distance cable that is not susceptible to EMI at high speeds.

Armed with the basics covered so far in this chapter, you're equipped to go to the next level and put Ethernet to work using various Ethernet cabling.

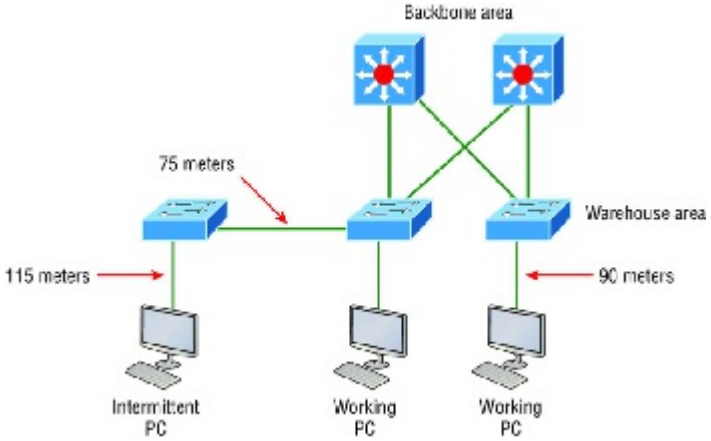
Interference or Host Distance Issue?

Quite a few years ago, I was consulting at a very large aerospace company in the Los Angeles area. In the very busy warehouse, they had hundreds of hosts providing many different services to the various departments working in that area.

However, a small group of hosts had been experiencing intermittent outages that no one could explain since most hosts in the same area had no problems whatsoever. So I decided to take a crack at this problem and see what I could find.

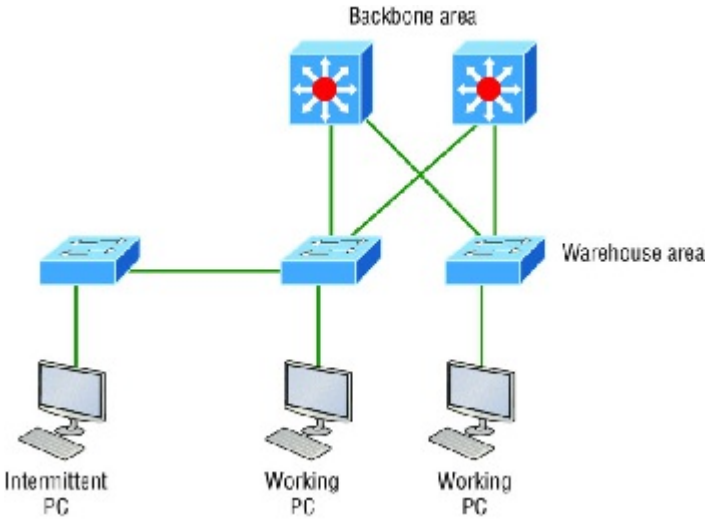
First, I traced the backbone connection from the main switch to multiple switches in the warehouse area. Assuming that the hosts with the issues were connected to the same switch, I traced each cable, and much to my surprise they were connected to various switches! Now my interest really peaked because the simplest issue had been eliminated right off the bat. It wasn't a simple switch problem!

I continued to trace each cable one by one, and this is what I found:



As I drew this network out, I noticed that they had many repeaters in place, which isn't a cause for immediate suspicion since bandwidth was not their biggest requirement here. So I looked deeper still. At this point, I decided to measure the distance of one of the intermittent hosts connecting to their hub/repeater.

This is what I measured. Can you see the problem?



Having a hub or repeater in your network isn't a problem, unless you need better bandwidth (which they didn't in this case), but the distance was! It's not always easy to tell how far away a host is from its connection in an extremely large area, so these hosts ended up having a connection past the 100-meter Ethernet specification, which created a problem for the hosts not cabled correctly. Understand that this didn't stop the hosts from completely working, but the workers felt the hosts stopped working when they were at their most stressful point of the day. Sure, that makes sense, because whenever my host stops working, that becomes my most stressful part of the day!

Ethernet Cabling

A discussion about Ethernet cabling is an important one, especially if you are planning on taking the Cisco exams. You need to really understand the following three types of cables:

1. Straight-through cable
2. Crossover cable
3. Rolled cable

We will look at each in the following sections, but first, let's take a look at the most common Ethernet cable used today, the category 5 Enhanced Unshielded Twisted Pair (UTP), shown in Figure 2.9.

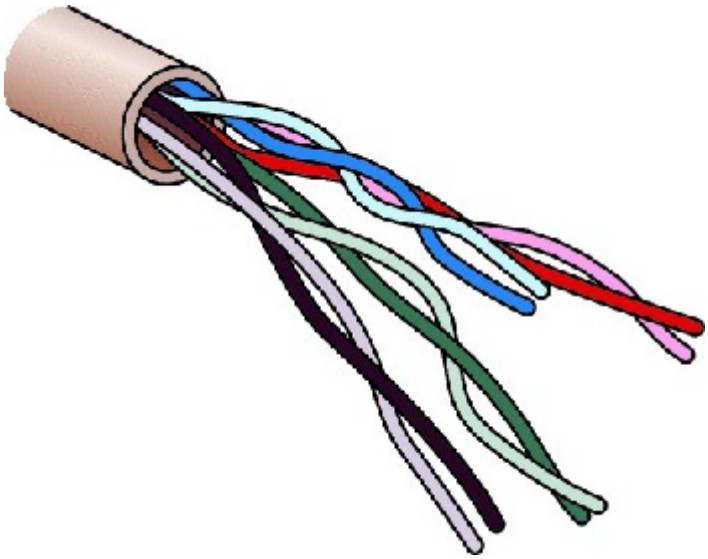


FIGURE 2.9 Category 5 Enhanced UTP cable

The category 5 Enhanced UTP cable can handle speeds up to a gigabit with a distance of up to 100 meters. Typically we'd use this cable for 100 Mbps and category 6 for a gigabit, but the category 5 Enhanced is rated for gigabit speeds and category 6 is rated for 10 Gbps!

Straight-Through Cable

The *straight-through cable* is used to connect the following devices:

1. Host to switch or hub
2. Router to switch or hub

Four w ires are used in straight-through cable to connect Ethernet devices. It's relatively simple to create this type, and Figure 2.10 shows the four wires used in a straight-through Ethernet cable.

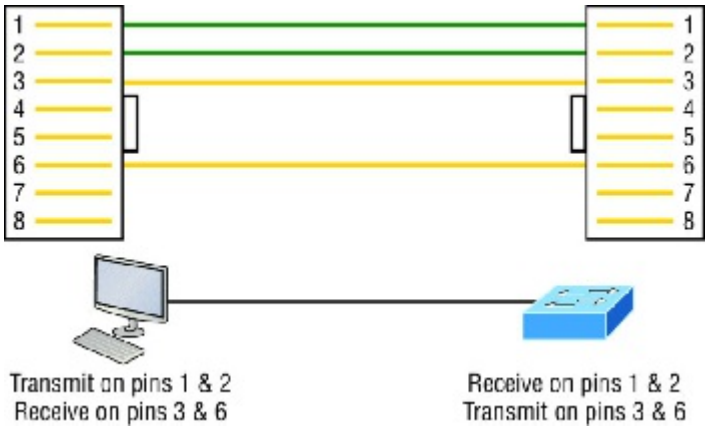


FIGURE 2.10 Straight-through Ethernet cable

Notice that only pins 1, 2, 3, and 6 are used. Just connect 1 to 1, 2 to 2, 3 to 3, and 6 to 6 and you'll be up and networking in no time. However, remember that this would be a 10/100 Mbps Ethernet-only cable and wouldn't work with gigabit, voice, or other LAN or WAN technology.

Crossover Cable

The *crossover cable* can be used to connect the following devic es:

1. Switch to switch

2. Hub to hub
3. Host to host
4. Hub to switch
5. Router direct to host
6. Router to router

The same four wires used in the straight-through cable are used in this cable—we just connect different pins together. Figure 2.11 shows how the four wires are used in a crossover Ethernet cable.

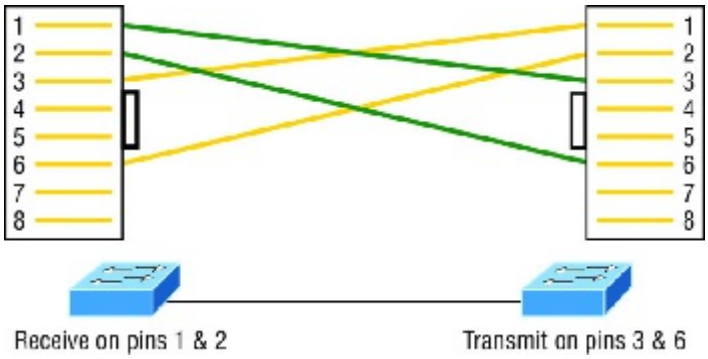


FIGURE 2.11 Crossover Ethernet cable

Notice that instead of connecting 1 to 1, 2 to 2, and so on, here we connect pins 1 to 3 and 2 to 6 on each side of the cable. Figure 2.12 shows some typical uses of straight-through and crossover cables.

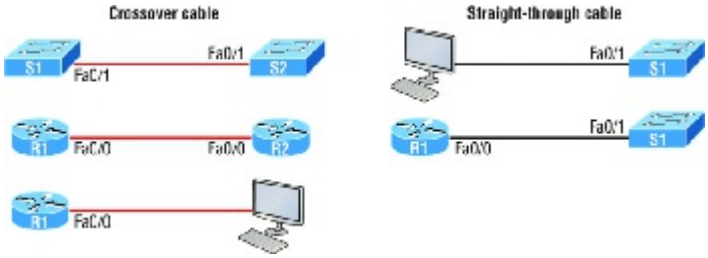


FIGURE 2.12 Typical uses for straight-through and cross-over Ethernet cables

The crossover examples in Figure 2.12 are switch port to switch port, router Ethernet po rt to router Ethernet port, and router Ethernet port to PC Ethernet port. For the straight-through examples I used PC Ethernet to switch port and router Ethernet port to switch port.

It's very possible to connect a straight-through cable between two switches, and it will start working because of autodetect mechanisms called auto-mdix. But be advised that the CCNA objectives do not typically consider autodetect mechanisms valid between devices!

UTP Gigabit Wiring (1000Base-T)

In the previous examples of 10Base-T and 100Base-T UTP wiring, only two wire pairs were used, but that is not good enough for Gigabit UTP transmission.

1000Base-T UTP wiring (Figure 2.13) requires four wire pairs and uses more advanced electronics so that each and every pair in the cable can transmit simultaneously. Even so, gigabit wiring is almost identical to my earlier 10/100 example, except that we'll use the other two pairs in the cable.

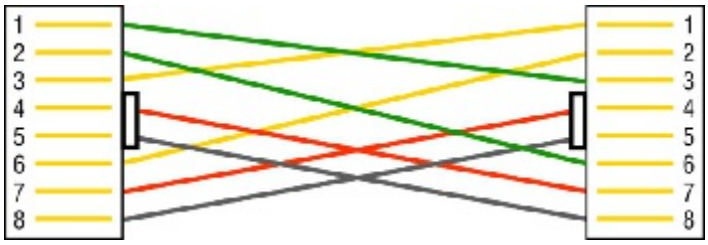


FIGURE 2.13 UTP Gigabit crossover Ethernet cable

For a straight-through cable it's still 1 to 1, 2 to 2, and so on up to pin 8. And in creating the gigabit crossover cable, you'd still cross 1 to 3 and 2 to 6, but you would add 4 to 7 and 5 to 8—pretty straightforward!

Rolled Cable

Although *rolled cable* isn't used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host EIA-TIA 232 interface to a router console serial communication (COM) port.

If you have a Cisco router or switch, you would use this cable to connect your PC, Mac, or a device like an iPad to the Cisco hardware. Eight wires a re used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networking. Figure 2.14 shows the eight wires used in a rolled cable.

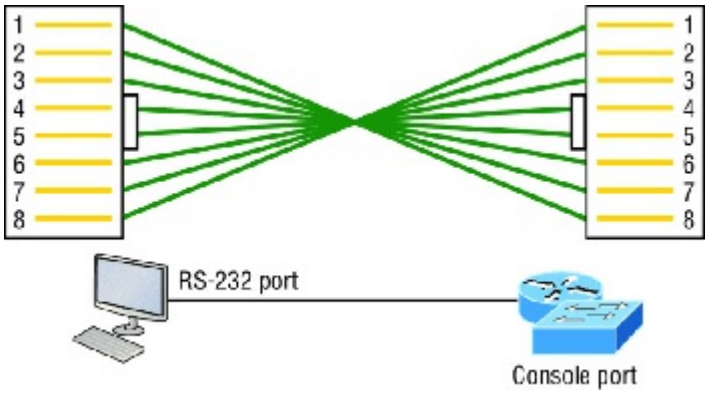


FIGURE 2.14 Rolled Ethernet cable

These are probably the easiest cables to make because you just cut the end off on one side of a straight-through cable, turn it over, and put it back on—with a new connector, of course!

Okay, once you have the correct cable connected from your PC to the Cisco router or switch console port, you can start your emulation program such as PuTTY or SecureCRT to create a console connection and configure the device. Set the configuration as shown in Figure 2.15 .

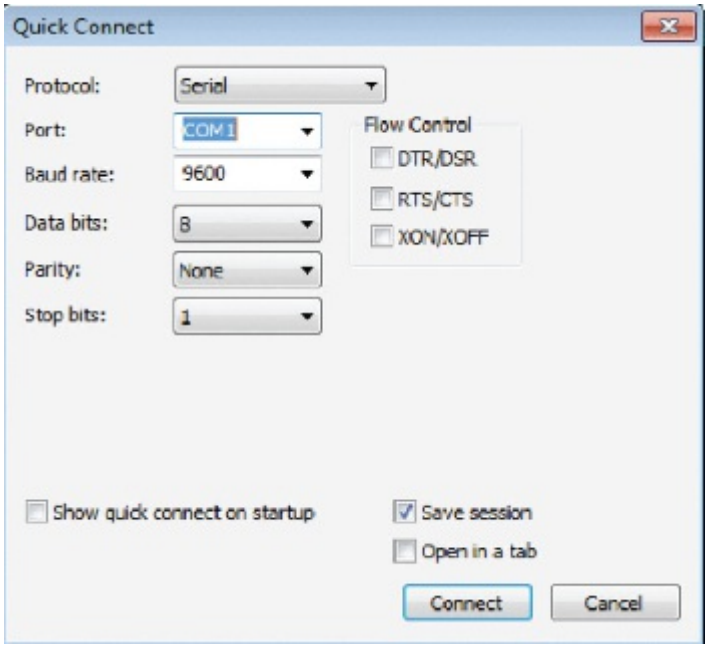


FIGURE 2.15 Configuring your console emulation program

Notice that Baud Rate is set to 9600, Data Bits to 8, Parity to None, and no Flow Control options are set. At this point, you can click Connect and press the Enter key and you should be connected to your Cisco device console port.

Figure 2.16 shows a nice new 2960 switch with two console ports.

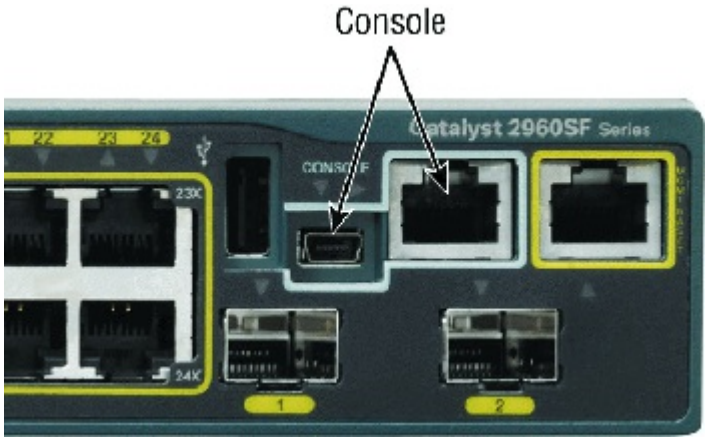


FIGURE 2.16 A Cisco 2960 console connections

Notice there are two console connections on this new switch—a typical original RJ45 con nection and the newer mini type-B USB console. Remember that the new USB port supersedes the RJ45 port if you just happen to plug into both at the same time, and the USB port can have speeds up to 115,200 Kbps, which is awesome if you have to use Xmodem to update an IOS. I've even seen some cables that work on iPhones and iPads and allow them to connect to these mini USB ports!

Now that you've seen the various RJ45 unshielded twisted-pair (UTP) cables, what type of cable is used between the switches in Figure 2.17?

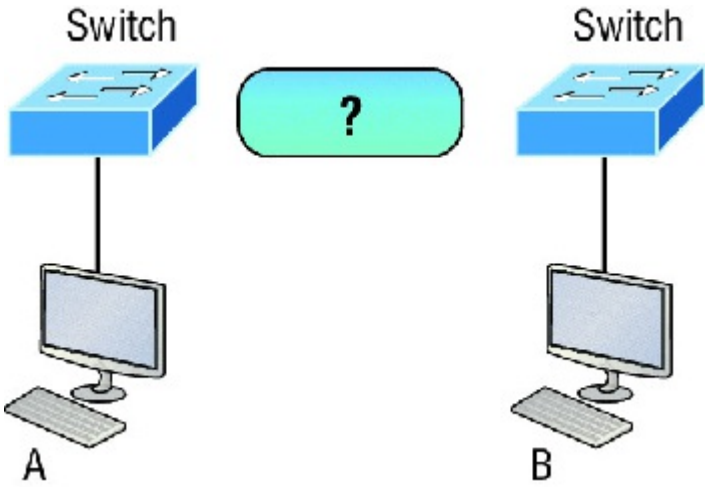


FIGURE 2.17 RJ45 UTP cable question #1

In order for host A to ping host B, you need a crossover cable to connect the two switches together. But what types of cables are used in the network shown in Figure 2.18?

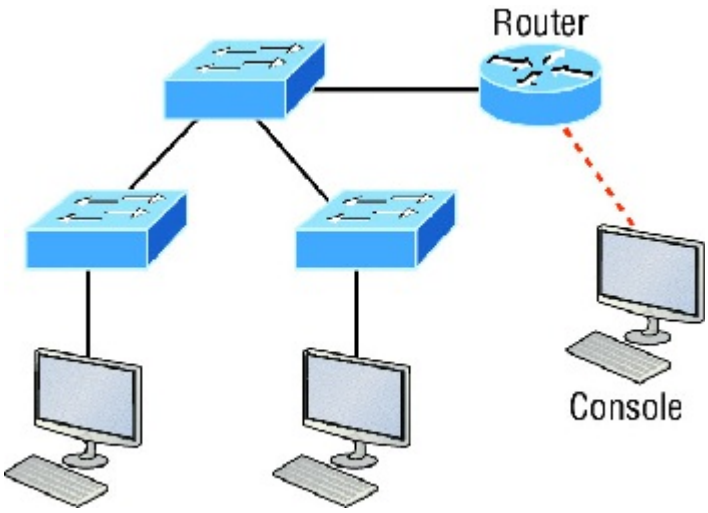


FIGURE 2.18 RJ45 UTP cable question #2

In Figure 2.18, there's a whole menu of cables in use. For the connection between the switches, we'd obviously use a crossover cable like we saw in Figure 2.13. The trouble is that you must understand that we have a console connection that uses a rolled cable. Plus, the connection from the router to the switch is a straight-through cable, as is true for the hosts to the switches. Keep in mind that if we had a serial connection, which we don't, we wou ld use a V.35 to connect us to a WAN.

Fiber Optic

Fiber-optic cabling has been around for a long time and has some solid standards. The cable allows for very fast transmission of data, is made of glass (or even plastic!), is very thin, and works as a waveguide to transmit light between two ends of the fiber. Fiber optics has been used to go very long distances, as in intercontinental connections, but it is becoming more and more popular in Ethernet LAN networks due to the fast speeds available and because, unlike UTP, it's immune to interference like cross-talk.

Some main components of this cable are the core and the cladding. The core will hold the light and the cladding confines the light in the core. The tighter the cladding, the smaller the core, and when the core is small, less light will be sent, but it can go faster and farther!

In Figure 2.19 you can see that there is a 9-micron core, which is very small and can be measured against a human hair, which is 50 microns.

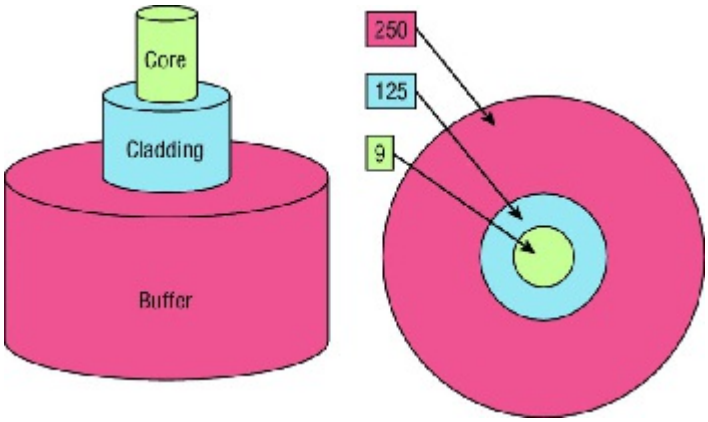


FIGURE 2.19 Typical fiber cable.

Dimensions are in um (10^{-6} meters). Not to scale.

The cladding is 125 microns, which is actually a fiber standard that allows manufacturers to make connectors for all fiber cables. The last piece of this cable is the buffer, which is there to protect the delicate glass.

There are two major types of fiber optics: single-mode and multimode. Figure 2.20 shows the differences between multimode and single-mode fibers.

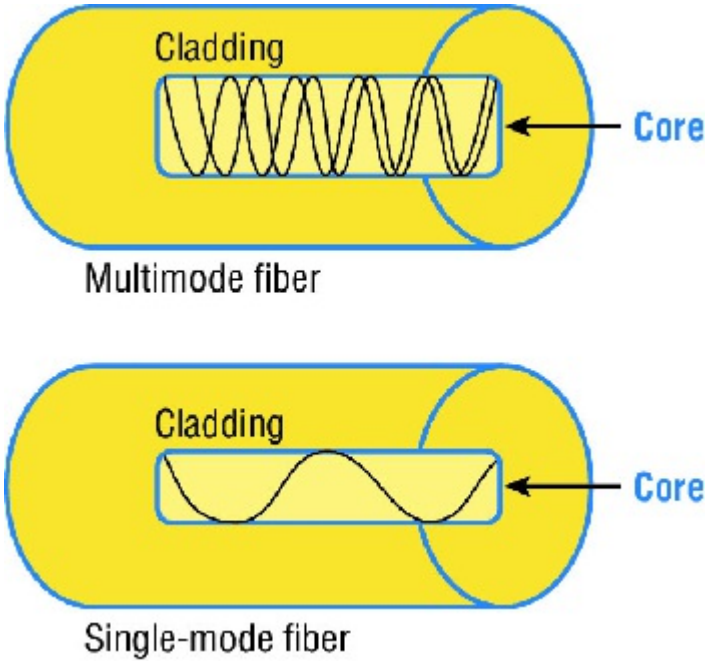


FIGURE 2.20 Multimode and single-mode fibers

Single-mode is more expensive, has a tighter cladding, and can go much farther distances than multimode. The difference comes in the tightness of the cladding, which makes a smaller core, meaning that only one mode of light will propagate down the fiber. Multimode is looser and has a larger core so it allows multiple light particles to travel down the glass. These particles have to be put back together at the receiving end, so distance is less than that with single-mode fiber, which allows only very few light particles to travel down the fiber.

There are about 70 different connectors for fiber, and Cisco uses a few different types. Looking back at Figure 2.16, the two bottom ports are referred to as Small Form-Factor Pluggables, or SFPs.

Data Encapsulation

When a host transmits data across a network to another device, the data goes through a process called *encapsulation* and is wrapped with protocol information at each layer of the OSI model. Each layer communicates

only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses *protocol data units (PDUs)*. These hold the control information attached to the data at each layer of the model. They are usually attached to the header in front of the data field but can also be at the trailer, or end, of it.

Each PDU attaches to the data by encapsulating it at each layer of the OSI model, and each has a specific name depending on the information provided in each header. This PDU information is read only by the peer layer on the receiving device. After its read, it's stripped off and the data is then handed to the next layer up.

Figure 2.21 shows the PDUs and how they attach control information to each layer. This figure demonstrates how the upper-layer user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending over a synch packet. Next, the data stream is broken up into smaller pieces, and a Transport layer header is created and attached to the header of the data field; now the piece of data is called a *segment* (a PDU). Each segment can be sequenced so the data stream can be put back together on the receiving side exactly as it was transmitted.

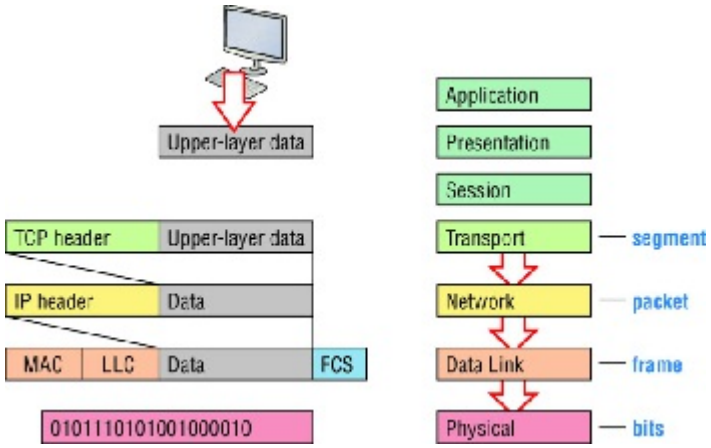


FIGURE 2.21 Data encapsulation

Each segment is then handed to the Network layer for network addressing and routing through the internetwork. Logical addressing (for example, IP and IPv6) is used to get each segment to the correct network. The Network layer protocol adds a control header to the segment handed down from the Transport layer, and what we have now is called a *packet* or *datagram*. Remember that the Transport and Network layers work together to rebuild a data stream on a receiving host, but it's not part of their work to place their PDUs on a local network segment—which is the only way to get the information to a router or host.

It's the Data Link layer that's responsible for taking packets from the Network layer and placing them on the network m edium (cable or wireless). The Data Link layer encapsulates each packet in a *frame*, and the frame's header carries the hardware addresses of the source and destination hosts. If the destination device is on a remote network, then the frame is sent to a router to be routed through an internetwork. Once it gets to the destination network, a new frame is used to get the packet to the destination host.

To put this frame on the network, it must first be put into a digital signal. Since a frame is really a logical group of 1s and 0s, the physical layer is responsible for encoding these digits into a digital signal, which is read by devices on the same local network. The receiving devices will synchronize on the digital signal and extract (decode) the 1s and 0s from the digital signal. At this point, the devices reconstruct the frames, run a CRC, and then check their answer against the answer in the frame's FCS field. If it matches, the packet is pulled from the frame and what's left of the frame is discarded. This process is called *de-encapsulation*. The packet is handed to the Network layer, where the address is checked. If the address matches, the segment is pulled from the packet and what's left of the packet is discarded. The segment is processed at the Transport layer, which rebuilds the data stream and acknowledges to the transmitting station that it received each piece. It then happily hands the data stream to the upper-layer application.

At a transmitting device, the data encapsulation method works like this:

1. User information is converted to data for transmission on the network.
2. Data is converted to segments, and a reliable connection is set up between the transmitting and receiving hosts.
3. Segments are converted to packets or datagrams, and a logical address is placed in the header so each packet can be routed through an internetwork.

4. Packets or datagrams are converted to frames for transmission on the local network. Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.
5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

To explain this in more detail using the layer addressing, I'll use Figure 2.22.

Remember that a data stream is handed down from the upper layer to the Transport layer. As technicians, we really don't care who the data stream comes from because that's really a programmer's problem. Our job is to rebuild the data stream reliably and hand it to the upper layers on the receiving device.

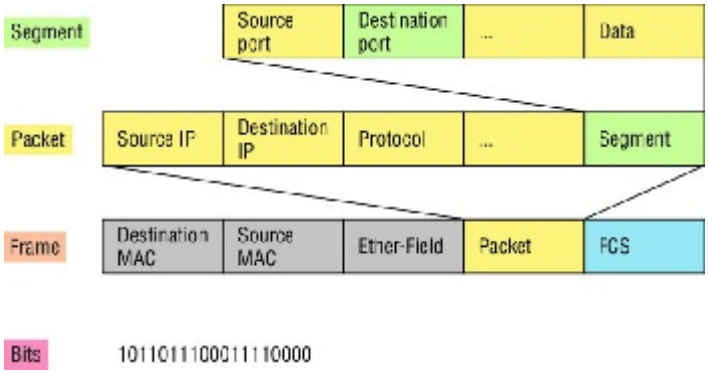


FIGURE 2.22 PDU and layer addressing

Before we go further in our discussion of Figure 2.22, let's discuss port numbers and make sure you understand them. The Transport layer uses port numbers to define both th e virtual circuit and the upper-layer processes, as you can see from Figure 2.23.

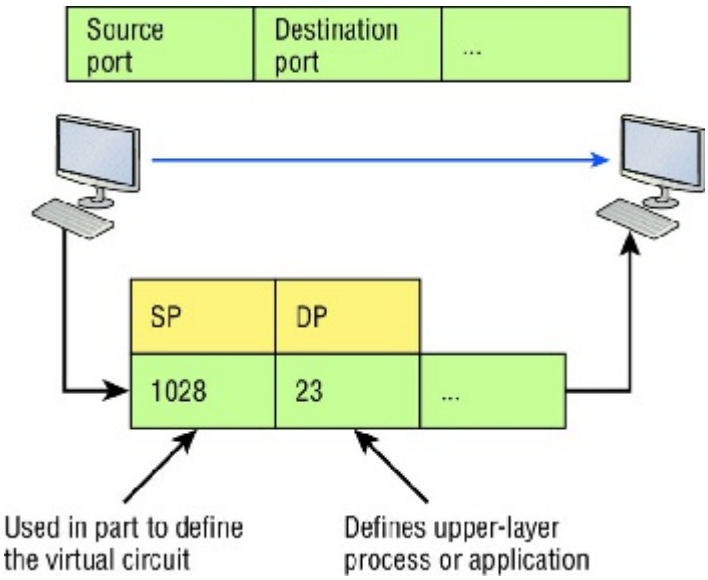


FIGURE 2.23 Port numbers at the Transport layer

When using a connection-oriented protocol like TCP, the Transport layer takes the data stream, makes segments out of it, and establishes a reliable session by creating a virtual circuit. It then sequences (numbers) each segment and uses acknowledgments and flow control. If you're using TCP, the virtual circuit is defined by the source and destination port number plus the source and destination IP address and called a socket. Understand that the host just makes this up, starting at port number 1024 because 0 through 1023 are reserved for well-known port numbers. The destination port number defines the upper-layer process or application that the dat a stream is handed to when the data stream is reliably rebuilt on the receiving host.

Now that you understand port numbers and how they are used at the Transport la yer, let's go back to Figure 2.22. Once the Transport layer header information is added to the piece of data, it becomes a segment that's handed down to the Network layer along with the destination IP address. As you know, the destination IP address was handed down from the upper layers to the Transport layer with the data stream and was identified via name resolution at the upper layers—probably with DNS.

The Network layer adds a header and adds the logical addressing such as IP addresses to the front of each segment. Once the header is added to the segment, the PDU is called a packet. The packet has a protocol field that describes where the segment came from (either UDP or TCP) so it can hand the segment to the correct protocol at the Transport layer when it reaches the receiving host.

The Network layer is responsible for finding the destination hardware address that dictates where the packet should be sent on the local network. It does this by using the Address Resolution Protocol (ARP)—something I'll talk about more in Chapter 3. IP at the Network layer looks at the destination IP address and compares that address to its own source IP address and subnet mask. If it turns out to be a local network request, the hardware address of the local host is requested via an ARP request. If the packet is destined for a host on a remote network, IP will look for the IP address of the default gateway (router) instead.

The packet, along with the destination hardware address of either the local host or default gateway, is then handed down to the Data Link layer. The Data Link layer will add a header to the front of the packet and the piece of data then becomes a frame. It's called a frame because both a header and a trailer are added to the packet, which makes it look like it's within bookends—a frame—as shown in Figure 2.22. The frame uses an Ether-Type field to describe which protocol the packet came from at the Network layer. Now a cyclic redundancy check is run on the frame, and the answer to the CRC is placed in the Frame Check Sequence field found in the trailer of the frame.

The frame is now ready to be handed down, one bit at a time, to the Physical layer, which will use bit-timing rules to encode the data in a digital signal. Every device on the network segment will receive the digital signal and synchronize with the clock and extract the 1s and 0s from the digital signal to build a frame. After the frame is rebuilt, a CRC is run to make sure the frame is in proper order. If everything turns out to be all good, the hosts will check the destination MAC and IP addresses to see if the frame is for them.

If all this is making your eyes cross and your brain freeze, don't freak. I'll be going over exactly how data is encapsulated and routed through an internetwork later, in Chapter 9, "IP Routing."

The Cisco Three-Layer Hierarchical Model

Most of us were exposed to hierarchy early in life. Anyone with older siblings learned what it was like to be at the bottom of the hierarchy. Regardless of where you first discovered the concept of hierarchy, most of us experience it in many aspects of our lives. It's *hierarchy* that helps us understand where things belong, how things fit together, and what functions go where. It brings order to otherwise complex models. If you want a pay raise, for instance, hierarchy dictates that you ask your boss, not your subordinate, because that's the person whose role it is to grant or deny your request. So basically, understanding hierarchy helps us discern where we should go to get what we need.

Hierarchy has many of the same benefits in network design that it does in other areas of life. When used properly, it makes networks more predict able and helps us define which areas should perform certain functions. Likewise, you can use tools such as access lists at certain levels in hierarchical networks and avoid them at others.

Let's face it: Large networks can be extremely complicated, with multiple protocols, detailed configurations, and diverse technologies. Hierarchy helps us summarize a complex collection of details into an understandable model, bringing order from the chaos. Then, as specific configurations are needed, the model dictates the appropriate manner in which to apply them.

The Cisco hierarchical model can help you design, implement, and maintain a scalable, reliable, cost-effective hierarchical internetwork. Cisco defines three layers of hierarchy, as shown in Figure 2.24, each with specific functions.

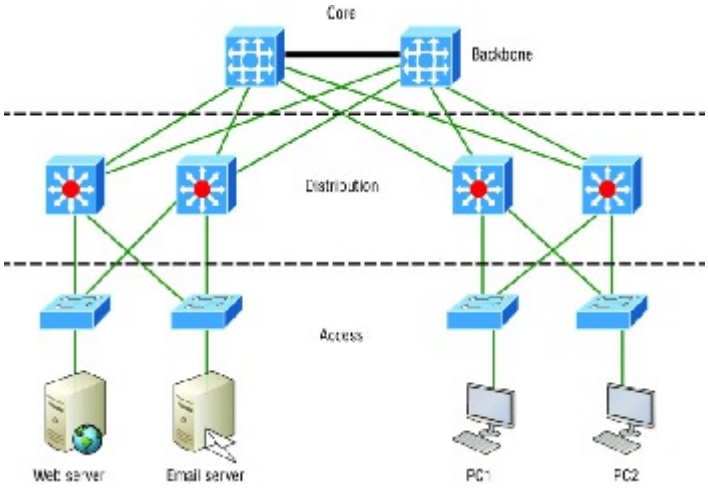


FIGURE 2.24 The Cisco hierarchical model

Each layer has specific responsibilities. Keep in mind that the three layers are logical and are not necessarily physical devices. Consider the OSI model, another logical hierarchy. Its seven layers describe functions but not necessarily protocols, right? Sometimes a protocol maps to more than one layer of the OSI model, and sometimes multiple protocols communicate within a single layer. In the same way, when we build physical implementations of hierarchical networks, we may have many devices in a single layer, or there may be a single device performing functions at two layers. Just remember that the definition of the layers is logical, not physical!

So let's take a closer look at each of the layers now.

The Core Layer

The *core layer* is literally the core of the network. At the top of the hierarchy, the core layer is responsible for transporting large amounts of traffic both reliably and quickly. The only purpose of the network's core layer is to switch traffic as fast as possible. The traffic transported across the core is common to a majority of users. But remember that user data is processed at the distribution layer, which forwards the requests to the core if needed.

If there's a failure in the core, *every single user* can be affected! This is why fault tolerance at this layer is so important. The core is likely to see large volumes of traffic, so speed and latency are driving concerns here. Given the function of the core, we can now consider some design specifics. Let's start with some things we don't want to do:

1. Never do anything to slow down traffic. This includes making sure you don't use access lists, perform routing between virtual local area networks, or implement packet filtering.
2. Don't support workgroup access here.
3. Avoid expanding the core (e.g., adding routers when the internetwork grows). If performance becomes an issue in the core, give preference to upgrades over expansion.

Here's a list of things that we want to achieve as we design the core:

1. Design the core for high reliability. Consider data-link technologies that facilitate both speed and redundancy, like Gigabit Ethernet with redundant links or even 10 Gigabit Ethernet.
2. Design with speed in mind. The core should have very little latency.
3. Select routing protocols with lower convergence times. Fast and redundant data-link connectivity is no help if your routing tables are shot!

The Distribution Layer

The *distribution layer* is sometimes referred to as the *workgroup layer* and is the communication point between the access layer and the core. The primary functions of the distribution layer are to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed. The distribution layer must determine the fastest way that network service requests are handled—for example, how a file request is forwarded to a server. After the distribution layer determines the best path, it forwards the request to the core layer if necessary. The core layer then quickly transports the request to the correct service.

The distribution layer is where we want to implement policies for the network because we are allowed a lot of flexibility in defining network operation here. There are several things that should generally be handled at the distribution layer:

1. Routing
2. Implementing tools (such as access lists), packet filtering, and queuing
3. Implementing security and network policies, including address translation and firewalls
4. Redistributing between routing protocols, including static routing
5. Routing between VLANs and other workgroup support functions
6. Defining broadcast and multicast domains

Key things to avoid at the distribution layer are those that are limited to functions that exclusively belong to one of the other layers!

The Access Layer

The *access layer* controls user and workgroup access to internetwork resources. The access layer is sometimes referred to as the *desktop layer*. The network resources most users need will be available locally because the distribution layer handles any traffic for remote services.

The following are some of the functions to be included at the access layer:

1. Continued (from distribution layer) use of access control and policies
2. Creation of separate collision domains (microsegmentation/switches)
3. Workgroup connectivity into the distribution layer
4. Device connectivity
5. Resiliency and security services
6. Advanced technology capabilities (voice/video, etc.)

Technologies like Gigabit or Fast Ethernet switching are frequently seen in the access layer.

I can't stress this enough—just because there are three separate levels does not imply three separate devices! There could be fewer or there could be more. After all, this is a *layered* approach.

Summary

In this chapter, you learned the fundamentals of Ethernet networking, how hosts communicate on a network. You discovered how CSMA/CD works in an Ethernet half-duplex network.

I also talked about the differences between half- and full-duplex modes, and we discussed the collision detection mechanism called CSMA/CD.

I described the common Ethernet cable types used in today's networks in this chapter as well, and by the way, you'd be wise to study that section really well!

Important enough to not gloss over, this chapter provided an introduction to encapsulation. Encapsulation is the process of encoding data as it goes down the OSI stack.

Last, I covered the Cisco three-layer hierarchical model. I described in detail the three layers and how each is used o help design and implement a Cisco internetwork.

Exam Essentials

Describe the operation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD is a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. Although it does not eliminate collisions, it helps to greatly reduce them, which reduces retransmissions, resulting in a more efficient transmission of data for all devices.

Differentiate half-duplex and full-duplex communication and define the requirements to utilize each method. Full-duplex Ethernet uses two pairs of wires at the same time instead of one wire pair like half-duplex. Full-duplex allows for sending and receiving at the same time, using different wires to eliminate collisions, while half-duplex can send or receive but not at the same time and still can suffer collisions. To use full-duplex, the devices at both ends of the cable must be capable of and configured to perfo rm full-duplex.

Describe the sections of a MAC address and the information contained in each section . The MAC, or hardware, address is a 48-bit (6-byte) address written in a hexadecimal format. The first 24 bits, or 3 bytes, are called the organizationally unique identifier (OUI), which is assigned by the IEEE to the manufacturer of the NIC. The balance of the number uniquely identifies the NIC.

Identify the binary and hexadecimal equivalent of a decimal number. Any number expressed in one format can also be expressed in the other two. The ability to perform this conversion is critical to understanding IP

addressing and subnetting. Be sure to go through the written labs covering binary to decimal to hexadecimal conversion.

Identify the fields in the Data Link portion of an Ethernet frame. The fields in the Data Link portion of a frame include the preamble, Start Frame Delimiter, destination MAC address, source MAC address, Length or Type, Data, and Frame Check Sequence.

Identify the IEEE physical standards for Ethernet cabling. These standards describe the capabilities and physical characteristics of various cable types and include but are not limited to 10Base-2, 10Base-5, and 10Base-T.

Differentiate types of Ethernet cabling and identify their proper application. The three types of cables that can be created from an Ethernet cable are straight-through (to connect a PC's or router's Ethernet interface to a hub or switch), crossover (to connect hub to hub, hub to switch, switch to switch, or PC to PC), and rolled (for a console connection from a PC to a router or switch).

Describe the data encapsulation process and the role it plays in packet creation. Data encapsulation is a process whereby information is added to the frame from each layer of the OSI model. This is also called packet creation. Each layer communicates only with its peer layer on the receiving device.

Understand how to connect a console cable from a PC to a router and switch. Take a rolled cable and connect it from the COM port of the host to the console port of a router. Start your emulations program such as putty or SecureCRT and set the bits per second to 9600 and flow control to None.

Identify the layers in the Cisco three-layer model and describe the ideal function of each layer. The three layers in the Cisco hierarchical model are the core (responsible for transporting large amounts of traffic both reliably and quickly), distribution (provides routing, filtering, and WAN access), and access (workgroup connectivity into the distribution layer). Technet24.ir

Written Labs

In this section, you'll complete the following labs to make sure you've got the information and concepts contained within them fully dialed in:

1. Lab 2.1: Binary/Decimal/Hexadecimal Conversion
2. Lab 2.2: CSMA/CD Operations
3. Lab 2.3: Cabling
4. Lab 2.4: Encapsulation

You can find the answers to these labs in Appendix A, "Answers to Written Labs."

Written Lab 2.1: Binary/Decimal/Hexadecimal Conversion

1. Convert from decimal IP address to binary format.

   Complete the following table to express 192.168.10.15 in binary format.

   Complete the following table to express 172.16.20.55 in binary format.

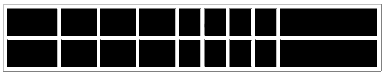
   

   Complete the following table to express 10.11.12.99 in binary format.

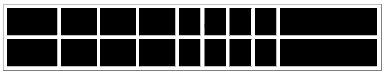
   

2. Convert the following from binary format to decimal IP address.

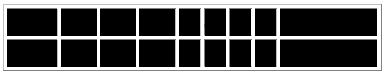
Complete the following table to express 11001100.00110011.10101010.01010101 in decimal IP address format.



Complete the following table to express 11000110.11010011.00111001.11010001 in decimal IP address format.

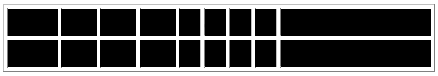


Complete the following table to express 10000100.11010010.10111000.10100110 in decimal IP address format.

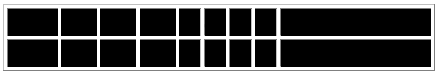


3. Convert the following from binary format to hexadecimal.

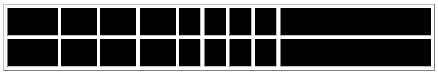
   Complete the following table to express 11011000.00011011.00111101.01110110 in hexadecimal.



Complete the following table to express 11001010.11110101.10000011.11101011 in hexadecimal.



Complete the following table to express 10000100.11010010.01000011.10110011 in hexadecimal.



Written Lab 2.2: CSMA/CD Operations

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) helps to minimize collisions in the network, thereby increasing data transmission efficiency. Place the following steps of its operation in the order in which they occur after a collision.

1. All hosts have equal priority to transmit after the timers have expired.
2. Each device on the Ethernet segment stops transmitting for a short time until the timers expire.
3. The collision invokes a random backoff algorithm.
4. A jam signal informs all devices that a collision occurred.

Written Lab 2.3: Cabling

For each of the following situations, determine whether a straight-through, crossover, or rolled cable would be used.

1. Host to host
2. Host to switch or hub
3. Router direct to host
4. Switch to switch
5. Router to switch or hub
6. Hub to hub
7. Hub to switch